



Configurar e gerenciar backends

Trident

NetApp
October 30, 2026

Índice

Configurar e gerenciar backends	1
Configure os backends do Trident	1
Azure NetApp Files	1
Configurar um backend do Azure NetApp Files	1
Prepare-se para configurar um backend do Azure NetApp Files	4
Opções e exemplos de configuração do backend do Azure NetApp Files	7
Google Cloud NetApp Volumes	18
Configurar Google Cloud NetApp Volumes	18
Configurar o Google Cloud NetApp Volumes para cargas de trabalho SAN	22
Prepare-se para configurar um backend do Google Cloud NetApp Volumes	28
Opções e exemplos de configuração do backend do Google Cloud NetApp Volumes	29
Configurar o auto-tiering para Google Cloud NetApp Volumes	40
Configurar pools de storage do Google Cloud NetApp Volumes em modo ONTAP	42
Configurar um NetApp HCI ou SolidFire backend	46
Detalhes do driver Element	47
Antes de começar	47
Opções de configuração do backend	47
Exemplo 1: configuração de backend para <code>solidfire-san</code> driver com três tipos de volume	48
Exemplo 2: configuração de backend e classe de armazenamento para <code>`solidfire-san`</code> driver com pools virtuais	49
Encontre mais informações	51
Drivers SAN do ONTAP	51
Visão geral do driver ONTAP SAN	51
Prepare-se para configurar o backend com os drivers ONTAP SAN	53
Opções e exemplos de configuração do ONTAP SAN	61
Drivers NAS do ONTAP	78
Visão geral do driver ONTAP NAS	78
Prepare-se para configurar um backend com drivers ONTAP NAS	79
Opções e exemplos de configuração do ONTAP NAS	91
Utilize o posicionamento balanceado com os backends ONTAP	112
Como funciona o posicionamento equilibrado	112
Requisitos	112
Valores padrão	112
Opção de configuração	113
Alocação equilibrada com pools virtuais	113
Exemplos	113
Erros de validação no backend	114
Amazon FSx for NetApp ONTAP	115
Use Trident com Amazon FSx for NetApp ONTAP	115
Crie uma função do IAM e um segredo da AWS	117
Instale Trident	122
Configure uma classe de armazenamento	128
Configurar um PVC	142

Implantar um aplicativo	143
Implante um aplicativo de exemplo	143
Configurar o complemento Trident EKS em um cluster EKS	145
Criar backends com kubectl	148
TridentBackendConfig	148
Visão geral das etapas	150
Passo 1: criar um segredo do Kubernetes	150
Etapa 2: Criar o TridentBackendConfig CR	151
Etapa 3: Verificar o status do `TridentBackendConfig` CR	152
(Opcional) Passo 4: obtenha mais detalhes	153
Gerenciar backends	154
Gerencie os backends do Trident com kubectl	154
Gerencie os backends do Trident com tridentctl	155
Escolha um método de gerenciamento de backend do Trident	157

Configurar e gerenciar backends

Configure os backends do Trident

Um backend define a relação entre Trident e um sistema de storage. Ele informa ao Trident como se comunicar com esse sistema de storage e como o Trident deve provisionar volumes a partir dele.

Trident oferece automaticamente pools de armazenamento de backends que correspondem aos requisitos definidos por uma classe de armazenamento. Saiba como configurar o backend para o seu sistema de storage.

- ["Configurar um backend do Azure NetApp Files"](#)
- ["Configurar um backend do Google Cloud NetApp Volumes"](#)
- ["Configurar um NetApp HCI ou SolidFire backend"](#)
- ["Configure um backend com drivers NAS do ONTAP ou Cloud Volumes ONTAP"](#)
- ["Configure um backend com drivers SAN do ONTAP ou Cloud Volumes ONTAP"](#)
- ["Use Trident com Amazon FSx for NetApp ONTAP"](#)

Azure NetApp Files

Configurar um backend do Azure NetApp Files

Use o Azure NetApp Files como backend para Trident. Esse backend oferece suporte a volumes NFS e SMB. Trident oferece suporte a identidades gerenciadas e identidade de carga de trabalho para clusters do Azure Kubernetes Service (AKS).

Ambientes de nuvem Azure suportados

Trident oferece suporte a back-ends do Azure NetApp Files em vários ambientes de nuvem do Azure.

As nuvens do Microsoft Azure compatíveis incluem:

- Azure Commercial
- Azure Government (Azure Government / MAG)
- O Azure China

Ao implantar Trident ou configurar um backend do Azure NetApp Files, certifique-se de que o Azure Resource Manager e os endpoints de autenticação correspondam ao seu ambiente de nuvem do Azure.

Revise o suporte do driver do Azure NetApp Files

Trident fornece o seguinte driver de armazenamento Azure NetApp Files.

Os modos de acesso suportados incluem *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX) e *ReadWriteOncePod* (RWOP).

Driver	Protocolo	volumeMod e	Modos de acesso suportados	Sistemas de arquivos suportados
azure-netapp-files	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	nfs, smb

Revisar considerações

- Azure NetApp Files não suporta volumes menores que 50 GiB. Trident cria um volume de 50 GiB quando um volume menor é solicitado.
- Trident suporta volumes SMB montados em pods executados apenas em nós Windows.
- As implantações do Azure NetApp Files em nuvens Azure não comerciais exigem endpoints do Azure Resource Manager e de autenticação específicos da nuvem. Certifique-se de que Trident e qualquer configuração de backend usem os endpoints apropriados para o seu ambiente de nuvem Azure.

Use identidades gerenciadas para AKS

Trident oferece suporte ["identidades gerenciadas"](#) para clusters AKS.

Se você utiliza `tridentctl` para criar ou gerenciar back-ends do Azure NetApp Files, certifique-se de que ele esteja configurado para o ambiente de nuvem Azure correto.

Para usar identidades gerenciadas, você deve ter:

- Um cluster Kubernetes implantado usando AKS
- Identidades gerenciadas configuradas no cluster Kubernetes do AKS
- Trident instalado com `cloudProvider` definido para "Azure"

Operador Trident

Edite `tridentorchestrator_cr.yaml` e defina `cloudProvider` como "Azure".

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
```

Helm

O exemplo a seguir instala Trident e define `cloudProvider` usando a variável de ambiente `$CP`:

```
helm install trident trident-operator-100.2606.0.tgz --create-namespace
--namespace <trident-namespace> --set cloudProvider=$CP
```

`<code>tridentctl</code>`

O exemplo a seguir instala Trident e define o cloud-provider sinalizador para Azure:

```
tridentctl install --cloud-provider="Azure" -n trident
```

Use identidade de carga de trabalho para AKS

A identidade de carga de trabalho permite que os pods do Kubernetes acessem recursos do Azure autenticando-se como uma identidade de carga de trabalho.

Se você utiliza `tridentctl` para criar ou gerenciar back-ends do Azure NetApp Files, certifique-se de que ele esteja configurado para o ambiente de nuvem Azure correto.

Para usar workload identity, você precisa ter:

- Um cluster Kubernetes implantado usando AKS
- Identidade de carga de trabalho e oidc-issuer configurados no cluster Kubernetes do AKS
- Trident instalado com `cloudProvider` definido para "Azure" e `cloudIdentity` definido para o valor de identidade da carga de trabalho

Operador Trident

Edite `tridentorchestrator_cr.yaml` e defina `cloudProvider` como "Azure". Defina `cloudIdentity` como `azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
  cloudIdentity: 'azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx' # Edit
```

Helm

Defina os valores para os parâmetros **cloud-provider (CP)** e **cloud-identity (CI)** usando as seguintes variáveis de ambiente:

```
export CP="Azure"
export CI="'azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx'"
```

O exemplo a seguir instala Trident e define `cloudProvider` usando `$CP` e define `cloudIdentity` usando `$CI`:

```
helm install trident trident-operator-100.6.0.tgz --set  
cloudProvider=$CP --set cloudIdentity="$CI"
```

`tridentctl`

Defina os valores para os parâmetros **cloud provider** e **cloud identity** usando as seguintes variáveis de ambiente:

```
export CP="Azure"  
export CI="azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx"
```

O exemplo a seguir instala Trident e define `cloud-provider` como `$CP` e `cloud-identity` como `$CI`:

```
tridentctl install --cloud-provider=$CP --cloud-identity="$CI" -n  
trident
```

Prepare-se para configurar um backend do Azure NetApp Files

Antes de configurar seu backend do Azure NetApp Files, você precisa garantir que os seguintes requisitos sejam atendidos.

Ambientes de nuvem Azure suportados

Trident oferece suporte a back-ends do Azure NetApp Files em vários ambientes de nuvem do Azure.

As nuvens do Microsoft Azure compatíveis incluem:

- Azure Commercial
- Azure Government (Azure Government / MAG)
- O Azure China

Ao preparar seu ambiente, certifique-se de que sua assinatura do Azure, configuração de identidade e recursos do Azure NetApp Files sejam criados no ambiente de nuvem do Azure apropriado.

Pré-requisitos para volumes NFS e SMB

Se você estiver usando o Azure NetApp Files pela primeira vez ou em um novo local, será necessária alguma configuração inicial para configurar o Azure NetApp Files e criar um volume NFS. Consulte ["Azure: configure o Azure NetApp Files e crie um volume NFS"](#).

Para configurar e usar um ["Azure NetApp Files"](#) backend, você precisa do seguinte:



- `subscriptionID`, `tenantID`, `clientID`, `location` e `clientSecret` são opcionais ao

usar identidades gerenciadas em um cluster AKS.

- `tenantID`, `clientID`, e `clientSecret` são opcionais ao usar uma identidade de nuvem em um cluster AKS.
- As implantações do Azure NetApp Files em nuvens Azure não comerciais exigem endpoints do Azure Resource Manager e de autenticação específicos da nuvem. Certifique-se de que Trident e qualquer configuração de backend usem os endpoints apropriados para o seu ambiente de nuvem Azure.

- Um pool de capacidade. Consulte ["Microsoft: criar um pool de capacidade para Azure NetApp Files"](#).
- Uma sub-rede delegada ao Azure NetApp Files. Consulte ["Microsoft: delegar uma sub-rede ao Azure NetApp Files"](#).
- `subscriptionID` de uma assinatura do Azure com o Azure NetApp Files ativado.
- `tenantID`, `clientID`, e `clientSecret` de um ["Registro de aplicativo"](#) no Azure Active Directory com permissões suficientes para o serviço NetApp Files do Azure. O registro do aplicativo deve usar um dos seguintes:
 - O papel de Owner ou Contributor ["predefinido pelo Azure"](#).
 - Uma ["Função de Contributor personalizada"](#) no nível da assinatura (`assignableScopes` com as seguintes permissões, que são limitadas apenas ao que Trident exige. Após criar a função personalizada, ["atribua a função usando o portal do Azure"](#)).

▼ Função de colaborador personalizado

```
{
  "id": "/subscriptions/<subscription-id>/providers/Microsoft.Authorization/roleDefinitions/<role-definition-id>",
  "properties": {
    "roleName": "custom-role-with-limited-perms",
    "description": "custom role providing limited permissions",
    "assignableScopes": [
      "/subscriptions/<subscription-id>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.NetApp/netAppAccounts/capacityPools/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/write",

          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",

          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",

```

```

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/MountTargets/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/read",

"Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/write",

"Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/delete",
    "Microsoft.Features/features/read",
    "Microsoft.Features/operations/read",
    "Microsoft.Features/providers/features/read",
    "Microsoft.Features/providers/features/register/action",

"Microsoft.Features/providers/features/unregister/action",

"Microsoft.Features/subscriptionFeatureRegistrations/read"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
}
}

```

- O Azure location que contém pelo menos um ["sub-rede delegada"](#). A partir do Trident 22.01, o location parâmetro é um campo obrigatório no nível superior do arquivo de configuração do backend. Os valores de localização especificados em pools virtuais são ignorados.
- Para usar Cloud Identity, obtenha o client ID de um ["identidade gerenciada atribuída pelo usuário"](#) e especifique esse ID em azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx.

Requisitos adicionais para volumes SMB

Para criar um volume SMB, você deve ter:

- Active Directory configurado e conectado ao Azure NetApp Files. Consulte ["Microsoft: criar e gerenciar conexões do Active Directory para Azure NetApp Files"](#).
- Um cluster Kubernetes com um nó controlador Linux e pelo menos um nó de trabalho Windows executando Windows Server 2022. Trident suporta volumes SMB montados em pods executados apenas em nós Windows.
- Pelo menos um segredo do Trident contendo suas credenciais do Active Directory para que o Azure NetApp Files possa autenticar no Active Directory. Para gerar o segredo `smbcreds`:

```
kubectl create secret generic smbcreds --from-literal username=user  
--from-literal password='password'
```

- Um proxy CSI configurado como um serviço do Windows. Para configurar um `csi-proxy`, consulte ["GitHub: CSI Proxy"](#) ou ["GitHub: CSI Proxy para Windows"](#) para nós do Kubernetes em execução no Windows.

Opções e exemplos de configuração do backend do Azure NetApp Files

Saiba mais sobre as opções de configuração de back-end NFS e SMB para o Azure NetApp Files e veja exemplos de configuração.

Opções de configuração do backend

Trident usa sua configuração de back-end (sub-rede, rede virtual, nível de serviço e localização) para criar volumes do Azure NetApp Files em pools de capacidade disponíveis na localização solicitada e que correspondam ao nível de serviço e à sub-rede solicitados.

Os backends do Azure NetApp Files fornecem essas opções de configuração.

Parâmetro	Descrição	Padrão
<code>version</code>	Versão de configuração do backend.	Sempre 1
<code>storageDriverName</code>	Nome do driver de armazenamento	"azure-netapp-files"
<code>backendName</code>	Nome personalizado para o backend de armazenamento	Nome do driver + "_" + caracteres aleatórios
<code>subscriptionID</code>	O ID da assinatura da sua assinatura do Azure opcional quando as identidades gerenciadas estão habilitadas em um cluster do AKS.	

Parâmetro	Descrição	Padrão
tenantID	O ID do locatário de um registro de aplicativo opcional quando identidades gerenciadas ou identidade na nuvem são usadas em um cluster AKS.	
clientID	O ID do cliente de um registro de aplicativo é opcional quando identidades gerenciadas ou identidade na nuvem são usadas em um cluster AKS.	
clientSecret	O segredo do cliente de um registro de aplicativo. Opcional quando identidades gerenciadas ou identidade na nuvem são usadas em um cluster AKS.	
serviceLevel	Um de Standard, Premium ou Ultra	"" (aleatório)
location	Nome da localização do Azure onde os novos volumes serão criados Opcional quando as identidades gerenciadas estão habilitadas em um cluster AKS.	
cloudConfiguration.cloudName	Identifica o ambiente de nuvem do Azure para o backend. Defina como AzureGovernment ao usar o Azure Government.	
resourceGroups	Lista de grupos de recursos para filtrar recursos descobertos	[] (sem filtro)
netappAccounts	Lista de contas NetApp para filtrar recursos descobertos	[] (sem filtro)
capacityPools	Lista de pools de capacidade para filtrar recursos descobertos	[] (sem filtro, aleatório)
virtualNetwork	Nome de uma rede virtual com uma sub-rede delegada	""
subnet	Nome de uma sub-rede delegada a Microsoft.Netapp/volumes	""

Parâmetro	Descrição	Padrão
networkFeatures	Conjunto de recursos de VNet para um volume, pode ser Basic ou Standard. Network Features não está disponível em todas as regiões e pode precisar ser habilitado em uma assinatura. Especificar networkFeatures quando a funcionalidade não está habilitada faz com que o provisionamento do volume falhe.	""
nfsMountOptions	Controle preciso das opções de montagem NFS. Ignorado para volumes SMB. Para montar volumes usando a versão de NFS 4.1, inclua nfsvers=4 na lista de opções de montagem separadas por vírgula para escolher NFS v4.1. As opções de montagem definidas em uma definição de classe de armazenamento substituem as opções de montagem definidas na configuração do backend.	"nfsvers=3"
limitVolumeSize	Falhar no provisionamento se o tamanho do volume solicitado for superior a este valor	"" (não aplicado por padrão)
debugTraceFlags	Sinalizadores de depuração para usar na resolução de problemas. Exemplo, <code>\{"api": false, "method": true, "discovery": true\}</code> . Não use isso a menos que esteja solucionando problemas e precise de um despejo de log detalhado.	null
nasType	Configurar a criação de volumes NFS ou SMB. As opções são nfs, smb ou null. Definir como null define volumes NFS por padrão.	nfs
supportedTopologies	Representa uma lista de regiões e zonas suportadas por este backend. Para obter mais informações, consulte "Usar a topologia CSI" .	
qosType	Representa o tipo de QoS: automático ou manual.	Automático
maxThroughput	Define a taxa de transferência máxima permitida em MiB/s. Compatível apenas com pools de capacidade QoS manuais.	4 MiB/sec



Para mais informações sobre recursos de rede, consulte ["Configurar recursos de rede para um volume do Azure NetApp Files"](#).

Considere ambientes de nuvem Azure (26.06)

A partir da versão 26.06, Trident oferece suporte à criação e ao gerenciamento de back-ends do Azure NetApp Files em vários ambientes de nuvem do Azure.

As nuvens do Microsoft Azure compatíveis incluem:

- Azure Commercial
- Azure Government (Azure Government / MAG)
- O Azure China

Ao implantar Trident ou criar um backend do Azure NetApp Files, certifique-se de que os endpoints do Azure Resource Manager e de autenticação correspondam ao seu ambiente de nuvem do Azure. Se os endpoints não corresponderem, `tridentctl` não será possível autenticar e a criação do backend falhará.

Para um backend do Azure Government, defina `cloudConfiguration.cloudName` na configuração do backend:

```
cloudConfiguration:
  cloudName: AzureGovernment
```

Permissões e recursos necessários

Se você receber um erro "Nenhum pool de capacidade encontrado" ao criar um PVC, é provável que o registro do seu aplicativo não tenha as permissões e os recursos necessários (sub-rede, rede virtual, pool de capacidade) associados. Se o modo de depuração estiver habilitado, Trident registra os recursos do Azure descobertos quando o backend é criado. Verifique se uma função apropriada está sendo usada.

Os valores para `resourceGroups`, `netappAccounts`, `capacityPools`, `virtualNetwork` e `subnet` podem ser especificados usando nomes curtos ou totalmente qualificados. Nomes totalmente qualificados são recomendados na maioria das situações, pois nomes curtos podem corresponder a vários recursos com o mesmo nome.



Se a vNet estiver localizada em um grupo de recursos diferente da conta de armazenamento Azure NetApp Files (ANF), especifique o grupo de recursos para a rede virtual ao configurar a lista `resourceGroups` para o backend.

Os `resourceGroups`, `netappAccounts` e `capacityPools` valores são filtros que restringem o conjunto de recursos descobertos àqueles disponíveis para este backend de armazenamento e podem ser especificados em qualquer combinação. Os nomes totalmente qualificados seguem este formato:

Tipo	Formatar
Grupo de recursos	<resource group>
Conta do NetApp	<resource group>/<netapp account>
Pool de capacidade	<resource group>/<netapp account>/<capacity pool>

Tipo	Formatar
Rede virtual	<resource group>/<virtual network>
Sub-rede	<resource group>/<virtual network>/<subnet>

Provisionamento de volume

Você pode controlar o provisionamento de volumes padrão especificando as seguintes opções em uma seção especial do arquivo de configuração. Consulte [Exemplos de configurações](#) para obter detalhes.

Parâmetro	Descrição	Padrão
exportRule	Regras de exportação para novos volumes. exportRule deve ser uma lista separada por vírgulas de qualquer combinação de endereços IPv4 ou sub-redes IPv4 na notação CIDR. Ignorado para volumes SMB.	"0.0.0.0/0"
snapshotDir	Acesso ao .snapshot diretório	true, false (Definido explicitamente).
size	O tamanho padrão de novos volumes	"100G"
unixPermissions	As permissões unix de novos volumes (4 dígitos octais). Ignorado para volumes SMB.	"" (recurso em pré-visualização, requer inclusão na lista de permissões na assinatura)

Exemplos de configurações

Os exemplos a seguir mostram configurações básicas que deixam a maioria dos parâmetros com os valores padrão. Esta é a maneira mais fácil de definir um backend.

▼ Configuração mínima

Esta é a configuração mínima absoluta de backend. Com esta configuração, Trident descobre todas as suas NetApp contas, pools de capacidade e sub-redes delegadas ao Azure NetApp Files no local configurado e coloca novos volumes em um desses pools e sub-redes aleatoriamente. Como `nasType` foi omitido, o `nfs` padrão se aplica e o backend irá provisionar volumes NFS.

Essa configuração é ideal quando você está começando a usar o Azure NetApp Files e testando as funcionalidades, mas, na prática, você vai querer fornecer um escopo adicional para os volumes que você provisionar.

```
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
```

```
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
```

▼ Identidades gerenciadas para AKS

Esta configuração de backend omite subscriptionID, tenantID, clientID e clientSecret, que são opcionais ao usar identidades gerenciadas.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools:
    - resource-group-1/netapp-account-1/ultra-pool
  resourceGroups:
    - resource-group-1
  netappAccounts:
    - resource-group-1/netapp-account-1
  virtualNetwork: resource-group-1/eastus-prod-vnet
  subnet: resource-group-1/eastus-prod-vnet/eastus-anf-subnet
```

▼ Identidade na nuvem para AKS

Esta configuração de backend omite tenantID, clientID e clientSecret, que são opcionais ao usar uma identidade na nuvem.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools:
    - ultra-pool
  resourceGroups:
```

```

- aks-ami-eastus-rg
netappAccounts:
- smb-na
virtualNetwork: eastus-prod-vnet
subnet: eastus-anf-subnet
location: eastus
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451

```

▼ Configuração específica de nível de serviço com filtros de pool de capacidade

Essa configuração de backend coloca volumes na localização do Azure eastus em um Ultra pool de capacidade. Trident descobre automaticamente todas as sub-redes delegadas ao Azure NetApp Files nesse local e coloca um novo volume em uma delas aleatoriamente.

```

---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2

```

▼ Exemplo de backend com pools de capacidade QoS manuais

Essa configuração de backend coloca volumes na localização do Azure eastus com pools de capacidade de QoS manuais.

```

---
version: 1
storageDriverName: azure-netapp-files
backendName: anf1
location: eastus
labels:
  clusterName: test-cluster-1
  cloud: anf
  nasType: nfs
defaults:
  qosType: Manual
storage:
- serviceLevel: Ultra
  labels:
    performance: gold

```

```

defaults:
  maxThroughput: 10
- serviceLevel: Premium
  labels:
    performance: silver
  defaults:
    maxThroughput: 5
- serviceLevel: Standard
  labels:
    performance: bronze
  defaults:
    maxThroughput: 3

```

▼ Configuração avançada

Essa configuração de backend reduz ainda mais o escopo do posicionamento de volumes para uma única sub-rede e também modifica alguns padrões de provisionamento de volumes.

```

---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
  - application-group-1/account-1/ultra-1
  - application-group-1/account-1/ultra-2
virtualNetwork: application-group-1/eastus-prod-vnet
subnet: application-group-1/eastus-prod-vnet/my-subnet
networkFeatures: Standard
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 500Gi
defaults:
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  snapshotDir: "true"
  size: 200Gi
  unixPermissions: "0777"

```

▼ Configuração de pool virtual

Esta configuração de backend define vários pools de armazenamento em um único arquivo. Isso é útil quando você tem vários pools de capacidade que suportam diferentes níveis de serviço e deseja criar classes de armazenamento no Kubernetes que os representem. Rótulos de pool virtual foram usados para diferenciar os pools com base em performance.

```

---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
resourceGroups:
  - application-group-1
networkFeatures: Basic
nfsMountOptions: vers=3,proto=tcp,timeo=600
labels:
  cloud: azure
storage:
  - labels:
      performance: gold
      serviceLevel: Ultra
      capacityPools:
        - application-group-1/netapp-account-1/ultra-1
        - application-group-1/netapp-account-1/ultra-2
      networkFeatures: Standard
  - labels:
      performance: silver
      serviceLevel: Premium
      capacityPools:
        - application-group-1/netapp-account-1/premium-1
  - labels:
      performance: bronze
      serviceLevel: Standard
      capacityPools:
        - application-group-1/netapp-account-1/standard-1
        - application-group-1/netapp-account-1/standard-2

```

▼ Configuração de topologias suportadas

Trident facilita o provisionamento de volumes para cargas de trabalho com base em regiões e zonas de disponibilidade. O `supportedTopologies` bloco nesta configuração de backend é usado para fornecer uma lista de regiões e zonas por backend. Os valores de região e zona especificados aqui devem corresponder aos valores de região e zona dos rótulos em cada nó de cluster Kubernetes. Essas regiões e zonas representam a lista de valores permitidos que podem ser fornecidos em uma classe de armazenamento. Para classes de armazenamento que contêm um subconjunto das regiões e zonas fornecidas em um backend, Trident cria volumes na região e zona mencionadas. Para obter mais informações, consulte ["Usar a topologia CSI"](#).

```
---
```

```

version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
  - application-group-1/account-1/ultra-1
  - application-group-1/account-1/ultra-2
supportedTopologies:
  - topology.kubernetes.io/region: eastus
    topology.kubernetes.io/zone: eastus-1
  - topology.kubernetes.io/region: eastus
    topology.kubernetes.io/zone: eastus-2

```

Definições de classe de armazenamento

As seguintes `StorageClass` definições referem-se aos pools de armazenamento acima.

Exemplo de definições usando `parameter.selector` field

Usando `parameter.selector` você pode especificar para cada `StorageClass` o pool virtual que é usado para hospedar um volume. O volume terá os aspectos definidos no pool escolhido.

```

---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gold
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=gold
allowVolumeExpansion: true

---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: silver
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=silver
allowVolumeExpansion: true

```

```

---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: bronze
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=bronze
allowVolumeExpansion: true

```

Exemplos de definições para volumes SMB

Usando `nasType`, `node-stage-secret-name` e `node-stage-secret-namespace`, você pode especificar um volume SMB e fornecer as credenciais necessárias do Active Directory.

▼ Configuração básica no namespace padrão

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"

```

▼ Usando segredos diferentes por namespace

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}

```

▼ Utilizando segredos diferentes em cada volume

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:

```

```
name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: ${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```



nasType: smb`Filtros para pools que suportam volumes SMB.
`nasType: nfs ou `nasType: null`filtros para pools NFS.

Criar o backend

Após criar o arquivo de configuração de backend, execute o seguinte comando:

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

Se você usa uma nuvem Azure não comercial, certifique-se de que `tridentctl` está configurado para usar o Azure Resource Manager e os endpoints de autenticação para o seu ambiente de nuvem Azure. Se a criação do backend falhar, verifique a configuração do backend e visualize os logs para determinar a causa:

```
tridentctl logs
```

Após identificar e corrigir o problema com o arquivo de configuração, você pode executar o comando `create` novamente.

Google Cloud NetApp Volumes

Configurar Google Cloud NetApp Volumes

Você pode configurar o Google Cloud NetApp Volumes como um backend para Trident a fim de provisionar storage para cargas de trabalho do Kubernetes.

Visão geral

Trident oferece suporte ao Google Cloud NetApp Volumes para cargas de trabalho NAS (NFS e SMB) e em bloco (iSCSI).

- As cargas de trabalho NAS usam o `google-cloud-netapp-volumes` backend
- As cargas de trabalho em bloco (iSCSI) usam o ``google-cloud-netapp-volumes-san`` backend

Os volumes NAS fornecem armazenamento baseado em arquivos e são acessados usando os protocolos NFS ou SMB. Esses volumes suportam acesso compartilhado entre vários pods ou nós.

Os volumes de bloco fornecem armazenamento bruto em bloco e são acessados como dispositivos iSCSI conectados a nós do Kubernetes. Esses volumes são usados quando os aplicativos exigem acesso em nível

de bloco.

Isso se aplica aos seguintes ambientes:

- Trident 26.02 e posteriores
- Google Kubernetes Engine (GKE) ou Red Hat OpenShift
- Pools de armazenamento do Google Cloud NetApp Volumes

Para configurar o armazenamento em bloco (iSCSI), consulte ["Configurar armazenamento em bloco \(iSCSI\)"](#).

Prepare-se para configurar

A identidade na nuvem permite que as cargas de trabalho do Kubernetes acessem recursos do Google Cloud autenticando-se como uma identidade de carga de trabalho em vez de usar credenciais estáticas.

Para usar a identidade na nuvem com Google Cloud NetApp Volumes, você deve ter:

- Um cluster Kubernetes implantado usando Google Kubernetes Engine (GKE)
- Identidade de carga de trabalho habilitada no cluster GKE e o servidor de metadados habilitado nos pools de nós
- Uma conta de serviço do Google Cloud com a função de Administrador do Google Cloud NetApp Volumes (`roles/netapp.admin`) ou uma função personalizada equivalente
- Trident instalado com o provedor de nuvem definido como GCP e a anotação de identidade da nuvem configurada

Operador Trident

Para instalar o Trident usando o operador Trident, edite `tridentorchestrator_cr.yaml`:

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  namespace: trident
  cloudProvider: "GCP"
  cloudIdentity: "iam.gke.io/gcp-service-account: cloudvolumes-admin-
sa@mygcpproject.iam.gserviceaccount.com"
```

Helm

Defina o provedor de nuvem e a identidade da nuvem ao instalar o Trident com o Helm:

```
helm install trident trident-operator-100.6.0.tgz \
  --set cloudProvider=GCP \
  --set cloudIdentity="iam.gke.io/gcp-service-account: cloudvolumes-
admin-sa@mygcpproject.iam.gserviceaccount.com"
```

tridentctl

Instale Trident especificando o provedor de nuvem e a identidade de nuvem:

```
tridentctl install \
  --cloud-provider=GCP \
  --cloud-identity="iam.gke.io/gcp-service-account: cloudvolumes-admin-
sa@mygcpproject.iam.gserviceaccount.com" \
  -n trident
```

Configurar armazenamento NAS



Para pools de armazenamento UNIFIED do Google Cloud NetApp Volumes, Trident aplica regras de nomenclatura e validação específicas do UNIFIED durante as operações de volume.

Ao localizar um volume, Trident pode avaliar várias variantes de nomes de volume compatíveis (por exemplo, formatos com hífen e sublinhado) para melhorar a confiabilidade da importação e da descoberta.

Detalhes do driver

Trident fornece o `google-cloud-netapp-volumes` driver para provisionar armazenamento NAS a partir do Google Cloud NetApp Volumes.

O driver suporta os seguintes modos de acesso:

- ReadWriteOnce (RWO)
- ReadOnlyMany (ROX)
- ReadWriteMany (RWX)
- ReadWriteOncePod (RWOP)

Driver	Protocolo	volumeMod e	Modos de acesso suportados	Sistemas de arquivos suportados
google-cloud-netapp-volumes	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	nfs, smb

Configurar um backend NAS do Trident

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: gcnv-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: "<project-number>"
```

```
location: "<region>"
sdkTimeout: "600"
storage:
- labels:
    cloud: gcp
    network: "<vpc-network>"
```

Provisionar volumes NAS

Os volumes NAS são provisionados usando o `google-cloud-netapp-volumes` backend e suportam os protocolos NFS e SMB.

StorageClass for volumes NFS

Para provisionar volumes NFS, defina `nasType` para `nfs`.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

StorageClass for volumes SMB

Para provisionar volumes SMB, defina `nasType` para `smb` e forneça as credenciais.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
allowVolumeExpansion: true
```

Exemplo de PersistentVolumeClaim (RWX)

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: gcnv-nas-rwx
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-nfs

```

Exemplo de PersistentVolumeClaim (RWO)

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: gcnv-nas-rwo
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-nfs

```



Volumes NAS usam `volumeMode: Filesystem`.

Configurar o Google Cloud NetApp Volumes para cargas de trabalho SAN

Você pode configurar Trident para provisionar volumes de armazenamento em bloco usando o protocolo iSCSI do Google Cloud NetApp Volumes. Os volumes SAN são provisionados a partir de pools de armazenamento Flex Unified usando o `google-cloud-netapp-volumes-san` driver de armazenamento.



Este driver é dedicado a cargas de trabalho em bloco e não oferece suporte a protocolos NAS.



O ``google-cloud-netapp-volumes-san`backend` é necessário para provisionar volumes de bloco iSCSI. O ``google-cloud-netapp-volumes`backend` suporta apenas protocolos NAS e não pode ser usado para cargas de trabalho SAN.

Visão geral

Trident oferece suporte ao Google Cloud NetApp Volumes SAN (iSCSI) para cargas de trabalho usando o driver `google-cloud-netapp-volumes-san`.

Os volumes SAN são provisionados a partir de pools de armazenamento Flex Unified e apresentados aos nós do Kubernetes como dispositivos de bloco iSCSI.

Isso se aplica aos seguintes ambientes:

- Trident 26.02 e posteriores
- Google Kubernetes Engine (GKE) ou Red Hat OpenShift
- Pools de storage unificado do Google Cloud NetApp Volumes Flex
- Cargas de trabalho baseadas em iSCSI

Pools de storage unificado Flex

Os pools de armazenamento Flex Unified fornecem armazenamento em bloco usando o protocolo iSCSI e são necessários para o provisionamento de SAN:

- Os pools regionais Flex Unified são suportados.
- Os pools Zonais unificados Flex são suportados a partir do Trident 26.02.1.
- Apenas o nível de serviço **Flex** é compatível com cargas de trabalho SAN.

Configurar um backend SAN do Trident

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: gcnv-san
  namespace: trident
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes-san
  projectNumber: "<project-number>"
  location: "<region>"
  sdkTimeout: "600"
  storage:
    - labels:
        cloud: gcp
        performance: flex
        network: "<vpc-network>"
        serviceLevel: Flex
```

Crie um StorageClass

Após configurar o backend SAN, crie um StorageClass que faça referência ao `google-cloud-netapp-`

volumes-san driver.

O tipo de sistema de arquivos é definido no StorageClass, não no backend.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-san
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes-san"
  fsType: "ext4"
allowVolumeExpansion: true
```

Tipos de sistemas de arquivos suportados:

- ext4 (padrão)
- ext3
- xfs



O driver SAN suporta apenas o nível de serviço Flex e não utiliza parâmetros de backend específicos do NAS, como `exportRule`, `unixPermissions`, `nasType`, `snapshotDir`, `nfsMountOptions` ou configurações relacionadas ao tiering.

Provisionar volumes de bloco

ReadWriteOnce (RWO)

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: gcnv-san-rwo
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-san
```

ReadWriteOncePod (RWOP)

```
apiVersion: v1
kind: PersistentVolumeClaim
```

```

metadata:
  name: gcnv-san-rwop
spec:
  accessModes:
    - ReadWriteOncePod
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-san

```

ReadOnlyMany (ROX)

Um padrão comum para o ROX é clonar um volume ReadWriteOnce existente e montar o clone como somente leitura.

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: gcnv-san-rox
spec:
  accessModes:
    - ReadOnlyMany
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-san
  dataSource:
    kind: PersistentVolumeClaim
    name: gcnv-san-rwo

```

ReadWriteMany (RWX) — somente bloco bruto

ReadWriteMany é suportado somente quando `volumeMode: Block`.

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: gcnv-san-raw-rwx
spec:
  accessModes:
    - ReadWriteMany
  volumeMode: Block
  resources:
    requests:
      storage: 100Gi

```

```
storageClassName: gcnv-san
```

Comportamento do volume do bloco

Os volumes de bloco são provisionados como LUNs iSCSI e apresentados aos nós do Kubernetes como dispositivos de bloco.

Volumes de bloco:

- Use o protocolo iSCSI
- Suporte ao sistema de arquivos e apresentação de blocos brutos
- Estão anexados e gerenciados pela Trident
- Suporte a múltiplos modos de acesso do Kubernetes

Modos de acesso

Os volumes de bloco provisionados pelo Trident suportam os seguintes modos de acesso:

- `ReadWriteOnce` (RWO)
- `ReadOnlyMany` (ROX)
- `ReadWriteOncePod` (RWOP)
- `ReadWriteMany` (RWX), suportado somente quando `volumeMode: Block`

Comportamento do volumeMode

O `volumeMode` campo controla como um volume de bloco é exposto:

- `Filesystem` Trident formata e monta o volume.
- `Block` Trident conecta o dispositivo e o expõe como um dispositivo de bloco raw.

Operações suportadas

Volumes de bloco provisionados usando o driver `google-cloud-netapp-volumes-san` oferecem suporte a:

- Criar
- Excluir
- Clonar
- Snapshot
- Redimensionar
- Importar

Comportamento de sobreprovisionamento de GiB extra

Os volumes em bloco do Google Cloud NetApp Volumes incluem sobrecarga de metadados internos. Essa sobrecarga reduz o tamanho do dispositivo visível para o kernel em comparação com a capacidade provisionada.

Os testes mostram:

- Aproximadamente 300 KiB de sobrecarga na criação inicial
- Até aproximadamente 107 MiB de overhead após um redimensionamento

Como o Google Cloud NetApp Volumes aceita apenas alocações de GiB inteiros, Trident garante que o tamanho utilizável do dispositivo sempre atenda ou exceda a solicitação do PVC por:

- Arredondando o tamanho solicitado para o próximo GiB inteiro
- Adicionando um buffer adicional de 1 GiB

Exemplo:

- Pedido de PVC: 100 GiB
- Tamanho provisionado no Google Cloud NetApp Volumes: 101 GiB
- Espaço utilizável visível para a aplicação: pelo menos 100 GiB

Exemplos de pods

Volume de bloco montado no sistema de arquivos (RWO)

```
apiVersion: v1
kind: Pod
metadata:
  name: app-rwo
spec:
  containers:
  - name: app
    image: ubuntu:22.04
    command: ["sleep", "infinity"]
    volumeMounts:
    - name: data
      mountPath: /mnt/data
  volumes:
  - name: data
    persistentVolumeClaim:
      claimName: gcnv-san-rwo
```

Dispositivo de bloco bruto (RWX)

```
apiVersion: v1
kind: Pod
metadata:
  name: app-raw-rwx
spec:
  containers:
```

```

- name: app
  image: ubuntu:22.04
  command: ["sleep", "infinity"]
  volumeDevices:
  - name: data
    devicePath: /dev/xda
volumes:
- name: data
  persistentVolumeClaim:
    claimName: gcnv-san-raw-rwx

```

Comportamento de attach e montagem

Para volumes SAN provisionados a partir do Google Cloud NetApp Volumes:

- Trident cria um Número de Unidade Lógica (LUN) em um pool de storage Flex Unified.
- Durante a publicação, Trident mapeia o LUN para um grupo de hosts por nó.
- Durante o preparo do nó, Trident:
 - Faz login no destino iSCSI
 - Descobre o LUN
 - Configura multipath
- Se `volumeMode: Filesystem`, o Trident formata o dispositivo, se necessário, e o monta.
- Se `volumeMode: Block` Trident anexar o dispositivo e expô-lo diretamente ao pod sem formatar ou montar.



Os volumes de bloco SAN não oferecem bloqueio distribuído nem coordenação de gravação. Quando um volume de bloco é acessado por vários nós (ReadWriteMany com `volumeMode: Block`), o aplicativo ou o sistema de arquivos deve gerenciar a concorrência.

Prepare-se para configurar um backend do Google Cloud NetApp Volumes

Antes de configurar seu backend do Google Cloud NetApp Volumes, você precisa garantir que os seguintes requisitos sejam atendidos.

Pré-requisitos para volumes NFS ou SMB

Se você estiver usando o Google Cloud NetApp Volumes pela primeira vez ou em um novo local, será necessária alguma configuração inicial para configurar o Google Cloud NetApp Volumes e criar um volume NFS ou SMB. Consulte ["Antes de começar"](#).

Certifique-se de ter o seguinte antes de configurar o backend do Google Cloud NetApp Volumes:

- Uma conta do Google Cloud configurada com o serviço Google Cloud NetApp Volumes. Consulte ["Google Cloud NetApp Volumes"](#).
- Número do projeto da sua conta do Google Cloud. Consulte ["Identificação de projetos"](#).
- Uma conta de serviço do Google Cloud com a função de NetApp Volumes Admin (

`roles/netapp.admin`. Consulte ["Funções e permissões de Identity and Access Management"](#).

- Arquivo de chave API para sua conta GCNV. Consulte ["Criar uma chave de conta de serviço"](#)
- Um pool de storage. Consulte ["Visão geral dos storage pools"](#).

Para obter mais informações sobre como configurar o acesso ao Google Cloud NetApp Volumes, consulte ["Configure o acesso ao Google Cloud NetApp Volumes"](#).

Opções e exemplos de configuração do backend do Google Cloud NetApp Volumes

Saiba mais sobre as opções de configuração de back-end para Google Cloud NetApp Volumes e veja exemplos de configuração.

Opções de configuração do backend

Cada backend provisiona volumes em uma única região do Google Cloud. Para criar volumes em outras regiões, você pode definir backends adicionais.

Parâmetro	Descrição	Padrão
<code>version</code>		Sempre 1
<code>storageDriverName</code>	Nome do driver de armazenamento	O valor de <code>storageDriverName</code> deve ser especificado como "google-cloud-netapp-volumes".
<code>backendName</code>	(Opcional) Nome personalizado do storage backend	Nome do driver + "_" + parte da chave da API
<code>storagePools</code>	Parâmetro opcional usado para especificar pools de storage para criação de volumes.	
<code>projectNumber</code>	Número do projeto da conta do Google Cloud. O valor é encontrado na página inicial do portal do Google Cloud.	
<code>location</code>	O local do Google Cloud onde Trident cria volumes GCNV. Ao criar clusters Kubernetes entre regiões, volumes criados em um <code>location</code> podem ser usados em cargas de trabalho agendadas em nós em várias regiões do Google Cloud. O tráfego entre regiões gera um custo adicional.	

Parâmetro	Descrição	Padrão
apiKey	Chave de API para a conta de serviço do Google Cloud com a <code>netapp.admin</code> função. Inclui o conteúdo formatado em JSON do arquivo de chave privada de uma conta de serviço do Google Cloud (copiado integralmente para o arquivo de configuração do backend). O <code>apiKey</code> deve incluir pares de chave-valor para as seguintes chaves: <code>type</code> , <code>project_id</code> , <code>client_email</code> , <code>client_id</code> , <code>auth_uri</code> , <code>token_uri</code> , <code>auth_provider_x509_cert_url</code> e <code>client_x509_cert_url</code> .	
nfsMountOptions	Controle preciso das opções de montagem NFS.	"nfsvers=3"
limitVolumeSize	Falhe no provisionamento se o tamanho do volume solicitado for superior a esse valor.	"" (não aplicado por padrão)
serviceLevel	O nível de serviço de um pool de storage e seus volumes. Os valores são <code>flex</code> , <code>standard</code> , <code>premium</code> , ou <code>extreme</code> .	
labels	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes	""
network	Rede Google Cloud usada para volumes GCNV.	
debugTraceFlags	Sinalizadores de depuração para usar na resolução de problemas. Exemplo, <code>{"api": false, "method": true}</code> . Não use isso a menos que esteja solucionando problemas e precise de um despejo de log detalhado.	null
nasType	Configurar a criação de volumes NFS ou SMB. As opções são <code>nfs</code> , <code>smb</code> ou <code>null</code> . Definir como <code>null</code> define volumes NFS por padrão.	nfs
supportedTopologies	Representa uma lista de regiões e zonas suportadas por este backend. Para obter mais informações, consulte " Usar a topologia CSI ". Por exemplo: supportedTopologies: - topology.kubernetes.io/region: asia-east1 topology.kubernetes.io/zone: asia-east1-a	

Opções de provisionamento de volume

Você pode controlar o provisionamento de volume padrão na seção `defaults` do arquivo de configuração.

Parâmetro	Descrição	Padrão
exportRule	As regras de exportação para novos volumes. Deve ser uma lista separada por vírgulas de qualquer combinação de endereços IPv4.	"0.0.0.0/0"

Parâmetro	Descrição	Padrão
snapshotDir	Acesso ao .snapshot diretório	true, false (o comportamento padrão pode variar. Defina explicitamente) "false" para NFSv3
snapshotReserve	Percentual do volume reservado para snapshots	"" (aceitar padrão de 0)
unixPermissions	As permissões unix de novos volumes (4 dígitos octais).	""

Exemplos de configurações

Os exemplos a seguir mostram configurações básicas que deixam a maioria dos parâmetros com os valores padrão. Esta é a maneira mais fácil de definir um backend.

▼ Configuração mínima

Esta é a configuração mínima absoluta de backend. Com esta configuração, Trident descobre todos os seus pools de storage delegados ao Google Cloud NetApp Volumes no local configurado e coloca novos volumes em um desses pools aleatoriamente. Como `nasType` foi omitido, o `nfs` padrão se aplica e o backend irá provisionar volumes NFS.

Essa configuração é ideal para quem está começando a usar o Google Cloud NetApp Volumes e testando seus recursos, mas na prática pode ser necessário definir um escopo adicional para os volumes provisionados.



Substitua `<id_value>` e `<key_value>` pelas credenciais da sua conta de serviço.

```

---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: "123455380079"

```

```

location: europe-west6
serviceLevel: premium
apiKey:
  type: service_account
  project_id: my-gcnv-project
  client_email: myproject-prod@my-gcnv-project.iam.gserviceaccount.com
  client_id: "103346282737811234567"
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
credentials:
  name: backend-tbc-gcnv-secret

```

▼ Configuração para volumes SMB

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv1
  namespace: trident
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: "123456789"
  location: asia-east1
  serviceLevel: flex
  nasType: smb
  apiKey:
    type: service_account
    project_id: cloud-native-data
    client_email: trident-sample@cloud-native-
data.iam.gserviceaccount.com
    client_id: "123456789737813416734"
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
    client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/trident-
sample%40cloud-native-data.iam.gserviceaccount.com
  credentials:

```

```
name: backend-tbc-gcnv-secret
```

▼ Configuração com filtro StoragePools

```
---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
---

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: "123455380079"
  location: europe-west6
  serviceLevel: premium
  storagePools:
    - premium-pool1-europe-west6
    - premium-pool2-europe-west6
  apiKey:
    type: service_account
    project_id: my-gcnv-project
    client_email: myproject-prod@my-gcnv-project.iam.gserviceaccount.com
    client_id: "103346282737811234567"
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
    client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
  credentials:
```

```
name: backend-tbc-gcnv-secret
```

▼ Configuração de pool virtual

Esta configuração de backend define vários pools virtuais em um único arquivo. Os pools virtuais são definidos na `storage` seção. Eles são úteis quando você tem vários pools de storage suportando diferentes níveis de serviço e deseja criar classes de storage no Kubernetes que os representem. Os rótulos dos pools virtuais são usados para diferenciá-los. Por exemplo, no exemplo abaixo `performance` label e `serviceLevel` type são usados para diferenciar os pools virtuais.

Você também pode definir alguns valores padrão que serão aplicáveis a todos os pools virtuais e sobrescrever os valores padrão para pools virtuais individuais. No exemplo a seguir, `snapshotReserve` e `exportRule` servem como padrões para todos os pools virtuais.

Para obter mais informações, consulte ["Pools virtuais"](#).

```
---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: "123455380079"
  location: europe-west6
  apiKey:
    type: service_account
    project_id: my-gcnv-project
    client_email: myproject-prod@my-gcnv-project.iam.gserviceaccount.com
    client_id: "103346282737811234567"
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
      https://www.googleapis.com/oauth2/v1/certs
```

```

client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
credentials:
  name: backend-tbc-gcnv-secret
defaults:
  snapshotReserve: "10"
  exportRule: 10.0.0.0/24
storage:
- labels:
  performance: extreme
  serviceLevel: extreme
  defaults:
    snapshotReserve: "5"
    exportRule: 0.0.0.0/0
- labels:
  performance: premium
  serviceLevel: premium
- labels:
  performance: standard
  serviceLevel: standard

```

▼ Identidade na nuvem para GKE

Ao instalar Trident com uma identidade de nuvem do GKE, os backends autenticam-se como uma identidade de carga de trabalho e omitem o `apiKey` bloco. A identidade de nuvem é configurada da mesma forma para ambos os drivers do Google Cloud NetApp Volumes. A única diferença é o `storageDriverName` valor: use `google-cloud-netapp-volumes` para volumes NAS (NFS ou SMB) e `google-cloud-netapp-volumes-san` para volumes SAN (iSCSI block).



O suporte à identidade na nuvem para o `google-cloud-netapp-volumes-san` driver requer Trident 26.06 ou posterior. Os volumes SAN são provisionados a partir de pools de storage Flex Unified, então defina `serviceLevel` como `flex`.

Driver NAS (`google-cloud-netapp-volumes`)

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcp-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: '012345678901'
  network: gcnv-network
  location: us-west2
  serviceLevel: Premium

```

```
storagePool: pool-premium1
```

Driver SAN (<code>google-cloud-netapp-volumes-san</code>)

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcp-gcnv-san
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes-san
  projectNumber: '012345678901'
  network: gcnv-network
  location: us-west2
  serviceLevel: flex
  storagePool: pool-flex1
```

▼ Configuração de topologias suportadas

Trident facilita o provisionamento de volumes para cargas de trabalho com base em regiões e zonas de disponibilidade. O `supportedTopologies` bloco nesta configuração de backend é usado para fornecer uma lista de regiões e zonas por backend. Os valores de região e zona especificados aqui devem corresponder aos valores de região e zona dos rótulos em cada nó de cluster Kubernetes. Essas regiões e zonas representam a lista de valores permitidos que podem ser fornecidos em uma classe de armazenamento. Para classes de armazenamento que contêm um subconjunto das regiões e zonas fornecidas em um backend, Trident cria volumes na região e zona mencionadas. Para obter mais informações, consulte "[Usar a topologia CSI](#)".

```
---
version: 1
storageDriverName: google-cloud-netapp-volumes
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: asia-east1
serviceLevel: flex
supportedTopologies:
  - topology.kubernetes.io/region: asia-east1
    topology.kubernetes.io/zone: asia-east1-a
  - topology.kubernetes.io/region: asia-east1
    topology.kubernetes.io/zone: asia-east1-b
```

Qual é o próximo passo?

Após criar o arquivo de configuração de backend, execute o seguinte comando:

```
kubectl create -f <backend-file>
```

Para verificar se o backend foi criado com sucesso, execute o seguinte comando:

```
kubectl get tridentbackendconfig
```

NAME	BACKEND NAME	BACKEND UUID
PHASE	STATUS	
backend-tbc-gcnv	backend-tbc-gcnv	b2fd1ff9-b234-477e-88fd-713913294f65
Bound	Success	

Se a criação do backend falhar, há algo errado com a configuração do backend. Você pode descrever o backend usando o `kubectl get tridentbackendconfig <backend-name>` comando ou visualizar os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs
```

Após identificar e corrigir o problema com o arquivo de configuração, você pode excluir o backend e executar o comando create novamente.

Definições de classe de armazenamento

A seguir está uma definição básica `StorageClass` que se refere ao backend acima.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-nfs-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
```

Exemplo de definições usando o `parameter.selector` campo:

Usando `parameter.selector` você pode especificar para cada `StorageClass` o "pool virtual" que é usado para hospedar um volume. O volume terá os aspectos definidos no pool escolhido.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: extreme-sc
provisioner: csi.trident.netapp.io
parameters:
```

```

selector: performance=extreme
backendType: google-cloud-netapp-volumes

---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: premium-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=premium
  backendType: google-cloud-netapp-volumes

---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: standard-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=standard
  backendType: google-cloud-netapp-volumes

```

Para mais detalhes sobre classes de armazenamento, consulte ["Crie uma storage class"](#).

Exemplos de definições para volumes SMB

Usando `nasType`, `node-stage-secret-name` e `node-stage-secret-namespace`, você pode especificar um volume SMB e fornecer as credenciais necessárias do Active Directory. Qualquer usuário/senha do Active Directory com qualquer/nenhuma permissão pode ser usado para o segredo do estágio do nó.

▼ Configuração básica no namespace padrão

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"

```

▼ Usando segredos diferentes por namespace

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}

```

▼ Utilizando segredos diferentes em cada volume

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: ${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}

```



nasType: smb`Filtros para pools que suportam volumes SMB. `nasType: nfs ou `nasType: null`filtros para pools NFS.

Exemplo de definição de PVC

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: gcnv-nfs-pvc
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-nfs-sc

```

Para verificar se o PVC está vinculado, execute o seguinte comando:

```
kubectl get pvc gcnv-nfs-pvc
```

NAME	STATUS	VOLUME	CAPACITY
gcnv-nfs-pvc	Bound	pvc-b00f2414-e229-40e6-9b16-ee03eb79a213	100Gi
ACCESS MODES	STORAGECLASS	AGE	
RWX	gcnv-nfs-sc	1m	

Configurar o auto-tiering para Google Cloud NetApp Volumes

O auto-tiering é configurado por meio dos parâmetros do backend do Trident e das anotações `PersistentVolumeClaim` durante o provisionamento de volumes. Você pode configurar o auto-tiering para Google Cloud NetApp Volumes usando Trident.

Visão geral

O recurso de tiering automático permite que o Trident provisione volumes que movem automaticamente dados inativos de uma camada de desempenho para uma camada de capacidade. Isso reduz o custo de armazenamento enquanto preserva o desempenho para dados acessados com frequência.

Trident aplica as configurações de armazenamento em camadas automático somente no momento da criação do volume. Alterações posteriores ao provisionamento não são suportadas em Trident 26.06.

Conceitos

Tiering automático

O auto-tiering move dados acessados com pouca frequência de uma camada de desempenho para uma camada de capacidade com base em padrões de acesso. A movimentação de dados ocorre de forma assíncrona e não é imediata.

Política de tiering

A política de tiering determina se o auto-tiering está habilitado para um volume.

As seguintes políticas são suportadas: * `auto`: ativa o tiering automático com base em padrões de acesso * `none`: desativa o tiering automático

Dias de resfriamento

Os dias de resfriamento especificam o número mínimo de dias que um bloco de dados deve permanecer inativo antes de se tornar elegível para o armazenamento em camadas. Os dias de resfriamento se aplicam somente quando a política de armazenamento em camadas está definida como `auto`.

Modelo de configuração

Escopos de configuração

O auto-tiering pode ser configurado em vários escopos:

- **Escopo do pool de armazenamento** Aplica-se a todos os volumes provisionados do pool.

- **Escopo do volume** Aplica-se a um único volume por meio de anotações PersistentVolumeClaim.

Trident determina a configuração efetiva com base em onde cada configuração está definida.

Precedência de configuração

Quando a mesma configuração é definida em vários escopos, Trident aplica a seguinte ordem de precedência:

1. Anotações de PersistentVolumeClaim
2. Configuração do backend Trident
3. Padrões do pool de armazenamento

As configurações definidas em uma precedência mais alta substituem os valores de nível inferior.

Funcionalidade suportada no Trident 26.06

Trident 26.06 oferece suporte aos seguintes recursos de auto-tiering para Google Cloud NetApp Volumes:

- Habilitar ou desabilitar o auto-tiering durante o provisionamento de volumes
- Definindo uma política de hierarquização na configuração do backend do Trident
- Substituindo a política de escalonamento e os dias de resfriamento por volume usando anotações de PVC
- Configurando dias de resfriamento para volumes com auto-tiering ativado

Funcionalidade não suportada no Trident 26.06

As seguintes operações não são suportadas:

- Modificando as configurações de auto-tiering após a criação do volume
- Alterando políticas de camadas em volumes existentes usando atualizações do Kubernetes
- Aplicando configurações de armazenamento em camadas automático fora dos fluxos de trabalho de provisionamento gerenciados pelo Trident

Parâmetros de configuração do backend

Os seguintes parâmetros controlam o comportamento de auto-tiering quando definidos na configuração do backend Trident:

Parâmetro	Obrigatório	Descrição
tieringPolicy	Não	Política de escalonamento para volumes (auto ou none)
tieringMinimumCoolingDays	Não	Número de dias de inatividade antes dos dados serem transferidos de camada (intervalo: 2–183, padrão: 31)

Substituições em nível de volume usando PersistentVolumeClaim anotações

Anotações suportadas

PersistentVolumeClaim anotações permitem a substituição das configurações de auto-tiering por volume.

Anotação	Descrição
trident.netapp.io/tieringPolicy	Substitui a política de hierarquização para o volume
trident.netapp.io/tieringMinimumCoolingDays	Substitui o valor dos dias de resfriamento para o volume

Exemplo: PersistentVolumeClaim com substituições de hierarquização automática

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: auto-tiering-pvc
  annotations:
    trident.netapp.io/tieringPolicy: auto
    trident.netapp.io/tieringMinimumCoolingDays: "45"
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: google-cloud-netapp-volumes-auto-tiering
  resources:
    requests:
      storage: 500Gi

```

Comportamento e limitações

Comportamento de provisionamento

- As configurações de auto-tiering são avaliadas e aplicadas somente no momento da criação do volume.
- Trident não reconcilia a configuração de tiering após o provisionamento.
- Os dias de resfriamento são ignorados quando a política de tiering está definida como `none`.

Limitações da plataforma

- O auto-tiering é compatível apenas com volumes NAS (NFS e SMB).
- Volumes em bloco (iSCSI) não suportam auto-tiering.
- O pool de storage do Google Cloud NetApp Volumes deve ter o armazenamento em camadas automático ativado no Google Cloud.

Valores suportados

- Intervalo válido para `tieringMinimumCoolingDays`: 2 a 183
- Valor padrão: 31

Configurar pools de storage do Google Cloud NetApp Volumes em modo ONTAP

A partir do Trident 26.06, você pode configurar `ontap-san` e `ontap-nas` back-ends

existentes para provisionar armazenamento em pools de storage do Google Cloud NetApp Volumes (GCNV) no modo ONTAP. Este recurso é uma Tech Preview.

OBSERVAÇÃO

Este recurso é uma Prévia Técnica no Trident 26.06. Recursos em Tech Preview não são suportados para uso em produção. A funcionalidade, os campos de configuração e a matriz de suporte podem ser alterados antes da disponibilidade geral (GA).

Como funciona

Trident reutiliza a `ontap-san` e `ontap-nas` lógica de driver existente e encaminha as chamadas REST do ONTAP por meio de um endpoint proxy do GCNV. Essa abordagem permite que você provisione e gerencie armazenamento em clusters ONTAP hospedados pelo GCNV, mantendo os mesmos fluxos de trabalho operacionais que você usa para um backend ONTAP direto. O modo ONTAP não introduz um novo driver de armazenamento. Você habilita isso por backend adicionando um `gcnv` bloco de configuração a um `ontap-san` ou `ontap-nas` backend.

O caminho de provisionamento é o seguinte:

PersistentVolumeClaim → Trident (`ontap-san` ou `ontap-nas`) → ONTAP cliente → GCNV proxy → ONTAP cluster no pool GCNV

Escopo suportado e não suportado

Esta versão de pré-visualização técnica oferece suporte ao seguinte:

- Drivers: `ontap-san` (iSCSI) e `ontap-nas` (NFS ou SMB).
- Operações de ciclo de vida por meio do proxy: inicialização do backend, criação e exclusão de volumes e fluxos REST do ONTAP relacionados.
- Modelos de autenticação: Workload Identity Pool (WIP), chave de conta de serviço e fallback de Application Default Credentials (ADC).

Os seguintes itens estão fora do escopo desta Tech Preview:

- Os `ontap-san-economy`, `ontap-nas-economy` e `ontap-nas-flexgroup` drivers.
- O caminho de personalidade ASA r2.
- Recurso alternativo ZAPI. O modo ONTAP utiliza apenas o ONTAP REST.

Pré-requisitos

Antes de configurar um backend no modo ONTAP, certifique-se de ter o seguinte:

- Trident 26.06 ou posterior.
- Um pool de storage GCNV ONTAP-mode em seu projeto e localização de destino.
- Permissões do GCP IAM para operações de proxy, com escopo adequado ao seu ambiente.
- Uma configuração de backend que inclui `proxyURL`, `projectNumber`, `location` e `poolID`.
- Para fluxos de trabalho iSCSI SAN, os pré-requisitos de iSCSI e multipath do lado do nó para sua plataforma. Consulte ["Prepare o nó de trabalho"](#).

Configurar o backend

A `TridentBackendConfig` requer `credentials`. Para o modo ONTAP, esse segredo contém as credenciais do proxy do GCP, não ONTAP `managementLIF/username/password`. `svm` é opcional: cada pool do GCNV no modo ONTAP atualmente possui um SVM, e Trident o deriva do pool quando omitido.

Use o mesmo padrão de conta de serviço do GCNV nativo: campos não sensíveis em `gcnv.apiKey`, `private_key` e `private_key_id` no segredo. Consulte ["Exemplos de configuração do Google Cloud NetApp Volumes"](#).

backend ontap-san

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: gcnv-ontap-san
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-san
  backendName: gcnv-ontap-san
  credentials:
    name: gcnv-sa-secret
    type: secret
  gcnv:
    proxyURL: "https://netapp.googleapis.com"
    projectNumber: "<project-number>"
    location: "<region-or-zone>"
    poolID: "<pool-id>"
    svm: "<svm-name>"
```

backend ontap-nas

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: gcnv-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: gcnv-ontap-nas
  credentials:
    name: gcnv-sa-secret
    type: secret
  gcnv:
    proxyURL: "https://netapp.googleapis.com"
    projectNumber: "<project-number>"
```

```

location: "<region-or-zone>"
poolID: "<pool-id>"
apiKey:
  type: service_account
  project_id: "<project-id>"
  client_email: "<service-account-email>"
  client_id: "<client-id>"
  auth_uri: "https://accounts.google.com/o/oauth2/auth"
  token_uri: "https://oauth2.googleapis.com/token"
  auth_provider_x509_cert_url:
    "https://www.googleapis.com/oauth2/v1/certs"
  client_x509_cert_url: "<client-x509-cert-url>"

```

Segredo

```

apiVersion: v1
kind: Secret
metadata:
  name: gcnv-sa-secret
  namespace: trident
type: Opaque
stringData:
  private_key_id: "<private-key-id>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <private-key>
    -----END PRIVATE KEY-----

```

OBSERVAÇÃO

Não coloque `private_key` ou `private_key_id` na `TridentBackendConfig` especificação — o CRD os rejeita. Use `ontap-san` com o mesmo `gcnv` e padrão de credencial para pool de storage em bloco.

```
svm: "<svm-name>"
```

== Authentication

Trident resolves credentials for proxy access in the following order:

- . Workload Identity Pool (WIP)
- . Service account key
- . Application Default Credentials (ADC)

For this Tech Preview, use the following practices:

- * Prefer Workload Identity Pool where it is available.
- * Do not embed raw private keys in version-controlled backend files. Store credentials in a Kubernetes secret.
- * Apply least-privilege IAM scoping to the service account.

== Validation and initialization behavior

Trident validates an ONTAP-mode backend during initialization and fails fast rather than partially initializing.

Backend initialization fails if a required ``gcnv`` field is missing, the driver is unsupported for ONTAP-mode, or credential resolution fails.

== Known limitations

- * This feature is a Tech Preview. Behavior and the supported matrix can change before GA.
- * ZAPI fallback is not used in ONTAP-mode.
- * Protocol and node-readiness requirements still apply. For example, iSCSI workflows require the node-side prerequisites described in [xref:{relative_path}../trident-use/worker-node-prep.html](#) [Prepare the worker node].
- * Existing ONTAP and GCNV environment constraints still apply.

== Upgrade and compatibility

ONTAP-mode is opt-in per backend through the ``gcnv`` configuration block:

- * Existing non-GCNV ONTAP backends are unaffected.
- * Mixed deployments that combine direct ONTAP backends and ONTAP-mode proxy backends are supported through backend-level configuration. Each backend is configured independently.
- * To stop using ONTAP-mode, remove or replace the affected backends. No global switch is required.

== What's next?

Apply secret before TBC; use ``kubectl apply`` and ``-n trident`` to match examples.

Configurar um NetApp HCI ou SolidFire backend

Aprenda como criar e usar um backend Element com sua instalação do Trident.

Detalhes do driver Element

Trident fornece o `solidfire-san` storage driver para se comunicar com o cluster. Os modos de acesso suportados são: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

O `solidfire-san` driver de armazenamento suporta os modos de volume *file* e *block*. Para o `Filesystem` volumeMode, Trident cria um volume e cria um sistema de arquivos. O tipo de sistema de arquivos é especificado pelo StorageClass.

Driver	Protocolo	VolumeMode	Modos de acesso suportados	Sistemas de arquivos suportados
solidfire-san	iSCSI	Bloco	RWO, ROX, RWX, RWOP	Sem sistema de arquivos. Dispositivo de bloco bruto.
solidfire-san	iSCSI	Sistema de arquivos	RWO, RWOP	xfs, ext3, ext4

Antes de começar

Você precisará do seguinte antes de criar um backend Element.

- Um sistema de storage compatível que execute o software Element.
- Credenciais para um administrador de cluster NetApp HCI/SolidFire ou usuário de locatário que possa gerenciar volumes.
- Todos os seus nós de trabalho do Kubernetes devem ter as ferramentas iSCSI apropriadas instaladas. Consulte ["Informações sobre preparação do nó de trabalho"](#).

Opções de configuração do backend

Consulte a tabela a seguir para as opções de configuração do backend:

Parâmetro	Descrição	Padrão
version		Sempre 1
storageDriverName	Nome do driver de armazenamento	Sempre "solidfire-san"
backendName	Nome personalizado ou o storage backend	"solidfire_" + endereço IP de storage (iSCSI)
Endpoint	MVIP para o SolidFire cluster com credenciais de locatário	
SVIP	Endereço IP e porta de storage (iSCSI)	
labels	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes.	""
TenantName	Nome do locatário a ser usado (criado se não for encontrado)	

Parâmetro	Descrição	Padrão
InitiatorIFace	Restringir o tráfego iSCSI a uma interface de host específica	"default"
UseCHAP	Use CHAP para autenticar iSCSI. Trident usa CHAP.	verdadeiro
AccessGroups	Lista de IDs de grupos de acesso a serem usados	Encontra o ID de um grupo de acesso chamado "trident"
Types	Especificações de QoS	
limitVolumeSize	Falhar no provisionamento se o tamanho do volume solicitado for superior a este valor	"" (não aplicado por padrão)
debugTraceFlags	Sinalizadores de depuração para usar na resolução de problemas. Exemplo, {"api":false, "method":true}	null

AVISO

Não utilize `debugTraceFlags` a menos que esteja solucionando problemas e necessite de um despejo de logs detalhado.

Exemplo 1: configuração de backend para `solidfire-san` driver com três tipos de volume

Este exemplo mostra um arquivo de backend usando autenticação CHAP e modelando três tipos de volume com garantias de QoS específicas. Muito provavelmente, você definiria classes de armazenamento para consumir cada um deles usando o `IOPS` parâmetro de classe de armazenamento.

```

---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: <svip>:3260
TenantName: <tenant>
labels:
  k8scluster: dev1
  backend: dev1-element-cluster
UseCHAP: true
Types:
  - Type: Bronze
    Qos:
      minIOPS: 1000
      maxIOPS: 2000
      burstIOPS: 4000
  - Type: Silver
    Qos:
      minIOPS: 4000

```

```

    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000

```

Exemplo 2: configuração de backend e classe de armazenamento para `solidfire-san` driver com pools virtuais

Este exemplo mostra o arquivo de definição de backend configurado com pools virtuais juntamente com StorageClasses que fazem referência a eles.

Trident copia os rótulos presentes em um pool de storage para o LUN de storage de backend durante o provisionamento. Para conveniência, administradores de storage podem definir rótulos por pool virtual e agrupar volumes por rótulo.

No arquivo de definição de backend de exemplo mostrado abaixo, valores padrão específicos são definidos para todos os pools de storage, que definem o `type` em Silver. Os pools virtuais são definidos na seção `storage`. Neste exemplo, alguns pools de storage definem seu próprio tipo e alguns pools substituem os valores padrão definidos acima.

```

---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: <svip>:3260
TenantName: <tenant>
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
type: Silver

```

```

labels:
  store: solidfire
  k8scluster: dev-1-cluster
region: us-east-1
storage:
- labels:
  performance: gold
  cost: "4"
  zone: us-east-1a
  type: Gold
- labels:
  performance: silver
  cost: "3"
  zone: us-east-1b
  type: Silver
- labels:
  performance: bronze
  cost: "2"
  zone: us-east-1c
  type: Bronze
- labels:
  performance: silver
  cost: "1"
  zone: us-east-1d

```

As seguintes definições de StorageClass referem-se aos pools virtuais acima. Usando o campo `parameters.selector`, cada StorageClass indica qual(is) pool(s) virtual(is) pode(m) ser usado(s) para hospedar um volume. O volume terá os aspectos definidos no pool virtual escolhido.

O primeiro StorageClass (`solidfire-gold-four`) mapeará o primeiro pool virtual. Este é o único pool que oferece desempenho Gold com um Volume Type QoS de Gold. O último StorageClass (`solidfire-silver`) indica qualquer pool de storage que ofereça desempenho Silver. Trident decidirá qual pool virtual será selecionado e garantirá que o requisito de storage seja atendido.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-gold-four
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=gold; cost=4
  fsType: ext4

---
apiVersion: storage.k8s.io/v1
kind: StorageClass

```

```

metadata:
  name: solidfire-silver-three
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=silver; cost=3
  fsType: ext4

---

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-bronze-two
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=bronze; cost=2
  fsType: ext4

---

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-one
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=silver; cost=1
  fsType: ext4

---

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver
provisioner: csi.trident.netapp.io
parameters:
  selector: performance=silver
  fsType: ext4

```

Encontre mais informações

- ["Grupos de acesso a volume"](#)

Drivers SAN do ONTAP

Visão geral do driver ONTAP SAN

Saiba mais sobre como configurar um backend ONTAP com os drivers SAN do ONTAP e

do Cloud Volumes ONTAP.

Detalhes do driver ONTAP SAN

Trident fornece os seguintes drivers de armazenamento SAN para se comunicar com o ONTAP cluster. Os modos de acesso suportados são: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Driver	Protocolo	volumeMod e	Modos de acesso suportados	Sistemas de arquivos suportados
ontap-san	iSCSI SCSI sobre FC	Bloco	RWO, ROX, RWX, RWOP	Sem sistema de arquivos; dispositivo de bloco bruto
ontap-san	iSCSI SCSI sobre FC	Sistema de arquivos	RWO, RWOP ROX e RWX não estão disponíveis no modo de volume de sistema de arquivos.	xfs, ext3, ext4
ontap-san	NVMe/TCP Consulte Considerações adicionais para NVMe/TCP .	Bloco	RWO, ROX, RWX, RWOP	Sem sistema de arquivos; dispositivo de bloco bruto
ontap-san	NVMe/TCP Consulte Considerações adicionais para NVMe/TCP .	Sistema de arquivos	RWO, RWOP ROX e RWX não estão disponíveis no modo de volume de sistema de arquivos.	xfs, ext3, ext4
ontap-san-economy	iSCSI	Bloco	RWO, ROX, RWX, RWOP	Sem sistema de arquivos; dispositivo de bloco bruto
ontap-san-economy	iSCSI	Sistema de arquivos	RWO, RWOP ROX e RWX não estão disponíveis no modo de volume de sistema de arquivos.	xfs, ext3, ext4

AVISO

- Use `ontap-san-economy` somente se a contagem de uso de volume persistente prevista for maior que "[limites de volume ONTAP suportados](#)".
- Use `ontap-nas-economy` somente se a contagem de uso de volume persistente prevista for maior que "[limites de volume ONTAP suportados](#)" e o driver `ontap-san-economy` não puder ser usado.
- Não utilize `ontap-nas-economy` se você prevê a necessidade de proteção de dados, recuperação de desastres ou mobilidade.

- NetApp não recomenda usar o crescimento automático do FlexVol em todos os drivers ONTAP, exceto ontap-san. Como alternativa, Trident oferece suporte ao uso de reserva de snapshot e dimensiona os volumes FlexVol de acordo.

Permissões do usuário

Trident espera ser executado como administrador do ONTAP ou do SVM, normalmente usando o `admin` usuário do cluster ou um `vsadmin` usuário do SVM, ou um usuário com um nome diferente que tenha a mesma função. Para implantações do Amazon FSx for NetApp ONTAP, Trident espera ser executado como administrador do ONTAP ou do SVM, usando o usuário do cluster `fsxadmin` ou um usuário do SVM `vsadmin`, ou um usuário com um nome diferente que tenha a mesma função. O `fsxadmin` usuário é um substituto limitado para o usuário administrador do cluster.

OBSERVAÇÃO

Se você usar o `limitAggregateUsage` parâmetro, são necessárias permissões de administrador do cluster. Ao usar Amazon FSx for NetApp ONTAP com Trident, o `limitAggregateUsage` parâmetro não funcionará com as contas de usuário `vsadmin` e `fsxadmin`. A operação de configuração falhará se você especificar este parâmetro.

Embora seja possível criar uma função mais restritiva dentro do ONTAP que um driver Trident possa usar, não recomendamos isso. A maioria das novas versões do Trident chamará APIs adicionais que precisariam ser consideradas, dificultando as atualizações e tornando-as propensas a erros.

Considerações adicionais para NVMe/TCP

Trident suporta o protocolo non-volatile memory express (NVMe) usando o `ontap-san` driver incluindo:

- IPv6
- Instantâneos e clones de volumes NVMe
- Redimensionando um volume NVMe
- Importando um volume NVMe criado fora do Trident para que seu ciclo de vida possa ser gerenciado pelo Trident
- Multipathing nativo NVMe
- Encerramento correto ou incorreto dos nós K8s (24.06)

Trident não suporta:

- DH-HMAC-CHAP que é suportado nativamente pelo NVMe
- Multipathing do device mapper (DM)
- LUKS criptografia

OBSERVAÇÃO

O NVMe é suportado apenas com as APIs REST do ONTAP e não é suportado com ONTAPI (ZAPI).

Prepare-se para configurar o backend com os drivers ONTAP SAN

Compreenda os requisitos e as opções de autenticação para configurar um backend ONTAP com drivers ONTAP SAN.

Requisitos

Para todos os backends ONTAP, Trident exige que pelo menos um agregado seja atribuído à SVM.

OBSERVAÇÃO

"Sistemas ASA r2" diferem de outros sistemas ONTAP (ASA, AFF e FAS) na implementação de sua camada de storage. Nos sistemas ASA r2, zonas de disponibilidade de storage são usadas em vez de agregados. Consulte o ["este"](#) artigo da Knowledge Base sobre como atribuir agregados a SVMs em sistemas ASA r2.

Lembre-se de que você também pode executar mais de um driver e criar classes de armazenamento que apontem para um ou outro. Por exemplo, você pode configurar uma `san-dev` classe que usa o `ontap-san` driver e uma `san-default` classe que usa o `ontap-san-economy` driver.

Todos os seus nós de trabalho do Kubernetes devem ter as ferramentas iSCSI apropriadas instaladas. Consulte ["Prepare o nó de trabalho"](#) para obter detalhes.

Autenticar o backend ONTAP

Trident oferece dois modos de autenticação de um backend ONTAP.

- Baseado em credenciais: o nome de usuário e a senha de um usuário do ONTAP com as permissões necessárias. Recomenda-se o uso de uma função de login de segurança predefinida, como `admin` ou `vsadmin` para garantir a máxima compatibilidade com as versões do ONTAP.
- Com base em certificado: Trident também pode se comunicar com um ONTAP cluster usando um certificado instalado no backend. Nesse caso, a definição do backend deve conter os valores codificados em Base64 do certificado do cliente, da chave e do certificado da CA confiável, se utilizado (recomendado).

Você pode atualizar os backends existentes para alternar entre métodos baseados em credenciais e baseados em certificados. No entanto, apenas um método de autenticação é suportado por vez. Para mudar para um método de autenticação diferente, você deve remover o método existente da configuração do backend.

AVISO

Se você tentar fornecer **tanto credenciais quanto certificados**, a criação do backend falhará com um erro informando que mais de um método de autenticação foi fornecido no arquivo de configuração.

Ativar autenticação baseada em credenciais

Trident requer as credenciais de um administrador com escopo de SVM/cluster para se comunicar com o backend do ONTAP. Recomenda-se o uso de funções padrão predefinidas, como `admin` ou `vsadmin`. Isso garante a compatibilidade futura com versões do ONTAP que possam expor APIs de recursos a serem usadas por versões futuras do Trident. Uma função de login de segurança personalizada pode ser criada e usada com Trident, mas não é recomendada.

Uma definição de backend de exemplo será semelhante a esta:

YAML

```
---  
version: 1
```

```
backendName: ExampleBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

Lembre-se de que a definição do backend é o único local onde as credenciais são armazenadas em texto simples. Após a criação do backend, nomes de usuário/senhas são codificados em Base64 e armazenados como segredos do Kubernetes. A criação ou atualização de um backend é a única etapa que requer conhecimento das credenciais. Assim, trata-se de uma operação exclusiva do administrador, a ser realizada pelo administrador de storage do Kubernetes.

Ativar autenticação baseada em certificado

Novos e existentes backends podem usar um certificado e se comunicar com o backend do ONTAP. Três parâmetros são necessários na definição do backend.

- `clientCertificate`: Valor codificado em Base64 do certificado do cliente.
- `clientPrivateKey`: Valor codificado em Base64 da chave privada associada.
- `trustedCACertificate`: valor codificado em Base64 do certificado CA confiável. Se uma CA confiável estiver sendo usada, este parâmetro deve ser fornecido. Isso pode ser ignorado se nenhuma CA confiável for usada.

Um fluxo de trabalho típico envolve as seguintes etapas.

Passos

1. Gere um certificado de cliente e uma chave. Ao gerar, defina o Nome Comum (CN) para o usuário ONTAP que será usado para autenticação.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=admin"
```

2. Adicione um certificado de CA confiável ao cluster ONTAP. Isso pode já ter sido configurado pelo

administrador de storage. Ignore se nenhuma CA confiável for utilizada.

```
security certificate install -type server -cert-name <trusted-ca-cert-name> -vserver <vserver-name>
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca <cert-authority>
```

3. Instale o certificado do cliente e a chave (do passo 1) no cluster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-name> -vserver <vserver-name>
security ssl modify -vserver <vserver-name> -client-enabled true
```

OBSERVAÇÃO

Após executar este comando, ONTAP solicitará a entrada do certificado. Cole o conteúdo do `k8senv.pem` arquivo gerado na etapa 1, depois pressione `END` para concluir a instalação.

4. Confirme se a função de login de segurança do ONTAP suporta `cert` método de autenticação.

```
security login create -user-or-group-name admin -application ontapi -authentication-method cert
security login create -user-or-group-name admin -application http -authentication-method cert
```

5. Teste a autenticação usando o certificado gerado. Substitua <ONTAP Management LIF> e <vserver name> pelo endereço IP da Management LIF e pelo nome da SVM.

```
curl -X POST -Lk https://<ONTAP-Management-LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key --cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp xmlns="http://www.netapp.com/filer/admin" version="1.21" vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Codifique o certificado, a chave e o certificado da CA confiável com Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Crie o backend usando os valores obtidos na etapa anterior.

```
cat cert-backend.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "trustedCACertificate": "QNFinfO...SiqOyN",
  "storagePrefix": "myPrefix_"
}

tridentctl create backend -f cert-backend.json -n trident
+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |          0 |
+-----+-----+-----+-----+
+-----+-----+
```

Atualize os métodos de autenticação ou altere as credenciais

Você pode atualizar um backend existente para usar um método de autenticação diferente ou para rotacionar suas credenciais. Isso funciona nos dois sentidos: backends que utilizam nome de usuário/senha podem ser atualizados para usar certificados; backends que utilizam certificados podem ser atualizados para usar nome de usuário/senha. Para fazer isso, você deve remover o método de autenticação existente e adicionar o novo método de autenticação. Em seguida, use o arquivo backend.json atualizado contendo os parâmetros necessários para executar `tridentctl backend update`.

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}
```

```
#Update backend with tridentctl
tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident
```

NAME	STORAGE DRIVER	UUID
SanBackend	ontap-san	586b1cd5-8cf8-428d-a76c-2872713612c1

```
STATE | VOLUMES |
online | 9 |
```

OBSERVAÇÃO

Ao rotacionar senhas, o administrador de storage deve primeiro atualizar a senha do usuário no ONTAP. Em seguida, é feita uma atualização no backend. Ao rotacionar certificados, vários certificados podem ser adicionados ao usuário. O backend é então atualizado para usar o novo certificado, após o que o certificado antigo pode ser excluído do cluster ONTAP.

A atualização do backend não interrompe o acesso aos volumes já criados, nem afeta as conexões de volume feitas posteriormente. Uma atualização bem-sucedida do backend indica que Trident pode se comunicar com o ONTAP backend e lidar com operações de volume futuras.

Criar função ONTAP personalizada para Trident

Você pode criar uma função de cluster ONTAP com privilégios mínimos para que não precise usar a função de administrador do ONTAP para executar operações no Trident. Ao incluir o nome de usuário em um arquivo de configuração de backend do Trident, o Trident usa a função de cluster ONTAP que você criou para executar as operações.

Consulte "[Gerador de funções personalizadas Trident](#)" para obter mais informações sobre como criar funções personalizadas do Trident.

Usando ONTAP CLI

1. Crie uma nova função usando o seguinte comando:

```
security login role create <role_name> -cmddirname "command" -access all
-vserver <svm_name>
```

2. Crie um nome de usuário para o usuário do Trident:

```
security login create -username <user_name> -application ontapi
-authmethod <password> -role <name_of_role_in_step_1> -vserver
<svm_name> -comment "user_description"
```

3. Mapeie a função para o usuário:

```
security login modify username <user_name> -vserver <svm_name> -role
<role_name> -application ontapi -application console -authmethod
```

<password\>

Usando System Manager

Execute as seguintes etapas no ONTAP System Manager:

1. Crie uma função personalizada:

- a. Para criar uma função personalizada no nível do cluster, selecione **Cluster > Settings**.

(Ou) Para criar uma função personalizada no nível da SVM, selecione **Storage > Storage VMs > required svm > Settings > Users and Roles**.

- b. Selecione o ícone de seta (→) ao lado de **Users and Roles**.

- c. Selecione **+Adicionar** em **Roles**.

- d. Defina as regras para a função e clique em **Save**.

2. Mapeie a função ao usuário Trident: + Execute as seguintes etapas na página **Usuários e Funções**:

- a. Selecione o ícone Adicionar + em **Usuários**.

- b. Selecione o nome de usuário desejado e selecione uma função no menu suspenso para **Função**.

- c. Clique em **Salvar**.

Consulte as seguintes páginas para obter mais informações:

- ["Funções personalizadas para administração do ONTAP"](#) ou ["Definir funções personalizadas"](#)
- ["Trabalhe com funções e usuários"](#)

Autentique conexões com CHAP bidirecional

Trident pode autenticar sessões iSCSI com CHAP bidirecional para os `ontap-san` e `ontap-san-economy` drivers. Isso requer a ativação da opção `useCHAP` na definição do seu backend. Quando definido como `true`, Trident configura a segurança do iniciador padrão da SVM para CHAP bidirecional e define o nome de usuário e os segredos do arquivo de backend. NetApp recomenda o uso de CHAP bidirecional para autenticar conexões. Veja o exemplo de configuração a seguir:

```
---
version: 1
storageDriverName: ontap-san
backendName: ontap_san_chap
managementLIF: 192.168.0.135
svm: ontap_iscsi_svm
useCHAP: true
username: vsadmin
password: password
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
```

AVISO

O `useCHAP` parâmetro é uma opção booleana que pode ser configurada apenas uma vez. Ele é definido como falso por padrão. Depois de defini-lo como verdadeiro, você não pode alterá-lo para falso.

Além de `useCHAP=true`, os campos `chapInitiatorSecret`, `chapTargetInitiatorSecret`, `chapTargetUsername` e `chapUsername` devem ser incluídos na definição do backend. Os segredos podem ser alterados após a criação de um backend executando `tridentctl update`.

Como funciona

Ao definir `useCHAP` como verdadeiro, o administrador de storage instrui Trident a configurar CHAP no backend de storage. Isso inclui o seguinte:

- Configurando CHAP no SVM:
 - Se o tipo de segurança do iniciador padrão da SVM for `none` (definido por padrão) e não houver LUNs preexistentes no volume, Trident definirá o tipo de segurança padrão para CHAP e prosseguirá com a configuração do nome de usuário e segredos do iniciador e destino CHAP.
 - Se a SVM contiver LUNs, Trident não habilitará CHAP na SVM. Isso garante que o acesso às LUNs já presentes na SVM não seja restringido.
- Configuração do nome de usuário e dos segredos do iniciador e do alvo CHAP; essas opções devem ser especificadas na configuração do backend (como mostrado acima).

Após a criação do backend, Trident cria um correspondente `tridentbackend` CRD e armazena os segredos CHAP e os nomes de usuário como segredos do Kubernetes. Todos os PVs que são criados pelo Trident nesse backend serão montados e anexados via CHAP.

Rotacionar credenciais e atualizar backends

Você pode atualizar as credenciais CHAP atualizando os parâmetros CHAP no `backend.json` arquivo. Isso exigirá atualizar os segredos CHAP e usar o `tridentctl update` comando para refletir essas alterações.

AVISO

Ao atualizar os segredos CHAP de um backend, você deve usar `tridentctl` para atualizar o backend. Não atualize as credenciais no cluster de storage usando a ONTAP CLI ou ONTAP System Manager, pois Trident não conseguirá detectar essas alterações.

```
cat backend-san.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap_san_chap",
  "managementLIF": "192.168.0.135",
  "svm": "ontap_iscsi_svm",
  "useCHAP": true,
  "username": "vsadmin",
  "password": "password",
  "chapInitiatorSecret": "cl9qxUpDaTeD",
  "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
```

```

    "chapUsername": "uh2aNCLSD6cNwxyz",
  }

./tridentctl update backend ontap_san_chap -f backend-san.json -n trident
+-----+-----+-----+
+-----+-----+
| NAME | STORAGE DRIVER | UUID |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| ontap_san_chap | ontap-san | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online | 7 |
+-----+-----+-----+
+-----+-----+

```

As conexões existentes permanecerão inalteradas; elas continuarão ativas se as credenciais forem atualizadas pelo Trident no SVM. Novas conexões usam as credenciais atualizadas e as conexões existentes continuam ativas. Desconectar e reconectar PVs antigos fará com que eles usem as credenciais atualizadas.

Opções e exemplos de configuração do ONTAP SAN

Crie e utilize os drivers ONTAP SAN com sua instalação do Trident. Esta seção fornece exemplos de configuração de backend e detalhes para mapear backends para StorageClasses. "[Sistemas ASA r2](#)" diferem de outros sistemas ONTAP (ASA, AFF e FAS) na implementação de sua camada de storage. Essas variações impactam o uso de certos parâmetros conforme indicado. "[Saiba mais sobre as diferenças entre sistemas ASA r2 e outros sistemas ONTAP](#)". Na configuração de backend do Trident, você não precisa especificar que seu sistema é ASA r2. Ao selecionar `ontap-san` como o `storageDriverName`, o Trident detecta automaticamente o ASA r2 ou outros sistemas ONTAP. Alguns parâmetros de configuração de backend não se aplicam a sistemas ASA r2, conforme observado na tabela abaixo.

OBSERVAÇÃO

Apenas o `ontap-san` driver (com os protocolos iSCSI, NVMe/TCP e FC) é compatível com sistemas ASA r2.

Opções de configuração do backend

A partir da versão 26.06, você pode habilitar o posicionamento balanceado do ONTAP para que o ONTAP selecione o agregado para novos volumes. Consulte "[Utilize o posicionamento balanceado com os backends ONTAP](#)" para requisitos e exemplos.

Consulte a tabela a seguir para as opções de configuração do backend:

Parâmetro	Descrição	Padrão
<code>version</code>		Sempre 1

Parâmetro	Descrição	Padrão
storageDriverName	Nome do driver de armazenamento. Não pode ser modificado após a criação. Para atualizar este parâmetro, você deve criar um novo backend.	ontap-san ou ontap-san-economy
backendName	Nome personalizado ou o storage backend	Nome do driver + "_" + dataLIF
managementLIF	<p>Endereço IP de um cluster ou LIF de gerenciamento de SVM.</p> <p>É possível especificar um nome de domínio totalmente qualificado (FQDN).</p> <p>Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p> <p>Para um switchover MetroCluster perfeito, consulte o Exemplo do MetroCluster.</p> <div> <div>OBSERVAÇÃO</div> <div>Se estiver usando credenciais "vsadmin", managementLIF deve ser a da SVM; se estiver usando credenciais "admin", managementLIF deve ser a do cluster.</div> </div>	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	<p>Endereço IP do protocolo LIF. Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Não especifique para iSCSI. Trident usa "Mapa de LUN seletivo do ONTAP" para descobrir os LIFs iSCSI necessários para estabelecer uma sessão de múltiplos caminhos. Um aviso é gerado se dataLIF for definido explicitamente. Omita para MetroCluster. Consulte o Exemplo do MetroCluster.</p>	Derivado pelo SVM
svm	Máquina virtual de storage a ser usada Omitir para MetroCluster. Consulte o Exemplo do MetroCluster .	Derivado se uma SVM managementLIF for especificada
useCHAP	Use CHAP para autenticar iSCSI para drivers ONTAP SAN [parâmetro booleano]. Defina como true para que Trident configure e use CHAP bidirecional como autenticação padrão para o SVM fornecido no backend. Consulte "Prepare-se para configurar o backend com os drivers ONTAP SAN" para obter detalhes. Não compatível com FCP ou NVMe/TCP.	false

Parâmetro	Descrição	Padrão
chapInitiatorSecret	Segredo do iniciador CHAP. Obrigatório se useCHAP=true	""
labels	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes	""
chapTargetInitiatorSecret	Segredo do iniciador do alvo CHAP. Obrigatório se useCHAP=true	""
chapUsername	Nome de usuário de entrada. Obrigatório se useCHAP=true	""
chapTargetUsername	Nome de usuário de destino. Obrigatório se useCHAP=true	""
clientCertificate	Valor codificado em Base64 do certificado do cliente. Usado para autenticação baseada em certificado	""
clientPrivateKey	Valor codificado em Base64 da chave privada do cliente. Usado para autenticação baseada em certificado	""
trustedCACertificate	Valor codificado em Base64 do certificado da CA confiável. Opcional. Usado para autenticação baseada em certificado.	""
username	Nome de usuário necessário para se comunicar com o cluster ONTAP. Usada para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autentique o Trident em um SVM de backend usando credenciais do Active Directory" .	""
password	Senha necessária para se comunicar com o cluster ONTAP. Usada para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autentique o Trident em um SVM de backend usando credenciais do Active Directory" .	""
svm	Máquina virtual de storage para usar	Derivado se uma SVM managementLIF for especificada
storagePrefix	Prefixo usado ao provisionar novos volumes no SVM. Não pode ser modificado posteriormente. Para atualizar este parâmetro, você precisa criar um novo backend.	trident

Parâmetro	Descrição	Padrão
aggregate	<p>Agregado para provisionamento (opcional; se definido, deve ser atribuído à SVM). Para o <code>ontap-nas-flexgroup</code> driver, esta opção é ignorada. Se não for atribuído, qualquer um dos agregados disponíveis pode ser usado para provisionar um FlexGroup volume.</p> <div> <div>OBSERVAÇÃO</div> <p>Quando o agregado é atualizado no SVM, ele é atualizado automaticamente no Trident por meio de polling no SVM, sem a necessidade de reiniciar o Trident Controller. Quando você configurou um agregado específico no Trident para provisionar volumes, se o agregado for renomeado ou movido para fora do SVM, o backend entra em estado de falha no Trident durante o polling do agregado no SVM. Você deve alterar o agregado para um que esteja presente no SVM ou removê-lo completamente para que o backend volte a ficar online.</p> <p>Não especificar para sistemas ASA r2.</p> <p>Não especifique quando <code>useBalancedPlacement</code> estiver definido como <code>true</code>.</p> </div>	""
useBalancedPlacement	<p>Delegar a seleção de aggregate para novos volumes ao ONTAP [Booleano]. Requer ONTAP 9.19.1 ou posterior e <code>useREST</code> definido como <code>true</code>. Não pode ser combinado com <code>aggregate</code>.</p> <p>Consulte "Utilize o posicionamento balanceado com os backends ONTAP" para requisitos e exemplos.</p>	false
limitAggregateUsage	<p>O provisionamento falhará se o uso ultrapassar essa porcentagem. Se você estiver usando um Amazon FSx para NetApp ONTAP backend, não especifique <code>limitAggregateUsage</code>. As configurações fornecidas <code>fsxadmin</code> e <code>vsadmin</code> não contêm as permissões necessárias para recuperar o uso agregado e limitá-lo usando Trident. Não especificar para sistemas ASA r2.</p>	"" (não aplicado por padrão)

Parâmetro	Descrição	Padrão
limitVolumeSize	O provisionamento falha se o tamanho do volume solicitado for superior a este valor. Também restringe o tamanho máximo dos volumes que gerencia para LUNs.	"" (não aplicado por padrão)
lunsPerFlexvol	Número máximo de LUNs por FlexVol, deve estar no intervalo [50, 200]	100
debugTraceFlags	Sinalizadores de depuração para usar na resolução de problemas. Exemplo, {"api":false, "method":true} Não use a menos que esteja solucionando problemas e precise de um despejo de log detalhado.	null
useREST	<p>Parâmetro booleano para usar as ONTAP REST APIs.</p> <div> <p><code>`useREST`</code> Quando definido como <code>`true`</code>, Trident usa as ONTAP REST APIs para se comunicar com o backend; quando definido como <code>`false`</code>, Trident usa chamadas ONTAPI (ZAPI) para se comunicar com o backend. Este recurso requer ONTAP 9.11.1 e versões posteriores. Além disso, a função de login do ONTAP utilizada deve ter acesso ao aplicativo <code>`ontapi`</code>. Isso é atendido pelas funções predefinidas <code>`vsadmin`</code> e <code>`cluster-admin`</code>. A partir da versão 24.06 do Trident e ONTAP 9.15.1 ou posterior, <code>`useREST`</code> é definido como <code>`true`</code> por padrão; altere <code>`useREST`</code> para <code>`false`</code> para usar chamadas ONTAPI (ZAPI).</p> </div> <p>useREST está totalmente qualificado para NVMe/TCP.</p> <div> <p>OBSERVAÇÃO</p> <p>O NVMe é suportado apenas com as APIs REST do ONTAP e não é suportado com ONTAPI (ZAPI).</p> </div> <p>Se especificado, defina sempre como <code>true</code> para sistemas ASA r2.</p>	true`para ONTAP 9.15.1 ou posterior, caso contrário `false.

Parâmetro	Descrição	Padrão
sanType	Use para selecionar <code>iscsi</code> para iSCSI, <code>nvme</code> para NVMe/TCP ou <code>fc</code> para SCSI sobre Fibre Channel (FC).	<code>iscsi</code> se estiver em branco
formatOptions	Use <code>formatOptions</code> para especificar argumentos de linha de comando para o comando <code>mkfs</code> , que é aplicado sempre que um volume é formatado. Isso permite que você formate o volume de acordo com suas preferências. Certifique-se de especificar as <code>formatOptions</code> de forma semelhante às opções do comando <code>mkfs</code> , excluindo o caminho do dispositivo. Exemplo: <code>"-E nodiscard"</code> Compatível para <code>ontap-san</code> e <code>ontap-san-economy</code> drivers com o protocolo iSCSI. Além disso, compatível com sistemas ASA r2 ao usar os protocolos iSCSI e NVMe/TCP.	
limitVolumePoolSize	Tamanho máximo solicitável de FlexVol ao usar LUNs no backend <code>ontap-san-economy</code> .	"" (não aplicado por padrão)
denyNewVolumePools	Restringe <code>ontap-san-economy</code> os backends de criar novos volumes FlexVol para conter seus LUNs. Somente FlexVols preexistentes são usados para o provisionamento de novos PVs.	

Recomendações para uso de formatOptions

Trident recomenda as seguintes opções para agilizar o processo de formatação:

- **-E nodiscard (ext3, ext4):** Não tente descartar blocos durante a criação do sistema de arquivos (o descarte inicial de blocos é útil em dispositivos de estado sólido e em storage esparso/com thin provisioning). Esta opção substitui a opção obsoleta `"-K"` e é aplicável aos sistemas de arquivos `ext3` e `ext4`.
- **-K (xfs):** Não tente descartar blocos durante a criação do sistema de arquivos (`mkfs`). Esta opção se aplica ao sistema de arquivos `xfs`.

Autentique o Trident em um SVM de backend usando credenciais do Active Directory

Você pode configurar Trident para autenticar em uma SVM de backend usando credenciais do Active Directory (AD). Antes que uma conta do AD possa acessar a SVM, você deve configurar o acesso do controlador de domínio do AD ao cluster ou à SVM. Para administração do cluster com uma conta do AD, você deve criar domain tunnel. Consulte ["Configurar o acesso do controlador de domínio do Active Directory no ONTAP"](#) para obter detalhes.

passos

1. Configurar as definições do Domain Name System (DNS) para uma SVM de backend:

```
vserver services dns create -vserver <svm_name> -dns-servers
<dns_server_ip1>,<dns_server_ip2>
```

2. Execute o seguinte comando para criar uma conta de computador para a SVM no Active Directory:

```
vserver active-directory create -vserver DataSVM -account-name ADSERVER1
-domain demo.netapp.com
```

3. Use este comando para criar um usuário ou grupo do AD para gerenciar o cluster ou SVM

```
security login create -vserver <svm_name> -user-or-group-name
<ad_user_or_group> -application <application> -authentication-method domain
-role vsadmin
```

4. No arquivo de configuração do Trident backend, defina os parâmetros `username` e `password` para o nome de usuário ou grupo do AD e a senha, respectivamente.

Opções de configuração de backend para provisionamento de volumes

Você pode controlar o provisionamento padrão usando essas opções na seção `defaults` do arquivo de configuração. Para um exemplo, veja os exemplos de configuração abaixo.

Parâmetro	Descrição	Padrão
<code>spaceAllocation</code>	Alocação de espaço para LUNs	"verdadeiro" Se especificado, defina como <code>true</code> para sistemas ASA r2.
<code>spaceReserve</code>	Modo de reserva de espaço; "nenhum" (com thin provisioning) ou "volume" (thick). Definido como <code>none</code> para sistemas ASA r2.	"none"
<code>snapshotPolicy</code>	Política do Snapshot a ser usada. Definida como <code>none</code> para sistemas ASA r2.	"none"
<code>qosPolicy</code>	Grupo de políticas de QoS a ser atribuído aos volumes criados. Escolha um dos <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> por pool de storage/backend. O uso de grupos de políticas de QoS com Trident requer ONTAP 9.8 ou posterior. Você deve usar um grupo de políticas de QoS não compartilhado e garantir que o grupo de políticas seja aplicado a cada componente individualmente. Um grupo de políticas de QoS compartilhado impõe o limite máximo para a taxa de transferência total de todas as cargas de trabalho.	""
<code>adaptiveQosPolicy</code>	Grupo de políticas de QoS adaptável para atribuir aos volumes criados. Escolha uma de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> por pool de storage/backend	""
<code>snapshotReserve</code>	Percentual do volume reservado para snapshots. Não especificar para sistemas ASA r2.	"0" se <code>snapshotPolicy</code> for "none", caso contrário ""
<code>splitOnClone</code>	Separar um clone de seu progenitor no momento da criação	"false"

Parâmetro	Descrição	Padrão
encryption	Habilite a NetApp Volume Encryption (NVE) no novo volume; o padrão é <code>false</code> . A NVE deve estar licenciada e habilitada no cluster para usar esta opção. Se a NAE estiver habilitada no backend, qualquer volume provisionado no Trident terá a NAE habilitada. Para mais informações, consulte: " Como Trident funciona com NVE e NAE ".	"falso" Se especificado, defina como <code>true</code> para sistemas ASA r2.
luksEncryption	Ative a criptografia LUKS. Consulte " Use Linux Unified Key Setup (LUKS) ".	Defina como <code>false</code> para sistemas ASA r2.
tieringPolicy	Política de tiering para usar "none" Não especificar para sistemas ASA r2.	
nameTemplate	Modelo para criar nomes de volume personalizados.	""

Exemplos de provisionamento de volume

Aqui está um exemplo com valores padrão definidos:

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: trident_svm
username: admin
password: <password>
labels:
  k8scluster: dev2
  backend: dev2-sanbackend
storagePrefix: alternate-trident
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: standard
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

OBSERVAÇÃO

Para todos os volumes criados usando o `ontap-san` driver, o Trident adiciona 10% de capacidade extra ao FlexVol para acomodar os metadados do LUN. O LUN é provisionado com o tamanho exato que o usuário solicita no PVC. O Trident adiciona 10% ao FlexVol (exibido como tamanho disponível no ONTAP). Os usuários agora obtêm a quantidade de capacidade utilizável que solicitaram. Essa alteração também impede que os LUNs se tornem somente leitura, a menos que o espaço disponível esteja totalmente utilizado. Isso não se aplica ao `ontap-san-`

economy.

Para backends que definem `snapshotReserve`, Trident calcula o tamanho dos volumes da seguinte forma:

```
Total volume size = [(PVC requested size) / (1 - (snapshotReserve percentage) / 100)] * 1.1
```

O valor 1.1 representa os 10% adicionais que o Trident adiciona ao FlexVol para acomodar os metadados da LUN. Para `snapshotReserve` = 5%, e solicitação de PVC = 5 GiB, o tamanho total do volume é 5,79 GiB e o tamanho disponível é 5,5 GiB. O comando `volume show` deve exibir resultados semelhantes a este exemplo:

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e42ec6fe_3baa_4af6_996d_134adbbb8e6d	online	RW	5.79GB	5.50GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

3 entries were displayed.

Atualmente, o redimensionamento é a única maneira de usar o novo cálculo para um existing volume.

Exemplos de configuração mínima

Os exemplos a seguir mostram configurações básicas que deixam a maioria dos parâmetros com os valores padrão. Esta é a maneira mais fácil de definir um backend.

OBSERVAÇÃO

Se você estiver usando Amazon FSx no NetApp ONTAP com Trident, NetApp recomenda que você especifique nomes DNS para LIFs em vez de endereços IP.

▼ Exemplo de ONTAP SAN

Esta é uma configuração básica usando o `ontap-san` driver.

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
username: vsadmin
password: <password>
```

▼ Exemplo do MetroCluster

Você pode configurar o backend para evitar ter que atualizar manualmente a definição do backend após switchover e switchback durante ["Replicação e recuperação de SVM"](#).

Para switchover e switchback sem interrupções, especifique a SVM usando `managementLIF` e omita os parâmetros `svm`. Por exemplo:

```
version: 1
storageDriverName: ontap-san
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

▼ Exemplo de economia ONTAP SAN

```
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
username: vsadmin
password: <password>
```

▼ Exemplo de autenticação baseada em certificado

Neste exemplo de configuração básica `clientCertificate`, `clientPrivateKey` e `trustedCACertificate` (opcional, se estiver usando uma CA confiável) são preenchidos em `backend.json` e recebem os valores codificados em base64 do certificado do cliente, da chave privada e do certificado da CA confiável, respectivamente.

```
---
version: 1
storageDriverName: ontap-san
backendName: DefaultSANBackend
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

▼ Exemplos bidirecionais CHAP

Esses exemplos criam um backend com `useCHAP` definido como `true`.

Exemplo ONTAP SAN CHAP

```
---
```

```

version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>

```

Exemplo de economia SAN CHAP do ONTAP

```

---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>

```

▼ Exemplo de colocação equilibrada

Este exemplo habilita o posicionamento balanceado do ONTAP, de forma que o ONTAP selecione o agregado para novos volumes. O posicionamento balanceado requer o ONTAP 9.19.1 ou posterior. Consulte ["Utilize o posicionamento balanceado com os backends ONTAP"](#) para obter detalhes.

```

---
version: 1
storageDriverName: ontap-san
backendName: san-balanced-placement
managementLIF: 10.0.0.1
svm: svm_iscsi
username: vsadmin
password: <password>
useBalancedPlacement: true

```

▼ Exemplo de NVMe/TCP

Você precisa ter uma SVM configurada com NVMe no seu backend ONTAP. Esta é uma configuração básica de backend para NVMe/TCP.

```
---  
version: 1  
backendName: NVMeBackend  
storageDriverName: ontap-san  
managementLIF: 10.0.0.1  
svm: svm_nvme  
username: vsadmin  
password: password  
sanType: nvme  
useREST: true
```

▼ Exemplo de SCSI sobre FC (FCP)

Você precisa ter uma SVM configurada com FC no seu ONTAP backend. Esta é uma configuração básica de backend para FC.

```
---  
version: 1  
backendName: fcp-backend  
storageDriverName: ontap-san  
managementLIF: 10.0.0.1  
svm: svm_fc  
username: vsadmin  
password: password  
sanType: fcp  
useREST: true
```

▼ Exemplo de configuração de backend com nameTemplate

```
---  
version: 1  
storageDriverName: ontap-san  
backendName: ontap-san-backend  
managementLIF: <ip address>  
svm: svm0  
username: <admin>  
password: <password>  
defaults:  
  nameTemplate:  
    "{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.volume.RequestName}}"  
labels:
```

```
cluster: ClusterA
PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

▼ formatOptions exemplo para o driver ontap-san-economy

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: ""
svm: svm1
username: ""
password: "!"
storagePrefix: whelk_
debugTraceFlags:
  method: true
  api: true
defaults:
  formatOptions: -E nodiscard
```

Exemplos de backends com pools virtuais

Nesses arquivos de definição de backend de exemplo, valores padrão específicos são definidos para todos os pools de storage, como `spaceReserve` em `none`, `spaceAllocation` em `false` e `encryption` em `false`. Os pools virtuais são definidos na seção de storage.

Trident define rótulos de provisionamento no campo "Comentários". Os comentários são definidos no volume FlexVol; Trident copia todos os rótulos presentes em um pool virtual para o volume de storage durante o provisionamento. Para conveniência, administradores de storage podem definir rótulos por pool virtual e agrupar volumes por rótulo.

Nestes exemplos, alguns pools de storage definem seus próprios `spaceReserve`, `spaceAllocation`, e `encryption` valores, e alguns pools substituem os valores padrão.

▼ Exemplo de ONTAP SAN

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
```

```

defaults:
  spaceAllocation: "false"
  encryption: "false"
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: "40000"
  zone: us_east_1a
  defaults:
    spaceAllocation: "true"
    encryption: "true"
    adaptiveQosPolicy: adaptive-extreme
- labels:
  protection: silver
  creditpoints: "20000"
  zone: us_east_1b
  defaults:
    spaceAllocation: "false"
    encryption: "true"
    qosPolicy: premium
- labels:
  protection: bronze
  creditpoints: "5000"
  zone: us_east_1c
  defaults:
    spaceAllocation: "true"
    encryption: "false"

```

▼ Exemplo de economia ONTAP SAN

```

---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin

```

```

password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
labels:
  store: san_economy_store
region: us_east_1
storage:
  - labels:
      app: oracledb
      cost: "30"
      zone: us_east_1a
      defaults:
        spaceAllocation: "true"
        encryption: "true"
  - labels:
      app: postgresdb
      cost: "20"
      zone: us_east_1b
      defaults:
        spaceAllocation: "false"
        encryption: "true"
  - labels:
      app: mysqldb
      cost: "10"
      zone: us_east_1c
      defaults:
        spaceAllocation: "true"
        encryption: "false"
  - labels:
      department: legal
      creditpoints: "5000"
      zone: us_east_1c
      defaults:
        spaceAllocation: "true"
        encryption: "false"

```

▼ Exemplo de NVMe/TCP

```

---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin

```

```
password: <password>
useREST: true
defaults:
  spaceAllocation: "false"
  encryption: "true"
storage:
  - labels:
      app: testApp
      cost: "20"
    defaults:
      spaceAllocation: "false"
      encryption: "false"
```

Mapear back-ends para StorageClasses

As seguintes definições de StorageClass referem-se ao [Exemplos de backends com pools virtuais](#). Usando o campo `parameters.selector`, cada StorageClass indica quais pools virtuais podem ser usados para hospedar um volume. O volume agora possui os aspectos definidos no pool virtual escolhido.

- O `protection-gold` StorageClass corresponde ao primeiro pool virtual no `ontap-san` backend. Este é o único pool que oferece proteção de nível ouro.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- O `protection-not-gold` StorageClass corresponde ao segundo e terceiro pool virtual no `ontap-san` backend. Estes são os únicos pools que oferecem um nível de proteção diferente do gold.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- O `app-mysqldb` StorageClass corresponde ao terceiro pool virtual no `ontap-san-economy` backend. Este é o único pool que oferece configuração de pool de storage para o aplicativo do tipo `mysqldb`.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"

```

- O protection-silver-creditpoints-20k StorageClass corresponde ao segundo pool virtual no ontap-san backend. Este é o único pool que oferece proteção de nível prata e 20000 pontos de crédito.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"

```

- O creditpoints-5k StorageClass corresponde ao terceiro pool virtual no ontap-san backend e ao quarto pool virtual no ontap-san-economy backend. Essas são as únicas ofertas de pool com 5000 creditpoints.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

- O my-test-app-sc StorageClass corresponde ao testAPP pool virtual no ontap-san driver com sanType: nvme. Este é o único pool que oferece testApp.

```

---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: my-test-app-sc
provisioner: csi.trident.netapp.io

```

```
parameters:
  selector: "app=testApp"
  fsType: "ext4"
```

O Trident decide qual pool virtual será selecionado e garante que o requisito de storage seja atendido.

Drivers NAS do ONTAP

Visão geral do driver ONTAP NAS

Saiba mais sobre como configurar um backend ONTAP com os drivers NAS do ONTAP e do Cloud Volumes ONTAP.

Detalhes do driver ONTAP NAS

Trident fornece os seguintes drivers de armazenamento NAS para se comunicar com o ONTAP cluster. Os modos de acesso suportados são: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Driver	Protocolo	volumeMod e	Modos de acesso suportados	Sistemas de arquivos suportados
ontap-nas	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	"", nfs, smb
ontap-nas-economy	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	"", nfs, smb
ontap-nas-flexgroup	NFS SMB	Sistema de arquivos	RWO, ROX, RWX, RWOP	"", nfs, smb

AVISO

- Use `ontap-san-economy` somente se a contagem de uso de volume persistente prevista for maior que "[limites de volume ONTAP suportados](#)".
- Use `ontap-nas-economy` somente se a contagem de uso de volume persistente prevista for maior que "[limites de volume ONTAP suportados](#)" e o driver `ontap-san-economy` não puder ser usado.
- Não utilize `ontap-nas-economy` se você prevê a necessidade de proteção de dados, recuperação de desastres ou mobilidade.
- NetApp não recomenda usar o crescimento automático do FlexVol em todos os drivers ONTAP, exceto `ontap-san`. Como alternativa, Trident oferece suporte ao uso de reserva de snapshot e dimensiona os volumes FlexVol de acordo.

Permissões do usuário

Trident espera ser executado como administrador do ONTAP ou do SVM, normalmente usando o `admin` usuário do cluster ou um `vsadmin` usuário do SVM, ou um usuário com um nome diferente que tenha a mesma função.

Para implantações do Amazon FSx for NetApp ONTAP, Trident espera ser executado como administrador do ONTAP ou do SVM, usando o usuário do cluster `fsxadmin` ou um usuário do SVM `vsadmin`, ou um usuário

com um nome diferente que tenha a mesma função. O `fsxadmin` usuário é um substituto limitado para o usuário administrador do cluster.

OBSERVAÇÃO

Se você usar o `limitAggregateUsage` parâmetro, são necessárias permissões de administrador do cluster. Ao usar Amazon FSx for NetApp ONTAP com Trident, o `limitAggregateUsage` parâmetro não funcionará com as contas de usuário `vsadmin` e `fsxadmin`. A operação de configuração falhará se você especificar este parâmetro.

Embora seja possível criar uma função mais restritiva dentro do ONTAP que um driver Trident possa usar, não recomendamos isso. A maioria das novas versões do Trident chamará APIs adicionais que precisariam ser consideradas, dificultando as atualizações e tornando-as propensas a erros.

Prepare-se para configurar um backend com drivers ONTAP NAS

Compreenda os requisitos, as opções de autenticação e as políticas de exportação para configurar um backend ONTAP com drivers ONTAP NAS. A partir da versão 25.10, o NetApp Trident oferece suporte "[NetApp AFX sistema de storage](#)". NetApp AFX storage systems diferem de outros sistemas ONTAP (ASA, AFF e FAS) na implementação de sua camada de storage. Na configuração do backend do Trident, não é necessário especificar que seu sistema é AFX. Ao selecionar `ontap-nas` como o `storageDriverName`, o Trident detecta automaticamente os sistemas AFX.

OBSERVAÇÃO

Apenas o `ontap-nas` driver (com o protocolo NFS) é compatível com sistemas AFX; o protocolo SMB não é compatível.

Requisitos

- Para todos os backends ONTAP, Trident exige que pelo menos um agregado seja atribuído à SVM.
- Você pode executar mais de um driver e criar classes de armazenamento que apontem para um ou outro. Por exemplo, você pode configurar uma classe Gold que usa o driver `ontap-nas` e uma classe Bronze que usa o `ontap-nas-economy`.
- Todos os seus nós de trabalho do Kubernetes devem ter as ferramentas NFS apropriadas instaladas. Consulte "[aqui](#)" para obter mais detalhes.
- Trident suporta volumes SMB montados em pods executados apenas em nós Windows. Consulte [Prepare-se para provisionar volumes SMB](#) para obter detalhes.

Autenticar o backend ONTAP

Trident oferece dois modos de autenticação de um backend ONTAP.

- Baseado em credenciais: Este modo requer permissões suficientes no backend do ONTAP. Recomenda-se usar uma conta associada a uma função de login de segurança predefinida, como `admin` ou `vsadmin` para garantir a máxima compatibilidade com as versões do ONTAP.
- Baseado em certificado: Este modo requer um certificado instalado no backend para o Trident se comunicar com um cluster ONTAP. Nesse caso, a definição do backend deve conter os valores codificados em Base64 do certificado do cliente, da chave e do certificado da CA confiável, se utilizado (recomendado).

Você pode atualizar os backends existentes para alternar entre métodos baseados em credenciais e baseados em certificados. No entanto, apenas um método de autenticação é suportado por vez. Para mudar para um método de autenticação diferente, você deve remover o método existente da configuração do backend.

AVISO

Se você tentar fornecer **tanto credenciais quanto certificados**, a criação do backend falhará com um erro informando que mais de um método de autenticação foi fornecido no arquivo de configuração.

Ativar autenticação baseada em credenciais

Trident requer as credenciais de um administrador com escopo de SVM/cluster para se comunicar com o backend do ONTAP. Recomenda-se o uso de funções padrão predefinidas, como `admin` ou `vsadmin`. Isso garante a compatibilidade futura com versões do ONTAP que possam expor APIs de recursos a serem usadas por versões futuras do Trident. Uma função de login de segurança personalizada pode ser criada e usada com Trident, mas não é recomendada.

Uma definição de backend de exemplo será semelhante a esta:

YAML

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
    "name": "secret-backend-creds"
  }
}
```

Lembre-se de que a definição do backend é o único local onde as credenciais são armazenadas em texto simples. Após a criação do backend, nomes de usuário/senhas são codificados em Base64 e armazenados

como segredos do Kubernetes. A criação/atualização de um backend é a única etapa que requer conhecimento das credenciais. Assim, trata-se de uma operação exclusiva do administrador, a ser realizada pelo administrador de storage do Kubernetes.

Habilitar autenticação baseada em certificado

Novos e existentes backends podem usar um certificado e se comunicar com o backend do ONTAP. Três parâmetros são necessários na definição do backend.

- `clientCertificate`: Valor codificado em Base64 do certificado do cliente.
- `clientPrivateKey`: Valor codificado em Base64 da chave privada associada.
- `trustedCACertificate`: valor codificado em Base64 do certificado CA confiável. Se uma CA confiável estiver sendo usada, este parâmetro deve ser fornecido. Isso pode ser ignorado se nenhuma CA confiável for usada.

Um fluxo de trabalho típico envolve as seguintes etapas.

Passos

1. Gere um certificado de cliente e uma chave. Ao gerar, defina o Nome Comum (CN) para o usuário ONTAP que será usado para autenticação.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=vsadmin"
```

2. Adicione um certificado de CA confiável ao cluster ONTAP. Isso pode já ter sido configurado pelo administrador de storage. Ignore se nenhuma CA confiável for utilizada.

```
security certificate install -type server -cert-name <trusted-ca-cert-name> -vserver <vserver-name>  
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled  
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca  
<cert-authority>
```

3. Instale o certificado do cliente e a chave (do passo 1) no cluster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-name> -vserver <vserver-name>  
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. Confirme se a função de login de segurança do ONTAP suporta `cert` método de autenticação.

```
security login create -user-or-group-name vsadmin -application ontapi  
-authentication-method cert -vserver <vserver-name>  
security login create -user-or-group-name vsadmin -application http  
-authentication-method cert -vserver <vserver-name>
```

5. Teste a autenticação usando o certificado gerado. Substitua <ONTAP Management LIF> e <vserver name> pelo endereço IP da Management LIF e pelo nome da SVM. Você deve garantir que o LIF tenha sua política de serviço definida como default-data-management.

```
curl -X POST -Lk https://<ONTAP-Management-  
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key  
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp  
xmlns="http://www.netapp.com/filer/admin" version="1.21"  
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Codifique o certificado, a chave e o certificado da CA confiável com Base64.

```
base64 -w 0 k8senv.pem >> cert_base64  
base64 -w 0 k8senv.key >> key_base64  
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Crie o backend usando os valores obtidos na etapa anterior.

```
cat cert-backend-updated.json  
{  
  "version": 1,  
  "storageDriverName": "ontap-nas",  
  "backendName": "NasBackend",  
  "managementLIF": "1.2.3.4",  
  "dataLIF": "1.2.3.8",  
  "svm": "vserver_test",  
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",  
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",  
  "storagePrefix": "myPrefix_"  
}  
  
#Update backend with tridentctl  
tridentctl update backend NasBackend -f cert-backend-updated.json -n  
trident  
  
+-----+-----+-----+-----+  
+-----+-----+  
|   NAME   | STORAGE DRIVER |                               UUID                               |  
STATE | VOLUMES |  
+-----+-----+-----+-----+  
+-----+-----+  
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |  
online |      9 |  
+-----+-----+-----+-----+  
+-----+-----+
```

Atualize os métodos de autenticação ou altere as credenciais

Você pode atualizar um backend existente para usar um método de autenticação diferente ou para rotacionar suas credenciais. Isso funciona nos dois sentidos: backends que utilizam nome de usuário/senha podem ser atualizados para usar certificados; backends que utilizam certificados podem ser atualizados para usar nome de usuário/senha. Para fazer isso, você deve remover o método de autenticação existente e adicionar o novo método de autenticação. Em seguida, use o arquivo `backend.json` atualizado contendo os parâmetros necessários para executar `tridentctl update backend`.

```
cat cert-backend-updated.json
```

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}
```

```
#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident

+-----+-----+-----+
+-----+-----+
| NAME | STORAGE DRIVER | UUID |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online | 9 |
+-----+-----+-----+
+-----+-----+

```

OBSERVAÇÃO

Ao rotacionar senhas, o administrador de storage deve primeiro atualizar a senha do usuário no ONTAP. Em seguida, é feita uma atualização no backend. Ao rotacionar certificados, vários certificados podem ser adicionados ao usuário. O backend é então atualizado para usar o novo certificado, após o que o certificado antigo pode ser excluído do cluster ONTAP.

A atualização do backend não interrompe o acesso aos volumes já criados, nem afeta as conexões de volume feitas posteriormente. Uma atualização bem-sucedida do backend indica que Trident pode se comunicar com

o ONTAP backend e lidar com operações de volume futuras.

Criar função ONTAP personalizada para Trident

Você pode criar uma função de cluster ONTAP com privilégios mínimos para que não precise usar a função de administrador do ONTAP para executar operações no Trident. Ao incluir o nome de usuário em um arquivo de configuração de backend do Trident, o Trident usa a função de cluster ONTAP que você criou para executar as operações.

Consulte "[Gerador de funções personalizadas Trident](#)" para obter mais informações sobre como criar funções personalizadas do Trident.

Usando ONTAP CLI

1. Crie uma nova função usando o seguinte comando:

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

2. Crie um nome de usuário para o usuário do Trident:

```
security login create -username <user_name\> -application ontapi  
-authmethod <password\> -role <name_of_role_in_step_1\> -vserver  
<svm_name\> -comment "user_description"
```

3. Mapeie a função para o usuário:

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod  
<password\>
```

Usando System Manager

Execute as seguintes etapas no ONTAP System Manager:

1. **Crie uma função personalizada:**

- a. Para criar uma função personalizada no nível do cluster, selecione **Cluster > Settings**.

(Ou) Para criar uma função personalizada no nível da SVM, selecione **Storage > Storage VMs > required SVM > Settings > Users and Roles**.

- b. Selecione o ícone de seta (→) ao lado de **Users and Roles**.
- c. Selecione **+Adicionar** em **Roles**.
- d. Defina as regras para a função e clique em **Save**.

2. **Mapeie a função ao usuário Trident:** + Execute as seguintes etapas na página **Usuários e Funções**:

- a. Selecione o ícone Adicionar + em **Usuários**.
- b. Selecione o nome de usuário desejado e selecione uma função no menu suspenso para **Função**.
- c. Clique em **Salvar**.

Consulte as seguintes páginas para obter mais informações:

- "Funções personalizadas para administração do ONTAP" ou "Definir funções personalizadas"
- "Trabalhe com funções e usuários"

Gerenciar políticas de exportação NFS

Trident usa políticas de exportação NFS para controlar o acesso aos volumes que provisiona.

Trident oferece duas opções ao trabalhar com políticas de exportação:

- Trident pode gerenciar dinamicamente a própria política de exportação; nesse modo de operação, o administrador de storage especifica uma lista de blocos CIDR que representam endereços IP admissíveis. Trident adiciona automaticamente os IPs de nó aplicáveis que se enquadram nesses intervalos à política de exportação no momento da publicação. Alternativamente, quando nenhum CIDR é especificado, todos os IPs unicast de escopo global encontrados no nó para o qual o volume está sendo publicado serão adicionados à política de exportação.
- Os administradores de storage podem criar uma política de exportação e adicionar regras manualmente. Trident usa a política de exportação padrão, a menos que um nome de política de exportação diferente seja especificado na configuração.

Gerencie dinamicamente as políticas de exportação

Trident oferece a capacidade de gerenciar dinamicamente políticas de exportação para backends ONTAP. Isso fornece ao administrador de storage a capacidade de especificar um espaço de endereços permitido para os endereços IP dos nós de trabalho, em vez de definir regras explícitas manualmente. Isso simplifica muito o gerenciamento de políticas de exportação; as modificações na política de exportação não exigem mais intervenção manual no cluster de storage. Além disso, isso ajuda a restringir o acesso ao cluster de storage apenas aos nós de trabalho que estão montando volumes e possuem endereços IP no intervalo especificado, oferecendo um gerenciamento detalhado e automatizado.

OBSERVAÇÃO

Não utilize Network Address Translation (NAT) ao usar políticas de exportação dinâmicas. Com NAT, o controlador de storage vê o endereço NAT de frontend e não o endereço IP real do host, portanto, o acesso será negado quando nenhuma correspondência for encontrada nas regras de exportação.

Exemplo

Existem duas opções de configuração que devem ser usadas. Veja um exemplo de definição de backend:

```
---
version: 1
storageDriverName: ontap-nas-economy
backendName: ontap_nas_auto_export
managementLIF: 192.168.0.135
svm: svm1
username: vsadmin
password: password
autoExportCIDRs:
  - 192.168.0.0/24
autoExportPolicy: true
```

OBSERVAÇÃO

Ao usar este recurso, você deve garantir que a junção raiz em sua SVM tenha uma política de exportação previamente criada com uma regra de exportação que permita o bloco CIDR do nó (como a política de exportação padrão). Sempre siga a prática recomendada pela NetApp de dedicar uma SVM ao Trident.

Aqui está uma explicação de como esse recurso funciona usando o exemplo acima:

- `autoExportPolicy` está definido como `true`. Isso indica que Trident cria uma política de exportação para cada volume provisionado com este backend para o `svm1` SVM e lida com a adição e exclusão de regras usando `autoexportCIDsRs` blocos de endereços. Até que um volume seja anexado a um nó, o volume usa uma política de exportação vazia, sem regras, para impedir o acesso indesejado a esse volume. Quando um volume é publicado em um nó, Trident cria uma política de exportação com o mesmo nome da `qtree` subjacente, contendo o endereço IP do nó dentro do bloco CIDR especificado. Esses IPs também serão adicionados à política de exportação usada pelo volume pai `FlexVol`.
 - Por exemplo:
 - UUID do backend `403b5326-8482-40db-96d0-d83fb3f4daec`
 - `autoExportPolicy` definido para `true`
 - prefixo de storage `trident`
 - PVC UUID `a79bcf5f-7b6d-4a40-9876-e2551f159c1c`
 - `qtree` denominada `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` cria uma política de exportação para a `FlexVol` denominada `trident-403b5326-8482-40db96d0-d83fb3f4daec`, uma política de exportação para a `qtree` denominada `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`, e uma política de exportação vazia denominada `trident_empty` no SVM. As regras para a política de exportação da `FlexVol` serão um superconjunto de quaisquer regras contidas nas políticas de exportação da `qtree`. A política de exportação vazia será reutilizada por quaisquer volumes que não estejam anexados.
- `autoExportCIDsRs` contém uma lista de blocos de endereços. Este campo é opcional e ele é definido por padrão como `["0.0.0.0/0", ":::0"]`. Se não for definido, Trident adiciona todos os endereços unicast de escopo global encontrados nos nós de trabalho com publicações.

Neste exemplo, o `192.168.0.0/24` espaço de endereços é fornecido. Isso indica que os IPs dos nós do Kubernetes que se enquadram nesse intervalo de endereços com publicações serão adicionados à política de exportação que o Trident cria. Quando o Trident registra um nó no qual está sendo executado, ele recupera os endereços IP do nó e os compara com os blocos de endereços fornecidos em `autoExportCIDsRs`. No momento da publicação, após filtrar os IPs, o Trident cria as regras da política de exportação para os endereços IP dos clientes do nó para o qual está publicando.

Você pode atualizar `autoExportPolicy` e `autoExportCIDsRs` para backends após criá-los. Você pode adicionar novos CIDRs para um backend que é gerenciado automaticamente ou excluir CIDRs existentes. Tenha cuidado ao excluir CIDRs para garantir que conexões existentes não sejam interrompidas. Você também pode optar por desativar `autoExportPolicy` para um backend e voltar para uma política de exportação criada manualmente. Isso exigirá a configuração do parâmetro `exportPolicy` no seu arquivo de configuração do backend.

Após Trident criar ou atualizar um backend, você pode verificar o backend usando `tridentctl` ou o correspondente `tridentbackend` CRD:

```
./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
```

```

- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
      - 192.168.0.0/24
    autoExportPolicy: true
    backendName: ontap_nas_auto_export
    chapInitiatorSecret: ""
    chapTargetInitiatorSecret: ""
    chapTargetUsername: ""
    chapUsername: ""
    dataLIF: 192.168.0.135
    debug: false
    debugTraceFlags: null
    defaults:
      encryption: "false"
      exportPolicy: <automatic>
      fileType: ext4

```

Quando um nó é removido, Trident verifica todas as políticas de exportação para remover as regras de acesso correspondentes ao nó. Ao remover esse endereço IP do nó das políticas de exportação dos backends gerenciados, Trident impede montagens não autorizadas, a menos que esse endereço IP seja reutilizado por um novo nó no cluster.

Para backends preexistentes, atualizar o backend com `tridentctl update backend` garante que Trident gerencie as políticas de exportação automaticamente. Isso cria duas novas políticas de exportação nomeadas de acordo com o UUID do backend e o nome da qtree quando necessário. Volumes presentes no backend usarão as novas políticas de exportação após serem desmontados e montados novamente.

OBSERVAÇÃO

A exclusão de um backend com políticas de exportação gerenciadas automaticamente excluirá a política de exportação criada dinamicamente. Se o backend for recriado, ele será tratado como um novo backend e resultará na criação de uma nova política de exportação.

Se o endereço IP de um nó ativo for atualizado, você deve reiniciar o pod do Trident nesse nó. Trident então atualizará a política de exportação dos backends que gerencia para refletir essa alteração de IP.

Prepare-se para provisionar volumes SMB

Com um pouco de preparação adicional, você pode provisionar volumes SMB usando `ontap-nas` drivers.

AVISO

Você deve configurar ambos os protocolos NFS e SMB/CIFS na SVM para criar um `ontap-nas-economy` volume SMB para clusters ONTAP locais. A falha ao configurar qualquer um desses protocolos fará com que a criação do volume SMB falhe.

OBSERVAÇÃO

`autoExportPolicy` não é compatível com volumes SMB.

Antes de começar

Antes de poder provisionar volumes SMB, você deve ter o seguinte.

- Um cluster Kubernetes com um nó controlador Linux e pelo menos um nó de trabalho Windows executando Windows Server 2022. Trident suporta volumes SMB montados em pods executados apenas em nós Windows.
- Pelo menos um segredo Trident contendo suas credenciais do Active Directory. Para gerar o segredo `smbcreds`:

```
kubectl create secret generic smbcreds --from-literal username=user  
--from-literal password='password'
```

- Um proxy CSI configurado como um serviço do Windows. Para configurar um `csi-proxy`, consulte ["GitHub: CSI Proxy"](#) ou ["GitHub: CSI Proxy para Windows"](#) para nós do Kubernetes em execução no Windows.

Passos

1. Para o ONTAP local, você pode opcionalmente criar um compartilhamento SMB ou o Trident pode criar um para você.

OBSERVAÇÃO

Os compartilhamentos SMB são necessários para Amazon FSx for ONTAP.

Você pode criar os compartilhamentos administrativos SMB de duas maneiras: usando o ["Microsoft Management Console"](#) snap-in Shared Folders ou usando a ONTAP CLI. Para criar os compartilhamentos SMB usando a ONTAP CLI:

- a. Se necessário, crie a estrutura de caminho de diretórios para o compartilhamento.

O `vserver cifs share create` comando verifica o caminho especificado na opção `-path` durante a criação do compartilhamento. Se o caminho especificado não existir, o comando falha.

- b. Crie um compartilhamento SMB associado à SVM especificada:

```
vserver cifs share create -vserver vserver_name -share-name  
share_name -path path [-share-properties share_properties,...]  
[other_attributes] [-comment text]
```

- c. Verifique se o compartilhamento foi criado:

```
vserver cifs share show -share-name share_name
```

OBSERVAÇÃO

Consulte ["Criar um compartilhamento SMB"](#) para obter detalhes completos.

2. Ao criar o backend, você deve configurar o seguinte para especificar os volumes SMB. Para todas as opções de configuração do backend do FSx para ONTAP, consulte ["Opções e exemplos de configuração do FSx for ONTAP"](#).

Parâmetro	Descrição	Exemplo
smbShare	Você pode especificar uma das seguintes opções: o nome de um compartilhamento SMB criado usando o Microsoft Management Console ou ONTAP CLI; um nome para permitir que o Trident crie o compartilhamento SMB; ou você pode deixar o parâmetro em branco para impedir o acesso comum aos volumes. Este parâmetro é opcional para ONTAP on-premises. Este parâmetro é obrigatório para Amazon FSx for ONTAP backends e não pode ficar em branco.	smb-share
nasType	Deve ser definido como smb. Se for nulo, o padrão é nfs.	smb
securityStyle	Estilo de segurança para novos volumes. Deve ser definido como ntfs ou mixed para volumes SMB.	ntfs ou mixed for SMB volumes
unixPermissions	Modo para novos volumes. Deve ser deixado em branco para volumes SMB.	""

Ativar SMB seguro

A partir da versão 25.06, NetApp Trident oferece suporte ao provisionamento seguro de volumes SMB criados usando `ontap-nas` e `ontap-nas-economy` backends. Quando o SMB seguro está habilitado, você pode fornecer acesso controlado aos compartilhamentos SMB para usuários e grupos de usuários do Active Directory (AD) usando listas de controle de acesso (ACLs).

Pontos a lembrar

- A importação de `ontap-nas-economy` volumes não é suportada.
- Apenas clones somente leitura são suportados para `ontap-nas-economy` volumes.
- Se o Secure SMB estiver ativado, Trident ignorará o compartilhamento SMB mencionado no backend.
- A atualização da anotação PVC, da anotação da storage class e do campo backend não atualiza a ACL de compartilhamento SMB.
- A ACL de compartilhamento SMB especificada na anotação do PVC clonado terá precedência sobre as do PVC de origem.
- Certifique-se de fornecer usuários válidos do Active Directory ao habilitar o SMB seguro. Usuários inválidos não serão adicionados à ACL.
- Se você fornecer o mesmo usuário do AD no backend, na storage class e no PVC com permissões diferentes, a prioridade de permissão será: PVC, storage class e, em seguida, backend.
- Secure SMB é compatível com `ontap-nas` importações de volumes gerenciados e não se aplica a importações de volumes não gerenciados.

Passos

1. Especifique `adAdminUser` em `TridentBackendConfig` conforme mostrado no exemplo a seguir:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
```

```

metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret

```

2. Adicione a anotação na storage class.

Adicione a `trident.netapp.io/smbShareAdUser` anotação à storage class para habilitar SMB seguro sem falhas. O valor de usuário especificado para a anotação `trident.netapp.io/smbShareAdUser` deve ser o mesmo que o nome de usuário especificado no `smbcreds secret`. Você pode escolher um dos seguintes para `smbShareAdUserPermission`: `full_control`, `change` ou `read`. A permissão padrão é `full_control`.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate

```

1. Crie um PVC.

O exemplo a seguir cria um PVC:

```

apiVersion: v1
kind: PersistentVolumeClaim
metadata:

```

```

name: my-pvc4
namespace: trident
annotations:
  trident.netapp.io/snapshotDirectory: "true"
  trident.netapp.io/smbShareAccessControl: |
    read:
      - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc

```

Opções e exemplos de configuração do ONTAP NAS

Crie e utilize os drivers ONTAP NAS com sua instalação do Trident. Esta seção fornece exemplos de configuração de backend e detalhes para mapear backends para StorageClasses. A partir da versão 25.10, o NetApp Trident oferece suporte ["NetApp sistemas de storage AFX"](#). Os sistemas de armazenamento AFX da NetApp diferem de outros sistemas baseados em ONTAP (ASA, AFF e FAS) na implementação de sua camada de storage.

OBSERVAÇÃO

Apenas o `ontap-nas` driver (com protocolo NFS) é compatível com sistemas AFX da NetApp; o protocolo SMB não é compatível.

Opções de configuração do backend

Na configuração do backend do Trident, não é necessário especificar que seu sistema é um NetApp AFX sistema de storage. Ao selecionar `ontap-nas` como o `storageDriverName`, o Trident detecta automaticamente o sistema de storage AFX. Alguns parâmetros de configuração do backend não se aplicam a sistemas de storage AFX.

A partir da versão 26.06, você pode habilitar o posicionamento balanceado do ONTAP para que o ONTAP selecione o agregado para novos volumes. O posicionamento balanceado é necessário para sistemas de storage AFX no ONTAP 9.19.1 ou posterior. Consulte ["Utilize o posicionamento balanceado com os backends ONTAP"](#) para requisitos e exemplos.

A tabela a seguir exibe as opções de configuração do backend:

Parâmetro	Descrição	Padrão
<code>version</code>		Sempre 1

Parâmetro	Descrição	Padrão
storageDriverName	<p>Nome do driver de armazenamento.</p> <p>Não pode ser modificado após a criação. Para atualizar este parâmetro, você deve criar um novo backend.</p> <div> <div>OBSERVAÇÃO</div> <div>Para sistemas NetApp AFX, apenas ontap-nas é suportado.</div> </div>	ontap-nas, ontap-nas-economy, ou ontap-nas-flexgroup
backendName	Nome personalizado ou o storage backend	Nome do driver + "_" + dataLIF
managementLIF	<p>Endereço IP de um cluster ou LIF de gerenciamento de SVM. Um nome de domínio totalmente qualificado (FQDN) pode ser especificado. Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como</p> <p>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Para um switchover MetroCluster perfeito, consulte o Exemplo do MetroCluster.</p>	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	<p>Endereço IP do protocolo LIF. NetApp recomenda especificar dataLIF. Caso não seja fornecido, Trident busca os dataLIFs da SVM. Você pode especificar um nome de domínio totalmente qualificado (FQDN) para ser usado nas operações de montagem NFS, permitindo criar um DNS round-robin para balancear a carga entre vários dataLIFs. Pode ser alterado após a configuração inicial. Consulte . Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como</p> <p>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Omita para MetroCluster. Consulte o Exemplo do MetroCluster.</p>	Endereço especificado ou derivado de SVM, caso não seja especificado (não recomendado)
svm	Máquina virtual de storage a ser usada Omitir para MetroCluster. Consulte o Exemplo do MetroCluster .	Derivado se uma SVM managementLIF for especificada
autoExportPolicy	Ativar a criação e atualização automática de políticas de exportação [Booleano]. Usando as opções autoExportPolicy e autoExportCIDRs, Trident pode gerenciar políticas de exportação automaticamente.	falso
autoExportCIDRs	Lista de CIDRs para filtrar os IPs dos nós do Kubernetes quando autoExportPolicy estiver habilitado. Usando as opções autoExportPolicy e autoExportCIDRs, Trident pode gerenciar políticas de exportação automaticamente.	["0.0.0.0/0", ":::/0"]

Parâmetro	Descrição	Padrão
labels	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes	""
clientCertificate	Valor codificado em Base64 do certificado do cliente. Usado para autenticação baseada em certificado	""
clientPrivateKey	Valor codificado em Base64 da chave privada do cliente. Usado para autenticação baseada em certificado	""
trustedCACertificate	Valor codificado em Base64 do certificado da CA confiável. Opcional. Usado para autenticação baseada em certificado	""
username	Nome de usuário para conectar-se ao cluster/SVM. Usada para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autentique o Trident em um SVM de backend usando credenciais do Active Directory" .	
password	Senha para conectar-se ao cluster/SVM. Usada para autenticação baseada em credenciais. Para autenticação do Active Directory, consulte "Autentique o Trident em um SVM de backend usando credenciais do Active Directory" .	
storagePrefix	<div> <div>Prefixo usado ao provisionar novos volumes no SVM. Não pode ser atualizado após ser definido</div> <div> <div>OBSERVAÇÃO</div> <div> Ao usar o ontap-nas-economy e um storagePrefix com 24 ou mais caracteres, as qtrees não têm o storage prefix incorporado, embora ele esteja presente no nome do volume. </div> </div> </div>	"Trident"

Parâmetro	Descrição	Padrão
aggregate	<p>Agregado para provisionamento (opcional; se definido, deve ser atribuído à SVM). Para o <code>ontap-nas-flexgroup</code> driver, esta opção é ignorada. Se não for atribuído, qualquer um dos agregados disponíveis pode ser usado para provisionar um FlexGroup volume.</p> <div> <div>OBSERVAÇÃO</div> <p>Quando o agregado é atualizado no SVM, ele é atualizado automaticamente no Trident por meio de polling no SVM, sem a necessidade de reiniciar o Trident Controller. Quando você configurou um agregado específico no Trident para provisionar volumes, se o agregado for renomeado ou movido para fora do SVM, o backend é movido para o estado de falha no Trident durante o polling do agregado no SVM. Você deve alterar o agregado para um que esteja presente no SVM ou removê-lo completamente para que o backend volte a ficar online.</p> <p>Não especifique para sistemas de storage AFX.</p> <p>Não especifique quando <code>useBalancedPlacement</code> estiver definido como <code>true</code>.</p> </div>	""
useBalancedPlacement	<p>Delegar a seleção de aggregate para novos volumes ao ONTAP [Booleano]. Requer ONTAP 9.19.1 ou posterior e <code>useREST</code> definido como <code>true</code>. Não pode ser combinado com <code>aggregate</code>.</p> <p>Consulte "Utilize o posicionamento balanceado com os backends ONTAP" para requisitos e exemplos.</p> <p>Se especificado, defina sempre como <code>true</code> para sistemas de storage AFX no ONTAP 9.19.1 ou posterior.</p>	<code>false</code> ; <code>true</code> para sistemas de armazenamento AFX no ONTAP 9.19.1 ou posterior
limitAggregateUsage	<p>O provisionamento falhará se o uso ultrapassar essa porcentagem. Não se aplica ao Amazon FSx para ONTAP. Não especifique para sistemas de storage AFX.</p>	"" (não aplicado por padrão)

Parâmetro	Descrição	Padrão
flexgroupAggregateList	<p>Lista de agregados para provisionamento (opcional; se definida, deve ser atribuída à SVM). Todos os agregados atribuídos à SVM são usados para provisionar um FlexGroup volume. Compatível com o driver de storage ontap-nas-flexgroup.</p> <p>OBSERVAÇÃO</p> <p>Quando a lista de agregados é atualizada no SVM, a lista é atualizada automaticamente no Trident por meio de consultas ao SVM, sem a necessidade de reiniciar o Trident Controller. Quando você configurou uma lista de agregados específica no Trident para provisionar volumes, se a lista de agregados for renomeada ou movida para fora do SVM, o backend será movido para o estado de falha no Trident durante a consulta à lista de agregados do SVM. Você deve alterar a lista de agregados para uma que esteja presente no SVM ou removê-la completamente para que o backend volte a ficar online.</p>	""
limitVolumeSize	O provisionamento falha se o tamanho do volume solicitado for superior a este valor.	"" (não aplicado por padrão)
debugTraceFlags	Sinalizadores de depuração para usar na resolução de problemas. Exemplo, {"api":false, "method":true} não use debugTraceFlags a menos que esteja solucionando problemas e precise de um despejo de log detalhado.	null
nasType	Configurar a criação de volumes NFS ou SMB. As opções são <code>nfs</code> , <code>smb</code> ou <code>null</code> . Definir como <code>null</code> define volumes NFS por padrão. Se especificado, defina sempre como <code>nfs</code> para sistemas de armazenamento AFX.	<code>nfs</code>

Parâmetro	Descrição	Padrão
nfsMountOptions	Lista separada por vírgulas de opções de montagem NFS. As opções de montagem para volumes persistentes do Kubernetes normalmente são especificadas nas classes de armazenamento, mas se nenhuma opção de montagem for especificada em uma classe de armazenamento, o Trident usará as opções de montagem especificadas no arquivo de configuração do backend de storage. Se nenhuma opção de montagem for especificada na classe de armazenamento ou no arquivo de configuração, o Trident não definirá nenhuma opção de montagem em um volume persistente associado.	""
qtreesPerFlexvol	Máximo de Qtrees por FlexVol, deve estar no intervalo [50, 300]	"200"
smbShare	Você pode especificar uma das seguintes opções: o nome de um compartilhamento SMB criado usando o Microsoft Management Console ou ONTAP CLI; um nome para permitir que o Trident crie o compartilhamento SMB; ou você pode deixar o parâmetro em branco para impedir o acesso comum aos volumes. Este parâmetro é opcional para ONTAP on-premises. Este parâmetro é obrigatório para Amazon FSx for ONTAP backends e não pode ficar em branco.	smb-share
useREST	Parâmetro booleano para usar as ONTAP REST APIs. <code>useREST</code> Quando definido como <code>true</code> , Trident usa as ONTAP REST APIs para se comunicar com o backend; quando definido como <code>false</code> , Trident usa chamadas ONTAPI (ZAPI) para se comunicar com o backend. Este recurso requer ONTAP 9.11.1 e versões posteriores. Além disso, a função de login do ONTAP utilizada deve ter acesso ao aplicativo <code>ontapi</code> . Isso é atendido pelas funções predefinidas <code>vsadmin</code> e <code>cluster-admin</code> . A partir da versão 24.06 do Trident e ONTAP 9.15.1 ou posterior, <code>useREST</code> é definido como <code>true</code> por padrão; altere <code>useREST</code> para <code>false</code> para usar chamadas ONTAPI (ZAPI). Se especificado, defina sempre como <code>true</code> para sistemas de armazenamento AFX.	<code>true</code> para ONTAP 9.15.1 ou posterior, caso contrário <code>false</code> .
limitVolumePoolSize	Tamanho máximo solicitável de FlexVol ao usar Qtrees no backend <code>ontap-nas-economy</code> .	"" (não aplicado por padrão)
denyNewVolumePools	Restringe <code>ontap-nas-economy</code> os backends de criarem novos volumes FlexVol para conter seus Qtrees. Somente FlexVols preexistentes são usados para o provisionamento de novos PVs.	

Parâmetro	Descrição	Padrão
adAdminUser	Usuário ou grupo de usuários administradores do Active Directory com acesso total aos compartilhamentos SMB. Use este parâmetro para conceder direitos de administrador ao compartilhamento SMB com controle total.	

Opções de configuração de backend para provisionamento de volumes

Você pode controlar o provisionamento padrão usando essas opções na seção `defaults` do arquivo de configuração. Para um exemplo, veja os exemplos de configuração abaixo.

Parâmetro	Descrição	Padrão
spaceAllocation	Alocação de espaço para Qtrees	"true"
spaceReserve	Modo de reserva de espaço; "none" (fino) ou "volume" (grosso)	"none"
snapshotPolicy	Política do Snapshot a ser usada	"none"
qosPolicy	Grupo de políticas de QoS a ser atribuído aos volumes criados. Escolha uma de qosPolicy ou adaptiveQosPolicy por pool de storage/backend	""
adaptiveQosPolicy	Grupo de políticas de QoS adaptável para atribuir aos volumes criados. Escolha um dos qosPolicy ou adaptiveQosPolicy por pool de storage/backend. Não compatível com ontap-nas-economy.	""
snapshotReserve	Percentual do volume reservado para snapshots	"0" se snapshotPolicy for "none", caso contrário ""
splitOnClone	Separar um clone de seu progenitor no momento da criação	"false"
encryption	Habilite a NetApp Volume Encryption (NVE) no novo volume; o padrão é false. A NVE deve estar licenciada e habilitada no cluster para usar esta opção. Se a NAE estiver habilitada no backend, qualquer volume provisionado no Trident terá a NAE habilitada. Para mais informações, consulte: "Como Trident funciona com NVE e NAE" .	"false"
tieringPolicy	Política de tiering para usar "none"	
unixPermissions	Modo para novos volumes	"777" para volumes NFS; vazio (não aplicável) para volumes SMB
snapshotDir	Controla o acesso ao .snapshot diretório	true, false (Definido explicitamente).
exportPolicy	Política de exportação a ser usada	"default"

Parâmetro	Descrição	Padrão
securityStyle	Estilo de segurança para novos volumes. NFS suporta <code>mixed</code> e <code>unix</code> estilos de segurança. SMB suporta <code>mixed</code> e <code>ntfs</code> estilos de segurança.	NFS default é <code>unix</code> . SMB default é <code>ntfs</code> .
nameTemplate	Modelo para criar nomes de volume personalizados.	""

OBSERVAÇÃO

O uso de grupos de políticas de QoS com Trident requer ONTAP 9.8 ou posterior. Você deve usar um grupo de políticas de QoS não compartilhado e garantir que o grupo de políticas seja aplicado a cada componente individualmente. Um grupo de políticas de QoS compartilhado impõe o limite máximo para a taxa de transferência total de todas as cargas de trabalho.

Exemplos de provisionamento de volume

Aqui está um exemplo com valores padrão definidos:

```
---
version: 1
storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: <password>
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: "10"
```

Para `ontap-nas` e `ontap-nas-flexgroups`, o Trident agora usa um novo cálculo para garantir que o FlexVol seja dimensionado corretamente com a porcentagem de `snapshotReserve` e o PVC. Quando o usuário solicita um PVC, o Trident cria o FlexVol original com mais espaço usando o novo cálculo. Esse cálculo garante que o usuário receba o espaço gravável solicitado no PVC, e não menos espaço do que o solicitado. Antes da v21.07, quando o usuário solicitava um PVC (por exemplo, 5 GiB), com o

snapshotReserve em 50 por cento, ele recebia apenas 2,5 GiB de espaço gravável. Isso ocorre porque o que o usuário solicitava era o volume total e snapshotReserve é uma porcentagem disso. Com o Trident 21.07, o que o usuário solicita é o espaço gravável e o Trident define o número de snapshotReserve como a porcentagem do volume total. Isso não se aplica a ontap-nas-economy. Veja o exemplo a seguir para ver como isso funciona:

O cálculo é o seguinte:

```
Total volume size = <PVC requested size> / (1 - (<snapshotReserve percentage> / 100))
```

Para snapshotReserve = 50%, e solicitação de PVC = 5 GiB, o tamanho total do volume é $5/0,5 = 10$ GiB e o tamanho disponível é 5 GiB, que é o que o usuário solicitou na solicitação de PVC. O comando `volume show` deve exibir resultados semelhantes a este exemplo:

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

2 entries were displayed.

Os backends existentes de instalações anteriores provisionam volumes conforme explicado acima ao atualizar o Trident. Para volumes que você criou antes da atualização, você deve redimensionar esses volumes para que a alteração seja observada. Por exemplo, um PVC de 2 GiB com snapshotReserve=50 anteriormente resultava em um volume que fornece 1 GiB de espaço gravável. Redimensionar o volume para 3 GiB, por exemplo, fornece ao aplicativo 3 GiB de espaço gravável em um volume de 6 GiB.

Exemplos de configuração mínima

Os exemplos a seguir mostram configurações básicas que deixam a maioria dos parâmetros com os valores padrão. Esta é a maneira mais fácil de definir um backend.

OBSERVAÇÃO

Se você estiver usando Amazon FSx no NetApp ONTAP com Trident, a recomendação é especificar nomes DNS para LIFs em vez de endereços IP.

▼ Exemplo de economia ONTAP NAS

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

▼ Exemplo de FlexGroup ONTAP NAS

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

▼ Exemplo do MetroCluster

Você pode configurar o backend para evitar ter que atualizar manualmente a definição do backend após switchover e switchback durante ["Replicação e recuperação de SVM"](#).

Para switchover e switchback sem interrupções, especifique a SVM usando `managementLIF` e omita os parâmetros `dataLIF` e `svm`. Por exemplo:

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 192.168.1.66
username: vsadmin
password: password
```

▼ Exemplo de volumes SMB

```
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
nasType: smb
securityStyle: ntfs
unixPermissions: ""
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
```

▼ Exemplo de autenticação baseada em certificado

Este é um exemplo mínimo de configuração de backend. `clientCertificate`, `clientPrivateKey` e `trustedCACertificate` (opcional, se estiver usando uma CA confiável) são preenchidos em `backend.json` e recebem os valores codificados em base64 do certificado do cliente, da chave privada e do certificado da CA confiável, respectivamente.

```

---
version: 1
backendName: DefaultNASBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.15
svm: nfs_svm
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_

```

▼ Exemplo de política de exportação automática

Este exemplo mostra como você pode instruir Trident a usar políticas de exportação dinâmicas para criar e gerenciar a política de exportação automaticamente. Isso funciona da mesma forma para os `ontap-nas-economy` e `ontap-nas-flexgroup` drivers.

```

---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4

```

▼ Exemplo de colocação equilibrada

Este exemplo habilita o posicionamento balanceado do ONTAP, de forma que o ONTAP selecione o agregado para novos volumes. O posicionamento balanceado requer o ONTAP 9.19.1 ou posterior. Consulte ["Utilize o posicionamento balanceado com os backends ONTAP"](#) para obter detalhes.

```

---
version: 1
storageDriverName: ontap-nas
backendName: nas-balanced-placement
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2

```

```
svm: svm_nfs
username: vsadmin
password: password
useBalancedPlacement: true
```

▼ Exemplo de endereços IPv6

Este exemplo mostra managementLIF usando um endereço IPv6.

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas_ipv6_backend
managementLIF: "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]"
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-ontap-ipv6
svm: nas_ipv6_svm
username: vsadmin
password: password
```

▼ Amazon FSx para ONTAP usando exemplo de volumes SMB

O smbShare parâmetro é necessário para Amazon FSx para ONTAP usando volumes SMB.

```
---
version: 1
backendName: SMBBackend
storageDriverName: ontap-nas
managementLIF: example.mgmt.fqdn.aws.com
nasType: smb
dataLIF: 10.0.0.15
svm: nfs_svm
smbShare: smb-share
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
storagePrefix: myPrefix_
```

▼ Exemplo de configuração de backend com nameTemplate

```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap-nas-backend
managementLIF: <ip address>
```

```

svm: svm0
username: <admin>
password: <password>
defaults:
  nameTemplate:
    "{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.vo\
      lume.RequestName}}"
labels:
  cluster: ClusterA
  PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"

```

Exemplos de backends com pools virtuais

Nos arquivos de definição de backend de exemplo mostrados abaixo, valores padrão específicos são definidos para todos os pools de storage, como `spaceReserve` em `none`, `spaceAllocation` em `false` e `encryption` em `false`. Os pools virtuais são definidos na seção de storage.

Trident define rótulos de provisionamento no campo "Comentários". Os comentários são definidos em FlexVol para `ontap-nas` ou `FlexGroup` para `ontap-nas-flexgroup`. Trident copia todos os rótulos presentes em um pool virtual para o volume de armazenamento durante o provisionamento. Para conveniência, administradores de storage podem definir rótulos por pool virtual e agrupar volumes por rótulo.

Nestes exemplos, alguns pools de storage definem seus próprios `spaceReserve`, `spaceAllocation`, e `encryption` valores, e alguns pools substituem os valores padrão.

▼ Exemplo de ONTAP NAS

```

---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: "false"
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      app: msoffice
      cost: "100"
      zone: us_east_1a

```

```

defaults:
  spaceReserve: volume
  encryption: "true"
  unixPermissions: "0755"
  adaptiveQosPolicy: adaptive-premium
- labels:
  app: slack
  cost: "75"
zone: us_east_1b
defaults:
  spaceReserve: none
  encryption: "true"
  unixPermissions: "0755"
- labels:
  department: legal
  creditpoints: "5000"
zone: us_east_1b
defaults:
  spaceReserve: none
  encryption: "true"
  unixPermissions: "0755"
- labels:
  app: wordpress
  cost: "50"
zone: us_east_1c
defaults:
  spaceReserve: none
  encryption: "true"
  unixPermissions: "0775"
- labels:
  app: mysqlldb
  cost: "25"
zone: us_east_1d
defaults:
  spaceReserve: volume
  encryption: "false"
  unixPermissions: "0775"

```

▼ Exemplo de ONTAP NAS FlexGroup

```

---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin

```

```

password: <password>
defaults:
  spaceReserve: none
  encryption: "false"
labels:
  store: flexgroup_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      protection: gold
      creditpoints: "50000"
      zone: us_east_1a
      defaults:
        spaceReserve: volume
        encryption: "true"
        unixPermissions: "0755"
  - labels:
      protection: gold
      creditpoints: "30000"
      zone: us_east_1b
      defaults:
        spaceReserve: none
        encryption: "true"
        unixPermissions: "0755"
  - labels:
      protection: silver
      creditpoints: "20000"
      zone: us_east_1c
      defaults:
        spaceReserve: none
        encryption: "true"
        unixPermissions: "0775"
  - labels:
      protection: bronze
      creditpoints: "10000"
      zone: us_east_1d
      defaults:
        spaceReserve: volume
        encryption: "false"
        unixPermissions: "0775"

```

▼ Exemplo de economia ONTAP NAS

```

---
version: 1

```

```
storageDriverName: ontap-nas-economy
```

```
managementLIF: 10.0.0.1
```

```
svm: svm_nfs
```

```
username: vsadmin
```

```
password: <password>
```

```
defaults:
```

```
    spaceReserve: none
```

```
    encryption: "false"
```

```
labels:
```

```
    store: nas_economy_store
```

```
region: us_east_1
```

```
storage:
```

```
  - labels:
```

```
    department: finance
```

```
    creditpoints: "6000"
```

```
    zone: us_east_1a
```

```
    defaults:
```

```
      spaceReserve: volume
```

```
      encryption: "true"
```

```
      unixPermissions: "0755"
```

```
  - labels:
```

```
    protection: bronze
```

```
    creditpoints: "5000"
```

```
    zone: us_east_1b
```

```
    defaults:
```

```
      spaceReserve: none
```

```
      encryption: "true"
```

```
      unixPermissions: "0755"
```

```
  - labels:
```

```
    department: engineering
```

```
    creditpoints: "3000"
```

```
    zone: us_east_1c
```

```
    defaults:
```

```
      spaceReserve: none
```

```
      encryption: "true"
```

```
      unixPermissions: "0775"
```

```
  - labels:
```

```
    department: humanresource
```

```
    creditpoints: "2000"
```

```
    zone: us_east_1d
```

```
    defaults:
```

```
      spaceReserve: volume
```

```
      encryption: "false"
```

```
      unixPermissions: "0775"
```

Mapear back-ends para StorageClasses

As seguintes definições de StorageClass referem-se a [Exemplos de backends com pools virtuais](#). Usando o campo `parameters.selector`, cada StorageClass indica quais pools virtuais podem ser usados para hospedar um volume. O volume possui os aspectos definidos no pool virtual escolhido.

- O `protection-gold` StorageClass corresponde ao primeiro e ao segundo pool virtual no `ontap-nas-flexgroup` backend. Esses são os únicos pools que oferecem proteção de nível ouro.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=gold"
  fsType: "ext4"
```

- O `protection-not-gold` StorageClass corresponde ao terceiro e quarto pool virtual no `ontap-nas-flexgroup` backend. Estes são os únicos pools que oferecem um nível de proteção diferente do gold.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
```

- O `app-mysqldb` StorageClass corresponde ao quarto pool virtual no `ontap-nas` backend. Este é o único pool que oferece configuração de pool de storage para aplicativo do tipo `mysqldb`.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
```

- O `protection-silver-creditpoints-20k` StorageClass corresponde ao terceiro pool virtual no `ontap-nas-flexgroup` backend. Este é o único pool que oferece proteção de nível prata e 20000 pontos de crédito.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: csi.trident.netapp.io
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"

```

- O creditpoints-5k StorageClass corresponde ao terceiro pool virtual no ontap-nas backend e ao segundo pool virtual no ontap-nas-economy backend. Essas são as únicas ofertas de pool com 5000 creditpoints.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: csi.trident.netapp.io
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

O Trident decide qual pool virtual será selecionado e garante que o requisito de storage seja atendido.

Atualize dataLIF após a configuração inicial

Você pode alterar o dataLIF após a configuração inicial executando o seguinte comando para fornecer o novo arquivo JSON de backend com o dataLIF atualizado.

```

tridentctl update backend <backend-name> -f <path-to-backend-json-file-
with-updated-dataLIF>

```

OBSERVAÇÃO

Se os PVCs estiverem conectados a um ou mais pods, você deve desligar todos os pods correspondentes e então ligá-los novamente para que o novo dataLIF entre em vigor.

Exemplos seguros de SMB

Configuração de backend com o driver ontap-nas

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas

```

```

    namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret

```

Configuração de backend com o driver ontap-nas-economy

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret

```

Configuração de backend com pool de storage

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:

```

```
- labels:
  app: msoffice
  defaults:
    adAdminUser: tridentADuser
nasType: smb
credentials:
  name: backend-tbc-ontap-invest-secret
```

Exemplo de classe de armazenamento com o driver ontap-nas

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

OBSERVAÇÃO

Certifique-se de adicionar annotations para habilitar o SMB seguro. O SMB seguro não funciona sem as anotações, independentemente das configurações definidas no Backend ou no PVC.

Exemplo de classe de armazenamento com o driver ontap-nas-economy

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
```

```
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Exemplo de PVC com um único usuário AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      change:
        - tridentADtest
      read:
        - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Exemplo de PVC com vários usuários de AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
```

```
- tridentTestuser2
- tridentTestuser3
- tridentADuser2
- tridentADuser3

spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```

Utilize o posicionamento balanceado com os backends ONTAP

Você pode habilitar o posicionamento balanceado do ONTAP nos backends do ONTAP. Com o posicionamento balanceado, o ONTAP seleciona o agregado ideal para cada novo volume, então você não precisa gerenciar a atribuição de agregados no Trident.

Como funciona o posicionamento equilibrado

Por padrão, o Trident descobre os agregados atribuídos a uma SVM, trata cada agregado como um pool de storage e seleciona um agregado ao provisionar um volume.

Ao ativar o posicionamento equilibrado:

- O Trident reporta toda a SVM como um único pool de storage, em vez de reportar agregados individuais.
- O ONTAP seleciona o agregado para cada novo volume e equilibra os volumes entre os agregados disponíveis.
- O Trident cria volumes usando a ONTAP `/application/containers` API REST.

O posicionamento balanceado está disponível para sistemas ONTAP unificados (AFF, FAS e ASA) e NetApp AFX storage systems.

Requisitos

- O backend deve usar o ONTAP 9.19.1 ou posterior.
- O Trident deve se comunicar com o ONTAP usando API REST. O posicionamento balanceado não está disponível com ZAPI.
- A configuração do backend não deve especificar agregados. Você não pode combinar posicionamento balanceado com seleção explícita de agregados.

Valores padrão

O valor padrão de `useBalancedPlacement` depende do sistema de storage:

Sistema de storage	Padrão	Notas
O ONTAP (AFF, FAS, ASA)	false	O Trident seleciona agregados, a menos que você habilite o posicionamento balanceado.
NetApp AFX (ONTAP 9.19.1 ou posterior)	true	É necessário um posicionamento equilibrado. Definir <code>useBalancedPlacement</code> para false causa falha na validação do backend.
NetApp AFX (anterior ao ONTAP 9.19.1)	false	A colocação balanceada não está disponível.

Opção de configuração

Parâmetro	Descrição	Padrão
<code>useBalancedPlacement</code>	Delegar a seleção de agregados para novos volumes ao ONTAP. Defina esta opção na raiz da configuração do backend ou em pools virtuais individuais.	false; true para AFX no ONTAP 9.19.1 ou posterior

Alocação equilibrada com pools virtuais

O sistema de alocação equilibrada funciona com ou sem pools virtuais:

- Sem pools virtuais, o Trident reporta o SVM como um único pool de storage e cria todos os novos volumes usando posicionamento balanceado.
- Com pools virtuais, o Trident reporta os pools virtuais e associa os volumes a eles normalmente. Se o pool virtual correspondente tiver o posicionamento balanceado ativado, o ONTAP seleciona o agregado para o volume.

Defina `useBalancedPlacement` na raiz da configuração do backend para aplicá-la a todos os pools virtuais ou defina em pools virtuais individuais para habilitar seletivamente.

Exemplos

O exemplo a seguir permite o posicionamento balanceado em um backend ONTAP unificado:

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas-balanced-placement
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: cluster-admin
password: <password>
useBalancedPlacement: true
```

O exemplo a seguir permite o posicionamento equilibrado usando `TridentBackendConfig`:

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: nas-balanced-placement
  managementLIF: 10.0.0.1
  svm: trident_svm
  useBalancedPlacement: true
  credentials:
    name: backend-tbc-ontap-nas-secret

```

O exemplo a seguir permite o posicionamento balanceado no `gold` pool virtual apenas. O Trident continua selecionando agregados para volumes que correspondam ao `bronze` pool virtual:

```

---
version: 1
storageDriverName: ontap-nas
backendName: nas-virtual-pools
managementLIF: 10.0.0.1
svm: trident_svm
username: cluster-admin
password: <password>
storage:
- labels:
    performance: gold
  useBalancedPlacement: true
- labels:
    performance: bronze

```

Erros de validação no backend

A criação ou atualização do backend falha nos seguintes casos:

Configuração	Resultado
<code>useBalancedPlacement: true</code> no ONTAP anterior à versão 9.19.1	A validação falhou. Atualize para o ONTAP 9.19.1 ou posterior.
<code>useBalancedPlacement: true</code> em um backend usando ZAPI	A validação falhou. Configure o backend para usar API REST.
<code>useBalancedPlacement: true</code> combinado com agregados específicos	A validação falhou. Remova a configuração do <code>aggregate</code> ou desative o posicionamento balanceado.

Configuração	Resultado
`useBalancedPlacement: false` no AFX com o ONTAP 9.19.1 ou posterior	A validação falhou. É necessário um posicionamento balanceado para o AFX no ONTAP 9.19.1 ou posterior.

Amazon FSx for NetApp ONTAP

Use Trident com Amazon FSx for NetApp ONTAP

"[Amazon FSx for NetApp ONTAP](#)" é um serviço totalmente gerenciado da AWS que executa sistemas de arquivos alimentados pelo sistema operacional de storage NetApp ONTAP. Ele fornece recursos, desempenho e administração do ONTAP com a escalabilidade e simplicidade operacional da AWS. Um sistema de arquivos é o recurso principal no Amazon FSx e é análogo a um cluster ONTAP local. Cada sistema de arquivos contém uma ou mais máquinas virtuais de armazenamento (SVMs), e cada SVM contém um ou mais volumes que armazenam arquivos e diretórios. Essa integração permite que clusters Kubernetes em execução no Amazon Elastic Kubernetes Service (EKS) provisionem volumes persistentes com suporte a ONTAP para cargas de trabalho de bloco e arquivo.

Requisitos

Além de "[Requisitos do Trident](#)", para integrar o FSx for ONTAP com Trident, você precisa de:

- Um cluster Amazon EKS existente ou um cluster Kubernetes autogerenciado com `kubectl` instalado.
- Um sistema de arquivos Amazon FSx for NetApp ONTAP e uma máquina virtual de armazenamento (SVM) existentes que sejam acessíveis a partir dos nós de trabalho do seu cluster.
- Nós de trabalho preparados para "[NFS ou iSCSI](#)".

OBSERVAÇÃO

Certifique-se de seguir os passos de preparação do nó necessários para Amazon Linux e Ubuntu "[Amazon Machine Images](#)" (AMIs), dependendo do seu tipo de AMI do EKS.

Considerações

- Volumes SMB:
 - Os volumes SMB são suportados usando apenas o driver `ontap-nas`.
 - Os volumes SMB não são suportados com o Trident EKS add-on.
 - Trident suporta volumes SMB montados em pods executados apenas em nós Windows. Consulte "[Prepare-se para provisionar volumes SMB](#)" para obter detalhes.
- Antes do Trident 24.02, volumes criados em sistemas de arquivos Amazon FSx que tinham backups automáticos ativados não podiam ser excluídos pelo Trident. Para evitar esse problema no Trident 24.02 ou posterior, especifique o `fsxFilesystemID`, `AWS apiRegion`, `AWS apikey` e `AWS secretKey` no arquivo de configuração do backend para AWS FSx for ONTAP.

OBSERVAÇÃO

Se você estiver especificando uma função do IAM para Trident, poderá omitir a

especificação dos campos `apiRegion`, `apiKey` e `secretKey` para o Trident explicitamente. Para obter mais informações, consulte ["Opções e exemplos de configuração do FSx for ONTAP"](#).

Uso simultâneo do Trident SAN/iSCSI e do driver EBS-CSI

Se você planeja usar drivers `ontap-san` (por exemplo, iSCSI) com AWS (EKS, ROSA, EC2 ou qualquer outra instância), a configuração de multipath necessária nos nós pode entrar em conflito com o driver CSI do Amazon Elastic Block Store (EBS). Para garantir que o multipath funcione sem interferir nos discos EBS no mesmo nó, você precisa excluir EBS da sua configuração de multipath. Este exemplo mostra um ``multipath.conf`` arquivo que inclui as configurações necessárias do Trident, excluindo os discos EBS do multipath:

```
defaults {
    find_multipaths no
}
blacklist {
    device {
        vendor "NVME"
        product "Amazon Elastic Block Store"
    }
}
```

Autenticação

Trident oferece dois modos de autenticação.

- Baseado em credenciais (recomendado): armazena as credenciais com segurança no AWS Secrets Manager. Você pode usar o `fsxadmin` usuário do seu sistema de arquivos ou o `vsadmin` usuário configurado para sua SVM.

AVISO

Trident espera ser executado como um `vsadmin` usuário SVM ou como um usuário com um nome diferente que tenha a mesma função. Amazon FSx for NetApp ONTAP possui um `fsxadmin` usuário que é um substituto limitado para o ONTAP `admin cluster user`. Recomendamos fortemente usar `vsadmin` com Trident.

- Com base em certificado: Trident se comunicará com a SVM no seu sistema de arquivos FSx usando um certificado instalado na sua SVM.

Para obter detalhes sobre como ativar a autenticação, consulte a autenticação para o seu tipo de driver:

- ["ONTAP NAS autenticação"](#)
- ["ONTAP SAN autenticação"](#)

Imagens de Máquina da Amazon (AMIs) testadas

O cluster EKS suporta diversos sistemas operacionais, mas a AWS otimizou determinadas Amazon Machine Images (AMIs) para contêineres e EKS. As seguintes AMIs foram testadas com NetApp Trident 25.02.

AMI	NAS	NAS-economy	iSCSI	iSCSI-economia
AL2023_x86_64_STANDARD	Sim	Sim	Sim	Sim
AL2_x86_64	Sim	Sim	Sim*	Sim*
BOTTLEROCKET_x86_64	Sim**	Sim	N/A	N/A
AL2023_ARM_64_STANDARD	Sim	Sim	Sim	Sim
AL2_ARM_64	Sim	Sim	Sim*	Sim*
BOTTLEROCKET_ARM_64	Sim**	Sim	N/A	N/A

- * Não foi possível excluir o PV sem reiniciar o nó
- ** Não funciona com NFSv3 com Trident versão 25.02.

OBSERVAÇÃO

Se a AMI desejada não estiver listada aqui, isso não significa que ela não seja compatível; significa apenas que ela não foi testada. Esta lista serve como um guia para AMIs que comprovadamente funcionam.

Testes realizados com:

- Versão do EKS: 1.32
- Método de instalação: Helm 25.06 e como um AWS add-On 25.06
- Para NAS, foram testados tanto NFSv3 quanto NFSv4.1.
- Para SAN, apenas iSCSI foi testado, não NVMe-oF.

Testes realizados:

- Criar: classe de armazenamento, pvc, pod
- Excluir: pod, pvc (regular, qtree/lun – econômico, NAS com backup da AWS)

Encontre mais informações

- ["Documentação do Amazon FSx for NetApp ONTAP"](#)
- ["Postagem no blog sobre Amazon FSx for NetApp ONTAP"](#)

Crie uma função do IAM e um segredo da AWS

Você pode configurar pods do Kubernetes para acessar recursos da AWS autenticando-se como uma função do AWS IAM em vez de fornecer credenciais explícitas da AWS.

OBSERVAÇÃO

Para autenticar usando uma função do AWS IAM, você deve ter um cluster Kubernetes implantado usando EKS.

Criar segredo do AWS Secrets Manager

Como Trident emitirá APIs contra um FSx vserver para gerenciar o storage para você, ele precisará de credenciais para isso. A maneira segura de passar essas credenciais é por meio de um segredo do AWS Secrets Manager. Portanto, se você ainda não tiver um, precisará criar um segredo do AWS Secrets Manager que contenha as credenciais da conta vsadmin.

Este exemplo cria um segredo do AWS Secrets Manager para armazenar credenciais do Trident CSI:

```
aws secretsmanager create-secret --name trident-secret --description
"Trident CSI credentials"\
  --secret-string
"{\"username\": \"vsadmin\", \"password\": \"<svmpassword>\"}"
```

Criar política de IAM

Trident também precisa de permissões da AWS para funcionar corretamente. Portanto, você precisa criar uma política que conceda ao Trident as permissões de que ele precisa.

Os exemplos a seguir criam uma política do IAM usando a AWS CLI:

```
aws iam create-policy --policy-name AmazonFSxNCSIDriverPolicy --policy
-document file://policy.json
  --description "This policy grants access to Trident CSI to FSxN and
Secrets manager"
```

Exemplo de JSON de policy:

```
{
  "Statement": [
    {
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:CreateVolume",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:UntagResource",
        "fsx:UpdateVolume",
        "fsx:TagResource",
        "fsx>DeleteVolume"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
  ],
}
```

```

    "Action": "secretsmanager:GetSecretValue",
    "Effect": "Allow",
    "Resource": "arn:aws:secretsmanager:<aws-region>:<aws-account-id>:secret:<aws-secret-manager-name>*"
  }
],
"Version": "2012-10-17"
}

```

Criar identidade de Pod ou função IAM para associação de conta de serviço (IRSA)

Você pode configurar uma conta de serviço do Kubernetes para assumir uma função do AWS Identity and Access Management (IAM) com EKS Pod Identity ou IAM role for Service account association (IRSA). Quaisquer Pods configurados para usar a conta de serviço podem então acessar qualquer serviço da AWS ao qual a função tenha permissões de acesso.

Identidade do Pod

As associações de identidade de pods do Amazon EKS permitem gerenciar credenciais para seus aplicativos, de forma semelhante à maneira como os perfis de instância do Amazon EC2 fornecem credenciais para instâncias do Amazon EC2.

Instale o Pod Identity no seu cluster EKS:

Você pode criar uma identidade de Pod via console da AWS ou usando o seguinte comando da AWS CLI:

```

aws eks create-addon --cluster-name <EKS_CLUSTER_NAME> --addon-name
eks-pod-identity-agent

```

Para obter mais informações, consulte ["Configure o agente de identidade do Amazon EKS Pod"](#).

Crie trust-relationship.json:

Crie o arquivo trust-relationship.json para permitir que o EKS Service Principal assuma essa função para Pod Identity. Em seguida, crie uma função com esta trust policy:

```

aws iam create-role \
  --role-name fsxn-csi-role --assume-role-policy-document file://trust-
relationship.json \
  --description "fsxn csi pod identity role"

```

arquivo trust-relationship.json:

```

{
  "Version": "2012-10-17",
  "Statement": [

```

```
{
  "Effect": "Allow",
  "Principal": {
    "Service": "pods.eks.amazonaws.com"
  },
  "Action": [
    "sts:AssumeRole",
    "sts:TagSession"
  ]
}
```

Anexe a política de função à função do IAM:

Anexe a política de função da etapa anterior à função IAM que foi criada:

```
aws iam attach-role-policy \
  --policy-arn arn:aws:iam::aws:111122223333:policy/fsxn-csi-policy \
  --role-name fsxn-csi-role
```

Crie uma associação de identidade de pod:

Crie uma associação de identidade de pod entre a função IAM e a conta de serviço Trident (trident-controller)

```
aws eks create-pod-identity-association \
  --cluster-name <EKS_CLUSTER_NAME> \
  --role-arn arn:aws:iam::111122223333:role/fsxn-csi-role \
  --namespace trident --service-account trident-controller
```

Função IAM para associação de conta de serviço (IRSA)

Usando a AWS CLI:

```
aws iam create-role --role-name AmazonEKS_FSxN_CSI_DriverRole \
  --assume-role-policy-document file:///trust-relationship.json
```

Arquivo trust-relationship.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Principal": {
      "Federated": "arn:aws:iam::<account_id>:oidc-
provider/<oidc_provider>"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "<oidc_provider>:aud": "sts.amazonaws.com",
        "<oidc_provider>:sub":
"system:serviceaccount:trident:trident-controller"
      }
    }
  }
]
}

```

Atualize os seguintes valores no arquivo `trust-relationship.json`:

- **<account_id>** - Seu ID de conta da AWS
- **<oidc_provider>** - O OIDC do seu cluster EKS. Você pode obter o `oidc_provider` executando:

```

aws eks describe-cluster --name my-cluster --query
"cluster.identity.oidc.issuer"\
--output text | sed -e "s/^https:\\/\\/\\/"

```

Associe a função IAM à política IAM:

Depois que a função for criada, associe a política (que foi criada na etapa acima) à função usando este comando:

```

aws iam attach-role-policy --role-name my-role --policy-arn <IAM policy
ARN>

```

Verifique se o provedor do OICD está associado:

Verifique se o seu provedor OIDC está associado ao seu cluster. Você pode verificar isso usando este comando:

```

aws iam list-open-id-connect-providers | grep $oidc_id | cut -d "/" -f4

```

Se a saída estiver vazia, use o seguinte comando para associar IAM OIDC ao seu cluster:

```

eksctl utils associate-iam-oidc-provider --cluster $cluster_name

```

--approve

Se você estiver usando o **eksctl**, use o exemplo a seguir para criar uma função IAM para conta de serviço no EKS:

```
eksctl create iamserviceaccount --name trident-controller --namespace
trident \
  --cluster <my-cluster> --role-name AmazonEKS_FSxN_CSI_DriverRole
--role-only \
  --attach-policy-arn <IAM-Policy ARN> --approve
```

Instale Trident

Trident simplifica o gerenciamento de storage do Amazon FSx for NetApp ONTAP no Kubernetes para permitir que seus desenvolvedores e administradores se concentrem na implantação de aplicativos. Você pode instalar Trident usando um dos seguintes métodos:

- Helm
- Complemento do EKS

Se você deseja utilizar a funcionalidade de instantâneo, instale o complemento do controlador de instantâneo CSI. Consulte ["Ative a funcionalidade de instantâneo para volumes CSI"](#) para obter mais informações.

Instale Trident via helm

Identidade do Pod

1. Adicione o repositório Trident:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-
chart
```

2. Instale Trident usando o seguinte exemplo:

```
helm install trident-operator netapp-trident/trident-operator
--version 100.2502.1 --namespace trident --create-namespace
```

Você pode usar o `helm list` comando para revisar detalhes da instalação, como nome, namespace, chart, status, versão do aplicativo e número da revisão.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14
14:31:22.463122 +0300 IDT		deployed	trident-operator-
100.2502.0	25.02.0		

Associação de conta de serviço (IRSA)

1. Adicione o repositório Trident:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Defina os valores para **provedor de nuvem e identidade de nuvem**:

```
helm install trident-operator netapp-trident/trident-operator
--version 100.2502.1 \
--set cloudProvider="AWS" \
--set cloudIdentity="'eks.amazonaws.com/role-arn:
arn:aws:iam::<accountID>:role/<AmazonEKS_FSxN_CSI_DriverRole>' " \
--namespace trident \
--create-namespace
```

Você pode usar o `helm list` comando para revisar detalhes da instalação, como nome, namespace, chart, status, versão do aplicativo e número da revisão.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14
14:31:22.463122 +0300 IDT		deployed	trident-operator-
100.2510.0	25.10.0		

OBSERVAÇÃO

Se você pretende usar iSCSI, certifique-se de que o iSCSI esteja habilitado em sua máquina cliente. Se você estiver usando o sistema operacional AL2023 Worker node, é possível automatizar a instalação do cliente iSCSI adicionando o parâmetro `node prep` na instalação do helm:

```
helm install trident-operator netapp-trident/trident-operator --version 100.2502.1 --namespace trident --create-namespace --set nodePrep={iscsi}
```

Instale o Trident via o add-on EKS

O Trident EKS add-on inclui os patches de segurança mais recentes, correções de bugs e é validado pela AWS para funcionar com o Amazon EKS. O EKS add-on permite garantir de forma consistente que seus clusters Amazon EKS estejam seguros e estáveis e reduz a quantidade de trabalho necessária para instalar, configurar e atualizar add-ons.

Pré-requisitos

Certifique-se de ter o seguinte antes de configurar o add-on Trident para AWS EKS:

- Uma conta de cluster Amazon EKS com assinatura adicional
- Permissões da AWS para o AWS marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Tipo de AMI: Amazon Linux 2 (AL2_x86_64) ou Amazon Linux 2 Arm(AL2_ARM_64)
- Tipo de nó: AMD ou ARM
- Um sistema de arquivos Amazon FSx for NetApp ONTAP existente

Habilite o complemento Trident para AWS

Console de gerenciamento

1. Abra o console do Amazon EKS em <https://console.aws.amazon.com/eks/home#/clusters>.
2. No painel de navegação à esquerda, selecione **Clusters**.
3. Selecione o nome do cluster para o qual deseja configurar o complemento Trident CSI da NetApp.
4. Selecione **Complementos** e depois selecione **Obter mais complementos**.
5. Siga estes passos para selecionar o software complementar:
 - a. Desça a página até a seção **Complementos do AWS Marketplace** e digite **"Trident"** na caixa de pesquisa.
 - b. Selecione a caixa de seleção no canto superior direito da caixa Trident by NetApp.
 - c. Selecione **Next**.
6. Na página de configurações **Configurar add-ons selecionados**, faça o seguinte:

OBSERVAÇÃO Ignore estas etapas se estiver usando a associação de Pod Identity.

- a. Selecione a **Version** que deseja usar.
- b. Se você estiver usando autenticação IRSA, certifique-se de definir os valores de configuração disponíveis nas configurações opcionais:

- Selecione a **Version** que deseja usar.
- Siga o **esquema de configuração do complemento** e defina o parâmetro **configurationValues** na seção **Valores de configuração** para o role-arn que você criou na etapa anterior (o valor deve estar no seguinte formato):

```
{
  "cloudIdentity": "'eks.amazonaws.com/role-arn: <role ARN>'",
  "cloudProvider": "AWS"
}
```

+

Se você selecionar Override como método de resolução de conflitos, uma ou mais configurações do add-on existente poderão ser substituídas pelas configurações do add-on do Amazon EKS. Se você não habilitar esta opção e houver um conflito com suas configurações existentes, a operação falhará. Você pode usar a mensagem de erro resultante para solucionar o conflito. Antes de selecionar esta opção, certifique-se de que o add-on do Amazon EKS não gerencie configurações que você precise gerenciar manualmente.

7. Escolha **Próximo**.

8. Na página **Revisar e adicionar**, escolha **Criar**.

Após a conclusão da instalação do complemento, você verá o complemento instalado.

AWS CLI

1. Crie o `add-on.json` arquivo:

Para Pod Identity, utilize o seguinte formato:

OBSERVAÇÃO Use o

```
{
  "clusterName": "<eks-cluster>",
  "addonName": "netapp_trident-operator",
  "addonVersion": "v25.6.0-eksbuild.1",
}
```

Para autenticação IRSA, utilize o seguinte formato:

```
{
  "clusterName": "<eks-cluster>",
  "addonName": "netapp_trident-operator",
  "addonVersion": "v25.6.0-eksbuild.1",
  "serviceAccountRoleArn": "<role ARN>",
  "configurationValues": {
```

```
"cloudIdentity": "'eks.amazonaws.com/role-arn: <role ARN>'",  
"cloudProvider": "AWS"  
}  
}
```

OBSERVAÇÃO

Substitua <role ARN> pelo ARN da função que foi criada na etapa anterior.

2. Instale o complemento Trident EKS.

```
aws eks create-addon --cli-input-json file://add-on.json
```

eksctl

O seguinte comando de exemplo instala o Trident EKS add-on:

```
eksctl create addon --name netapp_trident-operator --cluster  
<cluster_name> --force
```

Atualize o complemento Trident EKS

Console de gerenciamento

1. Abra o console do Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters>.
2. No painel de navegação à esquerda, selecione **Clusters**.
3. Selecione o nome do cluster para o qual deseja atualizar o software complementar NetApp Trident CSI.
4. Selecione a guia **Add-ons**.
5. Selecione **Trident por NetApp** e depois selecione **Editar**.
6. Na página **Configurar Trident por NetApp**, faça o seguinte:
 - a. Selecione a **Version** que deseja usar.
 - b. Expanda as **Configurações opcionais de configuração** e modifique conforme necessário.
 - c. Selecione **Salvar alterações**.

AWS CLI

O exemplo a seguir atualiza o add-on EKS:

```
aws eks update-addon --cluster-name <eks_cluster_name> --addon-name  
netapp_trident-operator --addon-version v25.6.0-eksbuild.1 \  
--service-account-role-arn <role-ARN> --resolve-conflict preserve \  
--configuration-values "{\"cloudIdentity\":  
\"'eks.amazonaws.com/role-arn: <role ARN>'\"}"
```

eksctl

- Verifique a versão atual do seu FSxN Trident CSI add-on. Substitua `my-cluster` pelo nome do seu cluster.

```
eksctl get addon --name netapp_trident-operator --cluster my-cluster
```

Exemplo de saída:

NAME	VERSION	STATUS	ISSUES
IAMROLE	UPDATE AVAILABLE	CONFIGURATION VALUES	
netapp_trident-operator	v25.6.0-eksbuild.1	ACTIVE	0
{ "cloudIdentity": "'eks.amazonaws.com/role-arn:arn:aws:iam::139763910815:role/AmazonEKS_FSXN_CSI_DriverRole'" }			

- Atualize o software complementar para a versão retornada em UPDATE AVAILABLE na saída da etapa anterior.

```
eksctl update addon --name netapp_trident-operator --version  
v25.6.0-eksbuild.1 --cluster my-cluster --force
```

Se você remover a `--force` opção e alguma das configurações do add-on do Amazon EKS entrar em conflito com suas configurações existentes, a atualização do add-on do Amazon EKS falhará; você receberá uma mensagem de erro para ajudá-lo a resolver o conflito. Antes de especificar esta opção, certifique-se de que o add-on do Amazon EKS não gerencie configurações que você precisa gerenciar, pois essas configurações serão sobrescritas com esta opção. Para mais informações sobre outras opções para esta configuração, consulte ["Complementos"](#). Para mais informações sobre o gerenciamento de campos do Kubernetes no Amazon EKS, consulte ["Gerenciamento de campos do Kubernetes"](#).

Desinstalar/remover o Trident EKS add-on

Você tem duas opções para remover um add-on do Amazon EKS:

- **Preservar software complementar no seu cluster** – Esta opção remove o gerenciamento de quaisquer configurações pelo Amazon EKS. Ela também remove a capacidade do Amazon EKS de notificá-lo sobre atualizações e atualizar automaticamente o add-on do Amazon EKS após você iniciar uma atualização. No entanto, ela preserva o software complementar no seu cluster. Esta opção transforma o add-on em uma instalação autogerenciada, em vez de um add-on do Amazon EKS. Com esta opção, não há tempo de inatividade para o add-on. Mantenha a `--preserve` opção no comando para preservar o add-on.
- **Remova o software complementar completamente do seu cluster** – NetApp recomenda que você remova o complemento do Amazon EKS do seu cluster somente se não houver recursos no seu cluster que dependam dele. Remova a `--preserve` opção do comando `delete` para remover o software complementar.

OBSERVAÇÃO

Se o software complementar tiver uma conta IAM associada a ele, a conta IAM não será removida.

Console de gerenciamento

1. Abra o console do Amazon EKS em <https://console.aws.amazon.com/eks/home#/clusters>.
2. No painel de navegação à esquerda, selecione **Clusters**.
3. Selecione o nome do cluster do qual você deseja remover o complemento NetApp Trident CSI.
4. Selecione a aba **Complementos** e depois selecione **Trident by NetApp**.*
5. Selecione **Remove**.
6. Na caixa de diálogo **Remover netapp_trident-operator confirmation**, faça o seguinte:
 - a. Se você deseja que o Amazon EKS pare de gerenciar as configurações do software complementar, selecione **Preservar no cluster**. Faça isso se quiser manter o software complementar no seu cluster para que você possa gerenciar todas as configurações do software complementar por conta própria.
 - b. Digite **netapp_trident-operator**.
 - c. Selecione **Remove**.

AWS CLI

Substitua `my-cluster` pelo nome do seu cluster e, em seguida, execute o seguinte comando.

```
aws eks delete-addon --cluster-name my-cluster --addon-name  
netapp_trident-operator --preserve
```

eksctl

O comando a seguir desinstala o Trident EKS add-on:

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

Configure uma classe de armazenamento

O "[Objeto Kubernetes StorageClass](#)" identifica um provisionador e instrui o provisionador sobre como provisionar volumes. Esta seção mostra como configurar um objeto StorageClass do Kubernetes que especifica Trident como provisionador.

Criar um StorageClass Objeto

Ao criar um StorageClass para FSx for ONTAP, o Trident criará automaticamente a configuração de backend.

OBSERVAÇÃO

Se você deseja configurar manualmente o backend de armazenamento, consulte a [Crie um Kubernetes StorageClass sem configuração automática de backend](#) seção sobre como criar o backend Trident e a classe de armazenamento separadamente.

Especifique os parâmetros necessários de StorageClass

Os três parâmetros a seguir precisam ser definidos ao criar um StorageClass:

Parâmetro	Obrigatório	Tipo	Descrição
fsxFilesystemID	Sim	string	FSx para NetApp ONTAP ID do sistema de arquivos
storageDriverName	Sim	string	Driver de storage Trident (por exemplo, <code>ontap-nas</code> ou <code>ontap-san</code>)
credentialsName	Sim	string	Nome do segredo do Kubernetes que contém as credenciais do FSx for ONTAP

Especifique parâmetros opcionais

Você pode passar parâmetros opcionais para o backend através do StorageClass. Defina todos os valores opcionais como strings na StorageClass `parameters` section. Para obter uma lista completa dos parâmetros de backend, consulte: "[Configuração do backend FSx para NetApp ONTAP](#)".

Exemplo de arquivos de configuração StorageClass.

O exemplo a seguir mostra um StorageClass que aciona a configuração automática do backend.

YAML

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-fsx-demo
  annotations:
    description: "Demo StorageClass for FSx for NetApp ONTAP"
provisioner: csi.trident.netapp.io
parameters:
  fsxFilesystemID: "fs-0abc123"
  storageDriverName: "ontap-nas"
  credentialsName: trident-fsx-credentials
allowVolumeExpansion: true
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

JSON

```
{
  "apiVersion": "storage.k8s.io/v1",
  "kind": "StorageClass",
  "metadata": {
    "name": "ontap-fsx-demo",
    "annotations": {
      "description": "Demo StorageClass for FSx for NetApp ONTAP"
    }
  },
}
```

```

"provisioner": "csi.trident.netapp.io",
"parameters": {
  "fsxFilesystemID": "fs-0abc123",
  "storageDriverName": "ontap-nas",
  "credentialsName": "trident-fsx-credentials"
},
"allowVolumeExpansion": true,
"reclaimPolicy": "Delete",
"volumeBindingMode": "Immediate"
}

```

Crie o StorageClass

Após criar o arquivo de configuração, execute o seguinte comando para criar a storage class.

```
kubectl create -f storage-class-ontapnas.yaml
```

Agora você deverá ver uma classe de storage **basic-csi** tanto no Kubernetes quanto no Trident, e o Trident deverá ter descoberto os pools no backend.

```
kubectl get sc basic-csi
```

NAME	PROVISIONER	AGE
basic-csi	csi.trident.netapp.io	15h

Após aplicar o StorageClass, Trident cria o backend automaticamente. Você pode então criar PersistentVolumeClaims que referenciam esse StorageClass.

Verifique o status da configuração do backend

Trident registra o resultado da criação do backend em anotações de StorageClass.

Anotação	Descrição
trident.netapp.io/configuratorStatus	Resultado da configuração (Success ou Failure)
trident.netapp.io/configuratorMessage	Mensagem detalhada de status ou erro
trident.netapp.io/configuratorName	Nome do recurso interno do configurador
trident.netapp.io/managed	Indica que o StorageClass é gerenciado pela Trident
trident.netapp.io/additionalStoragePools	Pools de storage criados para este backend

Para verificar o status, execute:

```
kubectl get storageclass ontap-fsx-demo -o yaml
```

Confirme que `trident.netapp.io/configuratorStatus` está definido como `Success`. Se o valor for `Failure`, revise `trident.netapp.io/configuratorMessage` para o erro.

Adicionar sistemas de arquivos FSxN adicionais

Se você precisar de capacidade de storage adicional enquanto continua usando o mesmo `StorageClass`, adicione IDs de sistema de arquivos FSxN adicionais.

Edite o `StorageClass` e adicione a seguinte anotação:

```
metadata:
  annotations:
    trident.netapp.io/additionalFsxnFileSystemID: '["fs-
xxxxxxxxxxxxxxxxxxxxxx"] '
```

Após aplicar a alteração, Trident atualiza a configuração do backend e atualiza as anotações de `StorageClass`.

Considerações operacionais e limitações

- Excluir um `StorageClass` que possui a configuração automática de backend geralmente exclui o Trident backend associado. Isso pode interromper a conectividade de storage e interromper cargas de trabalho em execução. Valide o impacto antes de excluir um `StorageClass` gerenciado.
- A configuração automática de backend é suportada apenas para AWS FSx para NetApp ONTAP.

Crie um Kubernetes `StorageClass` sem configuração automática de backend

Se você deseja criar o backend do Trident e o `StorageClass` separadamente, siga estas etapas.

Entenda como funciona a configuração automática do backend

Trident deriva a configuração do backend da definição de `StorageClass`. Quando você aplica o `StorageClass`, Trident valida os parâmetros necessários, cria o backend e anota o `StorageClass` com o status.

Trident cria o `VolumeSnapshotClass` apenas uma vez. Trident reutiliza o mesmo `VolumeSnapshotClass` para `StorageClasses` subsequentes.

Crie o backend do Trident

Para criar um backend Trident, você precisa criar um arquivo de configuração em formato JSON ou YAML. O arquivo deve especificar o tipo de storage desejado (NAS ou SAN), o sistema de arquivos, a SVM de onde obtê-lo e como autenticar com ela. O exemplo a seguir mostra como definir um storage baseado em NAS e usar um segredo da AWS para armazenar as credenciais da SVM que você deseja usar:

YAML

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
```

```

metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFileSystemID: fs-xxxxxxxxxx
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name"
    type: awsarn

```

JSON

```

{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas"
    "namespace": "trident"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
      "fsxFileSystemID": "fs-xxxxxxxxxx"
    },
    "managementLIF": null,
    "credentials": {
      "name": "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name",
      "type": "awsarn"
    }
  }
}

```

Detalhes do driver FSx for ONTAP

Você pode integrar Trident com Amazon FSx for NetApp ONTAP usando os seguintes drivers:

Nome do driver	Descrição
ontap-san	Cada PV provisionado é um LUN dentro de seu próprio volume Amazon FSx for NetApp ONTAP. Recomendado para armazenamento em bloco.
ontap-nas	Cada PV provisionado é um volume completo do Amazon FSx for NetApp ONTAP. Recomendado para NFS e SMB.
ontap-san-economy	Cada PV provisionado é um LUN com um número configurável de LUNs por Amazon FSx for NetApp ONTAP volume.
ontap-nas-economy	Cada PV provisionado é uma qtree, com um número configurável de qtrees por volume do Amazon FSx for NetApp ONTAP.
ontap-nas-flexgroup	Cada PV provisionado é um volume completo do Amazon FSx for NetApp ONTAP FlexGroup.

Para obter detalhes sobre o driver, consulte ["Drivers NAS"](#) e ["Drivers SAN"](#).

Criar o backend

Após criar o arquivo de configuração, execute os seguintes comandos para criar e validar a Trident Backend Configuration (TBC):

- Crie a configuração de backend do Trident (TBC) a partir do arquivo yaml e execute o seguinte comando:

```
kubectl create -f backendconfig.yaml -n trident
```

```
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-nas created
```

- Valide se a configuração do backend Trident (TBC) foi criada com sucesso:

```
Kubectl get tbc -n trident
```

NAME	BACKEND NAME	BACKEND UUID
PHASE STATUS		
backend-tbc-ontap-nas	tbc-ontap-nas	933e0071-66ce-4324-
b9ff-f96d916ac5e9 Bound	Success	

Para obter mais informações sobre outras opções de configuração, consulte a [Configuração avançada do backend e exemplos](#) seção abaixo.

Configurar uma Storage Class sem configuração automática de backend

A seguir, apresentamos exemplos de configurações de Storage Class para uso com Trident e FSx for ONTAP.

Classe de armazenamento para NFS

Você pode usar este exemplo para configurar StorageClass para volumes usando NFS (consulte a seção de Atributos do Trident abaixo para obter a lista completa de atributos):

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  provisioningType: "thin"
  snapshots: "true"
```

Classe de armazenamento para iSCSI

Use este exemplo para configurar StorageClass para volumes usando iSCSI:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  provisioningType: "thin"
  snapshots: "true"
```

Classe de armazenamento usando NFSv3 e AWS Bottlerocket

Para provisionar volumes NFSv3 no AWS Bottlerocket, adicione o `mountOptions` necessário à classe de armazenamento:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
mountOptions:
```

- nfsvers=3
- nolock

Atributos do Trident StorageClass

Esses parâmetros determinam quais pools de storage gerenciados pelo Trident devem ser utilizados para provisionar volumes de um determinado tipo.

Atributo	Tipo	Valores	Oferta	Solicitação	Apoiado por
mídia ¹	string	hdd, híbrido, ssd	O pool contém mídias deste tipo; híbrido significa ambos	Tipo de mídia especificado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
provisioningType	string	fino, grosso	Pool suporta este método de provisionamento	Método de provisionamento especificado	espeço: all ontap; fino: all ontap & solidfire-san
backendType	string	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, azure-netapp-files, ontap-san-economy	Pool pertence a este tipo de backend	Backend especificado	Todos os drivers
instantâneos	bool	true, false	O pool suporta volumes com snapshots	Volume com snapshots ativados	ontap-nas, ontap-san, solidfire-san
clones	bool	true, false	Pool suporta clonagem de volumes	Volume com clonagem ativada	ontap-nas, ontap-san, solidfire-san
criptografia	bool	true, false	Pool suporta volumes criptografados	Volume com criptografia ativada	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	inteiro	inteiro positivo	O pool é capaz de garantir IOPS nessa faixa	Volume garantiu esses IOPS	solidfire-san

¹: Não suportado pelo ONTAP Select ou FSx for ONTAP systems

Consulte "[Objetos Kubernetes e Trident](#)" para obter detalhes sobre como as classes de armazenamento interagem com o PersistentVolumeClaim e os parâmetros para controlar como Trident provisiona volumes.

Crie a classe de armazenamento

Depois de configurar o StorageClass, você pode criá-lo no Kubernetes.

Passos

1. Este é um objeto do Kubernetes, portanto, use `kubectl` para criá-lo no Kubernetes.

```
kubectl create -f storage-class-ontapas.yaml
```

2. Agora você deverá ver uma classe de storage **basic-csi** tanto no Kubernetes quanto no Trident, e o Trident deverá ter descoberto os pools no backend.

```
kubectl get sc basic-csi
```

NAME	PROVISIONER	AGE
basic-csi	csi.trident.netapp.io	15h

Provisionar volumes SMB

Você pode provisionar volumes SMB usando o `ontap-nas` driver. No entanto, para isso, você deve concluir estas etapas: ["Prepare-se para provisionar volumes SMB"](#).

Configuração avançada do backend e exemplos

Consulte a tabela a seguir para as opções de configuração do backend:

Parâmetro	Descrição	Exemplo
version		Sempre 1
storageDriverName	Nome do driver de armazenamento	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy
backendName	Nome personalizado ou o storage backend	Nome do driver + "_" + dataLIF

Parâmetro	Descrição	Exemplo
managementLIF	Endereço IP de um cluster ou LIF de gerenciamento de SVM. Um nome de domínio totalmente qualificado (FQDN) pode ser especificado. Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Se você fornecer o fsxFilesystemID sob o campo aws, não é necessário fornecer o managementLIF, pois Trident recupera as informações da SVM managementLIF da AWS. Portanto, você deve fornecer credenciais para um usuário na SVM (por exemplo: vsadmin) e o usuário deve ter a função vsadmin.	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	Endereço IP do protocolo LIF. ONTAP NAS drivers: NetApp recomenda especificar dataLIF. Caso não seja fornecido, Trident busca os dataLIFs da SVM. Você pode especificar um nome de domínio totalmente qualificado (FQDN) para ser usado nas operações de montagem NFS, permitindo criar um DNS round-robin para balancear a carga entre vários dataLIFs. Pode ser alterado após a configuração inicial. ONTAP SAN drivers: não especifique para iSCSI. Trident usa ONTAP Selective LUN Map para descobrir os LIFs iSCSI necessários para estabelecer uma sessão multipath. Um aviso é gerado se dataLIF for definido explicitamente. Pode ser configurado para usar endereços IPv6 se Trident foi instalado com o sinalizador IPv6. Os endereços IPv6 devem ser definidos entre colchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	

Parâmetro	Descrição	Exemplo
<code>autoExportPolicy</code>	Ativar a criação e atualização automática de políticas de exportação [Booleano]. Usando as opções <code>autoExportPolicy</code> e <code>autoExportCIDRs</code> , Trident pode gerenciar políticas de exportação automaticamente.	<code>false</code>
<code>autoExportCIDRs</code>	Lista de CIDRs para filtrar os IPs dos nós do Kubernetes quando <code>autoExportPolicy</code> estiver habilitado. Usando as opções <code>autoExportPolicy</code> e <code>autoExportCIDRs</code> , Trident pode gerenciar políticas de exportação automaticamente.	<code>["0.0.0.0/0", "::/0"]</code>
<code>labels</code>	Conjunto de rótulos arbitrários formatados em JSON para aplicar aos volumes	<code>""</code>
<code>clientCertificate</code>	Valor codificado em Base64 do certificado do cliente. Usado para autenticação baseada em certificado	<code>""</code>
<code>clientPrivateKey</code>	Valor codificado em Base64 da chave privada do cliente. Usado para autenticação baseada em certificado	<code>""</code>
<code>trustedCACertificate</code>	Valor codificado em Base64 do certificado da CA confiável. Opcional. Usado para autenticação baseada em certificado.	<code>""</code>
<code>username</code>	Nome de usuário para conectar-se ao cluster ou SVM. Usada para autenticação baseada em credenciais. Por exemplo, <code>vsadmin</code> .	
<code>password</code>	Senha para conectar-se ao cluster ou SVM. Usada para autenticação baseada em credenciais.	
<code>svm</code>	Máquina virtual de storage para usar	Derivado se um SVM managementLIF for especificado.
<code>storagePrefix</code>	Prefixo usado ao provisionar novos volumes no SVM. Não pode ser modificado após a criação. Para atualizar este parâmetro, você precisará criar um novo backend.	<code>trident</code>

Parâmetro	Descrição	Exemplo
limitAggregateUsage	Não especifique para Amazon FSx para NetApp ONTAP. As configurações fornecidas <code>fsxadmin</code> e <code>vsadmin</code> não contêm as permissões necessárias para recuperar o uso agregado e limitá-lo usando Trident.	Não use.
limitVolumeSize	O provisionamento falha se o tamanho do volume solicitado for superior a este valor. Também restringe o tamanho máximo dos volumes que gerencia para <code>qtrees</code> e LUNs, e a <code>qtreesPerFlexvol</code> opção permite personalizar o número máximo de <code>qtrees</code> por FlexVol volume	"" (não aplicado por padrão)
lunsPerFlexvol	LUNs máximas por FlexVol volume, deve estar no intervalo [50, 200]. Somente SAN.	"100"
debugTraceFlags	Sinalizadores de depuração para usar na resolução de problemas. Exemplo, <code>{"api":false, "method":true}</code> não use <code>debugTraceFlags</code> a menos que esteja solucionando problemas e precise de um despejo de log detalhado.	null
nfsMountOptions	Lista separada por vírgulas de opções de montagem NFS. As opções de montagem para volumes persistentes do Kubernetes são normalmente especificadas nas classes de armazenamento, mas se nenhuma opção de montagem for especificada em uma classe de armazenamento, Trident usará as opções de montagem especificadas no arquivo de configuração do backend de storage. Se nenhuma opção de montagem for especificada na classe de armazenamento ou no arquivo de configuração, Trident não definirá nenhuma opção de montagem em um volume persistente associado.	""

Parâmetro	Descrição	Exemplo
<code>nasType</code>	Configurar a criação de volumes NFS ou SMB. As opções são <code>nfs</code> , <code>smb</code> ou <code>null</code> . Deve ser definido como <code>smb</code> para volumes SMB. Definir como <code>null</code> define volumes NFS por padrão.	<code>nfs</code>
<code>qtreesPerFlexvol</code>	Número máximo de <code>qtrees</code> por FlexVol volume, deve estar no intervalo [50, 300]	<code>"200"</code>
<code>smbShare</code>	Você pode especificar uma das seguintes opções: o nome de um compartilhamento SMB criado usando o Microsoft Management Console ou ONTAP CLI, ou um nome para permitir que Trident crie o compartilhamento SMB. Este parâmetro é obrigatório para Amazon FSx for ONTAP backends.	<code>smb-share</code>
<code>useREST</code>	Parâmetro booleano para usar as ONTAP REST APIs. Quando definido como <code>true</code> , Trident usará as ONTAP REST APIs para se comunicar com o backend. Este recurso requer ONTAP 9.11.1 e versões posteriores. Além disso, a função de login do ONTAP utilizada deve ter acesso ao aplicativo <code>ontap</code> . Isso é atendido pelas funções predefinidas <code>vsadmin</code> e <code>cluster-admin</code> .	<code>false</code>
<code>aws</code>	Você pode especificar o seguinte no arquivo de configuração do AWS FSx para ONTAP: - <code>fsxFilesystemID</code> : especificar o ID do sistema de arquivos AWS FSx. - <code>apiRegion</code> : nome da região da API da AWS. - <code>apiKey</code> : chave da API da AWS. - <code>secretKey</code> : chave secreta da AWS.	<code>""</code> <code>""</code> <code>""</code>
<code>credentials</code>	Especifique as credenciais do FSx SVM a serem armazenadas no AWS Secrets Manager. - <code>name</code> : Amazon Resource Name (ARN) do segredo, que contém as credenciais do SVM. - <code>type</code> : Defina como <code>awsarn</code> . Consulte "Crie um segredo do AWS Secrets Manager" para obter mais informações.	

Opções de configuração de backend para provisionamento de volumes

Você pode controlar o provisionamento padrão usando essas opções na seção `defaults` do arquivo de configuração. Para um exemplo, veja os exemplos de configuração abaixo.

Parâmetro	Descrição	Padrão
<code>spaceAllocation</code>	Alocação de espaço para LUNs	<code>true</code>
<code>spaceReserve</code>	Modo de reserva de espaço; "none" (fino) ou "volume" (grosso)	<code>none</code>
<code>snapshotPolicy</code>	Política do Snapshot a ser usada	<code>none</code>
<code>qosPolicy</code>	Grupo de políticas de QoS a ser atribuído aos volumes criados. Escolha uma das opções <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> por pool de storage ou backend. O uso de grupos de políticas de QoS com Trident requer ONTAP 9.8 ou posterior. Você deve usar um grupo de políticas de QoS não compartilhado e garantir que o grupo de políticas seja aplicado a cada componente individualmente. Um grupo de políticas de QoS compartilhado impõe o limite máximo para a taxa de transferência total de todas as cargas de trabalho.	<code>""</code>
<code>adaptiveQosPolicy</code>	Grupo de políticas de QoS adaptável para atribuir aos volumes criados. Escolha uma das opções <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> por pool de storage ou backend. Não compatível com <code>ontap-nas-economy</code> .	<code>""</code>
<code>snapshotReserve</code>	Porcentagem do volume reservada para snapshots "0"	Se <code>snapshotPolicy</code> for <code>none</code> , else <code>""</code>
<code>splitOnClone</code>	Separar um clone de seu progenitor no momento da criação	<code>false</code>
<code>encryption</code>	Habilite a NetApp Volume Encryption (NVE) no novo volume; o padrão é <code>false</code> . A NVE deve estar licenciada e habilitada no cluster para usar esta opção. Se a NAE estiver habilitada no backend, qualquer volume provisionado no Trident terá a NAE habilitada. Para mais informações, consulte: "Como Trident funciona com NVE e NAE" .	<code>false</code>

Parâmetro	Descrição	Padrão
luksEncryption	Ative a criptografia LUKS. Consulte "Use Linux Unified Key Setup (LUKS)" . Somente SAN.	""
tieringPolicy	Política de tiering a ser usada <code>none</code>	
unixPermissions	Modo para novos volumes. Deixe em branco para volumes SMB.	""
securityStyle	Estilo de segurança para novos volumes. NFS suporta <code>mixed</code> e <code>unix</code> estilos de segurança. SMB suporta <code>mixed</code> e <code>ntfs</code> estilos de segurança.	NFS default é <code>unix</code> . SMB default é <code>ntfs</code> .

Configurar um PVC

Esta seção inclui instruções sobre como criar um `PersistentVolumeClaim` (PVC) que usa o `StorageClass` do Kubernetes configurado para solicitar um PV. Se a solicitação for bem-sucedida, você poderá montar o PV em um pod.

Crie o PVC

Um *"PersistentVolumeClaim"* (PVC) é uma solicitação de acesso ao `PersistentVolume` no cluster. O PVC pode ser configurado para solicitar armazenamento de um determinado tamanho ou modo de acesso. Usando o `StorageClass` associado, o administrador do cluster pode controlar mais do que apenas o tamanho e o modo de acesso do `PersistentVolume`—como desempenho ou nível de serviço.

Após criar o backend Trident e o `StorageClass`, você pode criar um PVC. Depois que o PVC for criado, você pode montar o volume em um pod.

Exemplos de manifestos

Os exemplos a seguir mostram opções básicas de configuração de PVC.

PVC com acesso RWX

Este exemplo mostra um PVC básico com acesso RWX associado a um `StorageClass` chamado `basic-csi`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-gold
```

Exemplo de PVC usando iSCSI

Este exemplo mostra um PVC básico para iSCSI com acesso RWO que está associado a um StorageClass chamado `protection-gold`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: protection-gold
```

Criar PVC

Passos

1. Crie o PVC.

```
kubectl create -f pvc.yaml
```

2. Verifique o status do PVC.

```
kubectl get pvc
```

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
pvc-storage	Bound	pv-name	2Gi	RWO		5m

Consulte "[Objetos Kubernetes e Trident](#)" para obter detalhes sobre como as classes de armazenamento interagem com o `PersistentVolumeClaim` e os parâmetros para controlar como Trident provisiona volumes.

Implantar um aplicativo

Após a criação da classe de armazenamento e do PVC, você pode montar o PV em um pod. Esta seção lista o comando de exemplo e a configuração para anexar o PV a um pod.

Implante um aplicativo de exemplo

Passos

1. Monte o volume em um pod.

```
kubectl create -f pv-pod.yaml
```

Estes exemplos mostram configurações básicas para conectar o PVC a um pod: **configuração básica**:

```
kind: Pod
apiVersion: v1
metadata:
  name: pv-pod
spec:
  volumes:
    - name: pv-storage
      persistentVolumeClaim:
        claimName: basic
  containers:
    - name: pv-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/my/mount/path"
          name: pv-storage
```

OBSERVAÇÃO

Você pode monitorar o progresso usando `kubectl get pod --watch`.

2. Verifique se o volume está montado em `/my/mount/path`.

```
kubectl exec -it pv-pod -- df -h /my/mount/path
```

Filesystem	Size
Used Avail Use% Mounted on	
192.168.188.78:/trident_pvc_ae45ed05_3ace_4e7c_9080_d2a83ae03d06	1.1G
320K 1.0G 1% /my/mount/path	

Agora você pode excluir o Pod. O aplicativo Pod deixará de existir, mas o volume permanecerá.

```
kubectl delete pod pv-pod
```

Configurar o complemento Trident EKS em um cluster EKS

NetApp Trident simplifica o gerenciamento de storage do Amazon FSx for NetApp ONTAP no Kubernetes para permitir que seus desenvolvedores e administradores se concentrem na implantação de aplicativos. O NetApp Trident EKS add-on inclui os patches de segurança mais recentes, correções de bugs e é validado pela AWS para funcionar com o Amazon EKS. O EKS add-on permite garantir de forma consistente que seus clusters Amazon EKS estejam seguros e estáveis e reduz a quantidade de trabalho necessária para instalar, configurar e atualizar add-ons.

Pré-requisitos

Certifique-se de ter o seguinte antes de configurar o add-on Trident para AWS EKS:

- Uma conta de cluster Amazon EKS com permissões para trabalhar com complementos. Consulte ["Complementos do Amazon EKS"](#).
- Permissões da AWS para o AWS marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Tipo de AMI: Amazon Linux 2 (AL2_x86_64) ou Amazon Linux 2 Arm(AL2_ARM_64)
- Tipo de nó: AMD ou ARM
- Um sistema de arquivos Amazon FSx for NetApp ONTAP existente

Passos

1. Certifique-se de criar uma função do IAM e um segredo da AWS para permitir que os pods do EKS acessem os recursos da AWS. Para obter instruções, consulte ["Crie uma função do IAM e um segredo da AWS"](#).
2. No seu cluster Kubernetes EKS, navegue até a guia **Add-ons**.

The screenshot shows the AWS EKS console interface for a cluster named 'tri-env-eks'. At the top, there are buttons for 'Delete cluster', 'Upgrade version', and 'View dashboard'. Below this is a notification bar about the end of standard support for Kubernetes version 1.30 on July 28, 2025, with an 'Upgrade now' button. The main section is titled 'Cluster info' and includes details such as 'Status: Active', 'Kubernetes version: 1.30', 'Support period: Standard support until July 28, 2025', and 'Provider: EKS'. It also shows 'Cluster health issues' and 'Upgrade insights', both with a green checkmark and a '0' indicating no issues or insights. Below the cluster info, there is a navigation bar with tabs for 'Overview', 'Resources', 'Compute', 'Networking', 'Add-ons' (which is selected and has a '1' badge), 'Access', 'Observability', 'Update history', and 'Tags'. A notification bar below the tabs states 'New versions are available for 1 add-on.' The 'Add-ons' section shows 'Add-ons (3)' with buttons for 'View details', 'Edit', 'Remove', and 'Get more add-ons'. There is a search bar with the placeholder 'Find add-on' and filters for 'Any categ...', 'Any status', and '3 matches'. A pagination control shows '< 1 >'.

3. Acesse **AWS Marketplace add-ons** e escolha a categoria *storage*.

AWS Marketplace add-ons (1)

Discover, subscribe to and configure EKS add-ons to enhance your EKS clusters.

Filtering options

Any category ▾
NetApp, Inc. ▾
Any pricing model ▾
Clear filters

NetApp, Inc. ✕
1

NetApp Trident

NetApp Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. [Product details](#)

Standard Contract

Category storage	Listed by NetApp, Inc.	Supported versions 1.31, 1.30, 1.29, 1.28, 1.27, 1.26, 1.25, 1.24, 1.23	Pricing starting at View pricing details
----------------------------	--	---	--

Cancel
Next

- Localize **NetApp Trident** e selecione a caixa de seleção para o add-on Trident e clique em **Próximo**.
- Escolha a versão desejada do add-on.

Configure selected add-ons settings

Configure the add-ons for your cluster by selecting settings.

NetApp Trident
Remove add-on

Listed by 	Category storage	Status Ready to install
---------------	---------------------	----------------------------

You're subscribed to this software

You can view the terms and pricing details for this product or choose another offer if one is available.

View subscription ✕

Version
Select the version for this add-on.

v25.6.0-eksbuild.1

► Optional configuration settings

Cancel
Previous
Next

- Configurar as definições adicionais necessárias.

Review and add

Step 1: Select add-ons

[Edit](#)

Selected add-ons (1)

< 1 >

Add-on name	Type	Status
netapp_trident-operator	storage	Ready to install

Step 2: Configure selected add-ons settings

[Edit](#)

Selected add-ons version (1)

< 1 >

Add-on name	Version	IAM role for service account (IRSA)
netapp_trident-operator	v24.10.0-eksbuild.1	Not set

EKS Pod Identity (0)

< 1 >

Add-on name	IAM role	Service account
-------------	----------	-----------------

No Pod Identity associations
None of the selected add-on(s) have Pod Identity associations.

[Cancel](#)[Previous](#)[Create](#)

7. Se você estiver usando IRSA (IAM roles para conta de serviço), consulte as etapas de configuração adicionais "aqui".

8. Selecione **Criar**.

9. Verifique se o status do add-on é *Ativo*.

Add-ons (1) [Info](#)

[View details](#)[Edit](#)[Remove](#)[Get more add-ons](#)

Any categ...

Any status

1 match

< 1 >

NetApp

NetApp Trident

NetApp Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. [Product details](#)

Category	Status	Version	EKS Pod Identity	IAM role for service account (IRSA)
storage	Active	v24.10.0-eksbuild.1	-	Not set

Listed by
[NetApp, Inc.](#)

[View subscription](#)

10. Execute o seguinte comando para verificar se Trident está instalado corretamente no cluster:

```
kubectl get pods -n trident
```

11. Continue a configuração e configure o backend de storage. Para informações, consulte ["Configurar o backend de armazenamento"](#).

Instalar/desinstalar o Trident EKS add-on usando CLI

Instale o NetApp Trident EKS add-on usando CLI:

O seguinte comando de exemplo instala o Trident EKS add-on:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.0-eksbuild.1 (com uma versão dedicada)
```

O seguinte comando de exemplo instala o Trident EKS add-on versão 25.6.1:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.1-eksbuild.1 (com uma versão dedicada)
```

O seguinte comando de exemplo instala o Trident EKS add-on versão 25.6.2:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.2-eksbuild.1 (com uma versão dedicada)
```

Desinstale o complemento NetApp Trident EKS usando a CLI:

O comando a seguir desinstala o Trident EKS add-on:

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

Criar backends com kubectl

Um backend define a relação entre Trident e um sistema de storage. Ele informa ao Trident como se comunicar com esse sistema de storage e como o Trident deve provisionar volumes a partir dele. Após a instalação do Trident, o próximo passo é criar um backend. A `TridentBackendConfig` Custom Resource Definition (CRD) permite que você crie e gerencie backends do Trident diretamente pela interface do Kubernetes. Você pode fazer isso usando `kubectl` ou a ferramenta de linha de comando equivalente para sua distribuição do Kubernetes.

TridentBackendConfig

`TridentBackendConfig` (tbc, tbconfig, tbackendconfig) é um CRD de frontend com namespace que permite gerenciar backends do Trident usando `kubectl`. Administradores de Kubernetes e de storage agora podem criar e gerenciar backends diretamente por meio da CLI do Kubernetes sem a necessidade de um utilitário de linha de comando dedicado (`tridentctl`).

Ao criar um `TridentBackendConfig` objeto, ocorre o seguinte:

- Um backend é criado automaticamente pelo Trident com base na configuração que você fornece. Isso é representado internamente como um `TridentBackend` (tbe, `tridentbackend`) CR.

- O `TridentBackendConfig` está exclusivamente ligado a um `TridentBackend` que foi criado pela Trident.

Cada `TridentBackendConfig` mantém um mapeamento um-para-um com um `TridentBackend`. O primeiro é a interface fornecida ao usuário para projetar e configurar backends; o segundo é como Trident representa o objeto backend real.

AVISO

`TridentBackend` Os CRs são criados automaticamente pelo Trident. Você **não deve** modificá-los. Se você quiser fazer atualizações nos backends, faça isso modificando o `TridentBackendConfig` objeto.

Veja o exemplo a seguir para o formato do `TridentBackendConfig` CR:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

Você também pode consultar os exemplos no ["trident-installer"](#) diretório para obter configurações de amostra para a plataforma de storage/serviço desejado.

O `spec` aceita parâmetros de configuração específicos do backend. Neste exemplo, o backend usa o `ontap-san` driver de storage e utiliza os parâmetros de configuração que estão tabulados aqui. Para a lista de opções de configuração para o driver de storage desejado, consulte o ["Informações de configuração do backend para o seu driver de storage"](#).

A `spec` seção também inclui `credentials` e `deletionPolicy` campos, que são recém-introduzidos no `TridentBackendConfig` CR:

- `credentials`: Este parâmetro é obrigatório e contém as credenciais usadas para autenticação com o sistema de storage/serviço. Isso é definido como um segredo do Kubernetes criado pelo usuário. As credenciais não podem ser passadas em texto simples e resultarão em um erro.
- `deletionPolicy`: Este campo define o que deve acontecer quando o `TridentBackendConfig` for excluído. Ele pode assumir um dos dois valores possíveis:
 - `delete`: Isso resulta na exclusão tanto do `TridentBackendConfig` CR quanto do backend associado. Este é o valor padrão.
 - `retain`: Quando uma `TridentBackendConfig` CR é excluída, a definição do backend ainda estará presente e poderá ser gerenciada com `tridentctl`. Definir a política de exclusão para `retain` permite que os usuários façam downgrade para uma versão anterior (pré-21.04) e mantenham os

backends criados. O valor deste campo pode ser atualizado após uma `TridentBackendConfig` CR ser criada.

OBSERVAÇÃO

O nome de um backend é definido usando `spec.backendName`. Se não for especificado, o nome do backend é definido como o nome do objeto `TridentBackendConfig` (`metadata.name`). Recomenda-se definir explicitamente os nomes dos backends usando `spec.backendName`.

DICA

Os backends que foram criados com `tridentctl` não possuem um objeto `TridentBackendConfig` associado. Você pode optar por gerenciar esses backends com `kubectl` criando um `TridentBackendConfig` CR. É preciso ter cuidado para especificar parâmetros de configuração idênticos (como `spec.backendName`, `spec.storagePrefix`, `spec.storageDriverName` e assim por diante). O Trident vinculará automaticamente o novo `TridentBackendConfig` ao backend preexistente.

Visão geral das etapas

Para criar um novo backend usando `kubectl`, você deve fazer o seguinte:

1. Crie um "Kubernetes Secret" segredo. O segredo contém as credenciais que Trident precisa para se comunicar com o cluster/serviço de storage.
2. Crie um `TridentBackendConfig` objeto. Isso contém detalhes sobre o cluster/serviço de storage e faz referência ao segredo criado na etapa anterior.

Após criar um backend, você pode observar seu status usando `kubectl get tbc <tbc-name> -n <trident-namespace>` e coletar detalhes adicionais.

Passo 1: criar um segredo do Kubernetes

Crie um segredo que contenha as credenciais de acesso ao backend. Isso é exclusivo para cada serviço/plataforma de storage. Veja um exemplo:

```
kubectl -n trident create -f backend-tbc-ontap-san-secret.yaml
```

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-san-secret
type: Opaque
stringData:
  username: cluster-admin
  password: password
```

Esta tabela resume os campos que devem ser incluídos no Secret para cada plataforma de storage:

Descrição dos campos secretos da plataforma de storage	Segredo	Descrição dos campos
Azure NetApp Files	clientID	O client ID de um registro de aplicativo
Element (NetApp HCI/SolidFire)	Endpoint	MVIP para o SolidFire cluster com credenciais de locatário
ONTAP	nome de usuário	Nome de usuário para conectar-se ao cluster/SVM. Usada para autenticação baseada em credencial
ONTAP	senha	Senha para conectar-se ao cluster/SVM. Usada para autenticação baseada em credencial
ONTAP	clientPrivateKey	Valor codificado em Base64 da chave privada do cliente. Usado para autenticação baseada em certificado
ONTAP	chapUsername	Nome de usuário de entrada. Obrigatório se useCHAP=true. Para <code>ontap-san</code> e <code>ontap-san-economy</code>
ONTAP	chapInitiatorSecret	Segredo do iniciador CHAP. Obrigatório se useCHAP=true. Para <code>ontap-san</code> e <code>ontap-san-economy</code>
ONTAP	chapTargetUsername	Nome de usuário de destino. Obrigatório se useCHAP=true. Para <code>ontap-san</code> e <code>ontap-san-economy</code>
ONTAP	chapTargetInitiatorSecret	Segredo do iniciador do alvo CHAP. Obrigatório se useCHAP=true. Para <code>ontap-san</code> e <code>ontap-san-economy</code>

O segredo criado nesta etapa será referenciado no campo `spec.credentials` do objeto `TridentBackendConfig` que é criado na próxima etapa.

Etapa 2: Criar o `TridentBackendConfig` CR

Agora você está pronto para criar seu `TridentBackendConfig` CR. Neste exemplo, um backend que utiliza o `ontap-san` driver é criado usando o `TridentBackendConfig` objeto mostrado abaixo:

```
kubectl -n trident create -f backend-tbc-ontap-san.yaml
```

```
apiVersion: trident.netapp.io/v1
```

```

kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret

```

Etapa 3: Verificar o status do `TridentBackendConfig` CR

Agora que você criou o TridentBackendConfig CR, pode verificar o status. Veja o exemplo a seguir:

```

kubectl -n trident get tbc backend-tbc-ontap-san

```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
Bound	Success	

Um backend foi criado e vinculado com sucesso ao TridentBackendConfig CR.

A fase pode assumir um dos seguintes valores:

- **Bound:** O TridentBackendConfig CR está associado a um backend, e esse backend contém configRef definido para o TridentBackendConfig uid do CR.
- **Unbound:** Representado usando "". O TridentBackendConfig objeto não está vinculado a um backend. Todos os CRs recém-criados TridentBackendConfig estão nesta fase por padrão. Após a mudança de fase, ele não pode retornar ao estado Unbound novamente.
- **Deleting:** O TridentBackendConfig CR deletionPolicy foi configurado para ser excluído. Quando o TridentBackendConfig CR é excluído, ele transita para o estado Deleting.
 - Caso não existam reivindicações de volume persistentes (PVCs) no backend, excluir o TridentBackendConfig resultará na exclusão do backend pelo Trident, bem como da TridentBackendConfig CR.
 - Se um ou mais PVCs estiverem presentes no backend, ele entra em estado de exclusão. O TridentBackendConfig CR subsequentemente também entra na fase de exclusão. O backend e TridentBackendConfig são excluídos somente após todos os PVCs serem excluídos.
- **Lost:** O backend associado ao TridentBackendConfig CR foi excluído acidentalmente ou deliberadamente e o TridentBackendConfig CR ainda possui uma referência ao backend excluído. O TridentBackendConfig CR ainda pode ser excluído independentemente do deletionPolicy valor.
- **Unknown:** Trident não consegue determinar o estado ou a existência do backend associado ao

TridentBackendConfig CR. Por exemplo, se o servidor da API não estiver respondendo ou se o `tridentbackends.trident.netapp.io` CRD estiver ausente. Isso pode exigir intervenção.

Nesta etapa, um backend foi criado com sucesso! Existem diversas operações que também podem ser realizadas, como ["atualizações de backend e exclusões de backend"](#).

(Opcional) Passo 4: obtenha mais detalhes

Você pode executar o seguinte comando para obter mais informações sobre seu backend:

```
kubectl -n trident get tbc backend-tbc-ontap-san -o wide
```

NAME	BACKEND NAME	BACKEND UUID	
PHASE	STATUS	STORAGE DRIVER	DELETION POLICY
backend-tbc-ontap-san	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8	Bound Success ontap-san delete

Além disso, você também pode obter um dump YAML/JSON de `TridentBackendConfig`.

```
kubectl -n trident get tbc backend-tbc-ontap-san -o yaml
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  creationTimestamp: 2021-04-21T20:45:11Z
  finalizers:
    - trident.netapp.io
  generation: 1
  name: backend-tbc-ontap-san
  namespace: trident
  resourceVersion: "947143"
  uid: 35b9d777-109f-43d5-8077-c74a4559d09c
spec:
  backendName: ontap-san-backend
  credentials:
    name: backend-tbc-ontap-san-secret
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  storageDriverName: ontap-san
  svm: trident_svm
  version: 1
status:
  backendInfo:
```

```
backendName: ontap-san-backend
backendUUID: 8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
deletionPolicy: delete
lastOperationStatus: Success
message: Backend 'ontap-san-backend' created
phase: Bound
```

`backendInfo` contém o `backendName` e o `backendUUID` do backend criado em resposta ao `TridentBackendConfig` CR. O `lastOperationStatus` campo representa o status da última operação do `TridentBackendConfig` CR, que pode ser iniciada pelo usuário (por exemplo, o usuário alterou algo em `spec`) ou iniciada pelo Trident (por exemplo, durante reinicializações do Trident). Pode ser `Success` ou `Failed`. `phase` representa o status da relação entre o `TridentBackendConfig` CR e o backend. No exemplo acima, `phase` tem o valor `Bound`, o que significa que o `TridentBackendConfig` CR está associado ao backend.

Você pode executar o `kubectl -n trident describe tbc <tbc-cr-name>` comando para obter detalhes dos registros de eventos.

AVISO

Não é possível atualizar ou excluir um backend que contenha um objeto associado `TridentBackendConfig` usando `tridentctl`. Para entender as etapas envolvidas na troca entre `tridentctl` e `TridentBackendConfig`, ["veja aqui"](#).

Gerenciar backends

Gerencie os backends do Trident com kubectl

Saiba como realizar operações de gerenciamento de backend usando `kubectl`.

Excluir um backend

Ao excluir um `TridentBackendConfig`, você instrui Trident a excluir/manter backends (com base em `deletionPolicy`). Para excluir um backend, certifique-se de que `deletionPolicy` esteja definido como `delete`. Para excluir apenas o `TridentBackendConfig`, certifique-se de que `deletionPolicy` esteja definido como `retain`. Isso garante que o backend ainda esteja presente e possa ser gerenciado usando `tridentctl`.

Execute o seguinte comando:

```
kubectl delete tbc <tbc-name> -n trident
```

Trident não exclui os segredos do Kubernetes que estavam em uso por `TridentBackendConfig`. O usuário do Kubernetes é responsável por limpar os segredos. É preciso ter cuidado ao excluir segredos. Você só deve excluir segredos se eles não estiverem em uso pelos backends.

Veja os backends existentes

Execute o seguinte comando:

```
kubectl get tbc -n trident
```

Você também pode executar `tridentctl get backend -n trident` ou `tridentctl get backend -o yaml -n trident` para obter uma lista de todos os backends existentes. Essa lista também incluirá backends que foram criados com `tridentctl`.

Atualizar um backend

Podem haver vários motivos para atualizar um backend:

- As credenciais do sistema de storage foram alteradas. Para atualizar as credenciais, o Kubernetes Secret usado no `TridentBackendConfig` objeto deve ser atualizado. Trident atualizará automaticamente o backend com as credenciais mais recentes fornecidas. Execute o seguinte comando para atualizar o Kubernetes Secret:

```
kubectl apply -f <updated-secret-file.yaml> -n trident
```

- Parâmetros (como o nome da SVM do ONTAP que está sendo usada) precisam ser atualizados.
 - Você pode atualizar `TridentBackendConfig` objetos diretamente pelo Kubernetes usando o seguinte comando:

```
kubectl apply -f <updated-backend-file.yaml>
```

- Alternativamente, você pode fazer alterações no CR existente `TridentBackendConfig` usando o seguinte comando:

```
kubectl edit tbc <tbc-name> -n trident
```

OBSERVAÇÃO

- Se uma atualização do backend falhar, o backend continuará em sua última configuração conhecida. Você pode visualizar os logs para determinar a causa executando `kubectl get tbc <tbc-name> -o yaml -n trident` ou `kubectl describe tbc <tbc-name> -n trident`.
- Após identificar e corrigir o problema com o arquivo de configuração, você pode executar novamente o comando de atualização.

Gerencie os backends do Trident com `tridentctl`

Saiba como realizar operações de gerenciamento de backend usando `tridentctl`.

Criar um backend

Após criar um "arquivo de configuração backend", execute o seguinte comando:

```
tridentctl create backend -f <backend-file> -n trident
```

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

```
tridentctl logs -n trident
```

Após identificar e corrigir o problema com o arquivo de configuração, você pode simplesmente executar o `create` comando novamente.

Excluir um backend

Para excluir um backend do Trident, faça o seguinte:

1. Recupere o nome do backend:

```
tridentctl get backend -n trident
```

2. Exclua o backend:

```
tridentctl delete backend <backend-name> -n trident
```

OBSERVAÇÃO

Se Trident tiver provisionado volumes e snapshots desse backend que ainda existam, a exclusão do backend impede que novos volumes sejam provisionados por ele. O backend continuará existindo no estado "Deleting".

Veja os backends existentes

Para visualizar os backends que Trident conhece, faça o seguinte:

- Para obter um resumo, execute o seguinte comando:

```
tridentctl get backend -n trident
```

- Para obter todos os detalhes, execute o seguinte comando:

```
tridentctl get backend -o json -n trident
```

Atualizar um backend

Após criar um novo arquivo de configuração backend, execute o seguinte comando:

```
tridentctl update backend <backend-name> -f <backend-file> -n trident
```

Se a atualização do backend falhar, algo estava errado com a configuração do backend ou você tentou uma atualização inválida. Você pode visualizar os logs para determinar a causa executando o seguinte comando:

```
tridentctl logs -n trident
```

Após identificar e corrigir o problema com o arquivo de configuração, você pode simplesmente executar o `update` comando novamente.

Identifique as classes de armazenamento que usam um backend

Este é um exemplo do tipo de perguntas que você pode responder com o JSON que `tridentctl` gera para objetos do backend. Isso usa o utilitário `jq`, que você precisa instalar.

```
tridentctl get backend -o json | jq '[.items[] | {backend: .name, storageClasses: [.storage[].storageClasses] | unique}]'
```

Isso também se aplica a backends que foram criados usando `TridentBackendConfig`.

Escolha um método de gerenciamento de backend do Trident

Aprenda sobre as diferentes maneiras de gerenciar backends no Trident.

Opções para gerenciamento de backends

Com a introdução de `TridentBackendConfig`, os administradores agora têm duas maneiras únicas de gerenciar backends. Isso levanta as seguintes questões:

- Backends criados usando `tridentctl` podem ser gerenciados com `TridentBackendConfig`?
- Backends criados usando `TridentBackendConfig` podem ser gerenciados usando `tridentctl`?

Gerencie `tridentctl` back-ends usando `TridentBackendConfig`

Esta seção aborda os passos necessários para gerenciar backends que foram criados usando `tridentctl` diretamente através da interface do Kubernetes, criando `TridentBackendConfig` objetos.

Isso se aplica aos seguintes cenários:

- Backends pré-existentes, que não possuem um `TridentBackendConfig` porque foram criados com `tridentctl`.
- Novos backends que foram criados com `tridentctl`, enquanto outros `TridentBackendConfig` objetos existem.

Em ambos os cenários, os backends continuarão presentes, com Trident agendando volumes e operando sobre eles. Os administradores têm uma das duas opções aqui:

- Continue usando `tridentctl` para gerenciar os backends que foram criados com ele.
- Vincule os backends criados usando `tridentctl` a um novo `TridentBackendConfig` objeto. Fazer isso significa que os backends serão gerenciados usando `kubectl` e não `tridentctl`.

Para gerenciar um backend preexistente usando `kubectl`, você precisará criar um `TridentBackendConfig` que se conecte ao backend existente. Aqui está uma visão geral de como isso funciona:

1. Crie um segredo do Kubernetes. O segredo contém as credenciais que Trident precisa para se comunicar com o cluster/serviço de armazenamento.
2. Crie um `TridentBackendConfig` objeto. Isso contém detalhes sobre o cluster/serviço de storage e faz referência ao segredo criado na etapa anterior. É preciso ter cuidado para especificar parâmetros de configuração idênticos (como `spec.backendName`, `spec.storagePrefix`, `spec.storageDriverName`, e assim por diante). `spec.backendName` deve ser definido com o nome do backend existente.

Etapa 0: identificar o backend

Para criar uma `TridentBackendConfig` que se vincula a um backend existente, você precisará obter a configuração do backend. Neste exemplo, vamos supor que um backend foi criado usando a seguinte definição JSON:

```
tridentctl get backend ontap-nas-backend -n trident
```

NAME		STORAGE DRIVER	UUID
STATE	VOLUMES		
online	25	ontap-nas	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7

```
cat ontap-nas-backend.json
```

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.10.10.1",
  "dataLIF": "10.10.10.2",
  "backendName": "ontap-nas-backend",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "admin-password",
}
```

```

"defaults": {
  "spaceReserve": "none",
  "encryption": "false"
},
"labels": {
  "store": "nas_store"
},
"region": "us_east_1",
"storage": [
  {
    "labels": {
      "app": "msoffice",
      "cost": "100"
    },
    "zone": "us_east_1a",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "true",
      "unixPermissions": "0755"
    }
  },
  {
    "labels": {
      "app": "mysqldb",
      "cost": "25"
    },
    "zone": "us_east_1d",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "false",
      "unixPermissions": "0775"
    }
  }
]
}

```

Passo 1: criar um segredo do Kubernetes

Crie um segredo que contenha as credenciais para o backend, conforme mostrado neste exemplo:

```
cat tbc-ontap-nas-backend-secret.yaml
```

```

apiVersion: v1
kind: Secret

```

```
metadata:
  name: ontap-nas-backend-secret
type: Opaque
stringData:
  username: cluster-admin
  password: admin-password
```

```
kubectl create -f tbc-ontap-nas-backend-secret.yaml -n trident
secret/backend-tbc-ontap-san-secret created
```

Etapa 2: Criar um `TridentBackendConfig` CR

O próximo passo é criar uma `TridentBackendConfig` CR que se vinculará automaticamente à já existente `ontap-nas-backend` (como neste exemplo). Certifique-se de que os seguintes requisitos sejam atendidos:

- O mesmo nome de backend está definido em `spec.backendName`.
- Os parâmetros de configuração são idênticos aos do backend original.
- Pools virtuais (se presentes) devem manter a mesma ordem que no backend original.
- As credenciais são fornecidas por meio de um Kubernetes Secret e não em texto simples.

Nesse caso, o `TridentBackendConfig` ficará assim:

```
cat backend-tbc-ontap-nas.yaml
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: tbc-ontap-nas-backend
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.10.10.1
  dataLIF: 10.10.10.2
  backendName: ontap-nas-backend
  svm: trident_svm
  credentials:
    name: mysecret
  defaults:
    spaceReserve: none
    encryption: 'false'
  labels:
    store: nas_store
    region: us_east_1
```

```

storage:
- labels:
  app: msoffice
  cost: '100'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  app: mysqlldb
  cost: '25'
  zone: us_east_1d
  defaults:
    spaceReserve: volume
    encryption: 'false'
    unixPermissions: '0775'

```

```

kubectl create -f backend-tbc-ontap-nas.yaml -n trident
tridentbackendconfig.trident.netapp.io/tbc-ontap-nas-backend created

```

Etapa 3: Verificar o status do `TridentBackendConfig` CR

Após o TridentBackendConfig ter sido criado, sua fase deve ser Bound. Ele também deve refletir o mesmo nome de backend e UUID do backend existente.

```

kubectl get tbc tbc-ontap-nas-backend -n trident

```

NAME	BACKEND NAME	BACKEND UUID
tbc-ontap-nas-backend	ontap-nas-backend	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7

```

tridentctl get backend -n trident

```

NAME	STORAGE DRIVER	UUID
ontap-nas-backend	ontap-nas	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7

```

#confirm that no new backends were created (i.e., TridentBackendConfig did
not end up creating a new backend)

```

```
+-----+-----+-----+
```

O backend será agora completamente gerenciado usando o `tbc-ontap-nas-backend TridentBackendConfig` objeto.

Gerencie `TridentBackendConfig` back-ends usando `tridentctl`

``tridentctl`` pode ser usado para listar backends que foram criados usando ``TridentBackendConfig``. Além disso, administradores também podem optar por gerenciar completamente esses backends através de ``tridentctl``, excluindo ``TridentBackendConfig`` e certificando-se de que ``spec.deletionPolicy`` esteja definido como ``retain``.

Etapa 0: identificar o backend

Por exemplo, vamos supor que o seguinte backend foi criado usando `TridentBackendConfig`:

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME                BACKEND UUID
PHASE    STATUS    STORAGE DRIVER    DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-
0a5315ac5f82    Bound    Success    ontap-san    delete

tridentctl get backend ontap-san-backend -n trident
+-----+-----+-----+
+-----+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |                               UUID
| STATE  | VOLUMES |
+-----+-----+-----+
+-----+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |          33 |
+-----+-----+-----+
+-----+-----+-----+-----+-----+
```

A partir da saída, observa-se que `TridentBackendConfig` foi criado com sucesso e está vinculado a um backend [observe o UUID do backend].

Etapa 1: confirmar `deletionPolicy` está definido como `retain`

Vamos analisar o valor de `deletionPolicy`. Isso precisa ser definido como `retain`. Isso garante que, quando um `TridentBackendConfig` CR for excluído, a definição de backend ainda estará presente e poderá ser gerenciada com `tridentctl`.

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
```

```

NAME                                BACKEND NAME    BACKEND UUID
PHASE    STATUS    STORAGE DRIVER  DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-
0a5315ac5f82    Bound    Success    ontap-san    delete

# Patch value of deletionPolicy to retain
kubectl patch tbc backend-tbc-ontap-san --type=merge -p
'{"spec":{"deletionPolicy":"retain"}}' -n trident
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-san patched

#Confirm the value of deletionPolicy
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME    BACKEND UUID
PHASE    STATUS    STORAGE DRIVER  DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-
0a5315ac5f82    Bound    Success    ontap-san    retain

```

OBSERVAÇÃO

Não prossiga para a próxima etapa a menos que `deletionPolicy` esteja definido como `retain`.

Passo 2: Exclua o `TridentBackendConfig` CR

A etapa final é excluir o `TridentBackendConfig` CR. Após confirmar que o `deletionPolicy` está definido como `retain`, você pode prosseguir com a exclusão:

```

kubectl delete tbc backend-tbc-ontap-san -n trident
tridentbackendconfig.trident.netapp.io "backend-tbc-ontap-san" deleted

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|      NAME      | STORAGE DRIVER |                               UUID
| STATE  | VOLUMES |
+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |      33 |
+-----+-----+
+-----+-----+-----+-----+

```

Ao excluir o `TridentBackendConfig` objeto, Trident simplesmente o remove sem realmente excluir o próprio backend.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.