



Configurar y gestionar back-ends

Trident

NetApp

February 02, 2026

Tabla de contenidos

Configurar y gestionar back-ends	1
Configurar los back-ends	1
Azure NetApp Files	1
Configure un back-end de Azure NetApp Files	1
Prepárese para configurar un back-end de Azure NetApp Files	5
Opciones y ejemplos de configuración del back-end de Azure NetApp Files	8
NetApp Volumes para Google Cloud	21
Configura un back-end de Google Cloud NetApp Volumes	21
Prepárate para configurar un back-end de Google Cloud NetApp Volumes	24
Opciones de configuración y ejemplos de back-end de Google Cloud NetApp Volumes	24
Configure un back-end de NetApp HCI o SolidFire	38
Detalles del controlador de elementos	38
Antes de empezar	39
Opciones de configuración del back-end	39
Ejemplo 1: Configuración de back-end para solidfire-san controlador con tres tipos de volumen	40
Ejemplo 2: Configuración de clase de almacenamiento y de entorno de administración para solidfire-san controlador con pools virtuales	41
Obtenga más información	44
Unidades SAN de ONTAP	44
Información general del controlador de SAN de ONTAP	44
Prepárese para configurar el back-end con los controladores SAN de ONTAP	46
Opciones y ejemplos de configuración DE SAN ONTAP	54
Unidades NAS de ONTAP	74
Información general del controlador NAS de ONTAP	74
Prepárese para configurar un back-end con controladores NAS de ONTAP	75
Opciones y ejemplos de configuración NAS de ONTAP	88
Amazon FSX para ONTAP de NetApp	112
Utiliza Trident con Amazon FSx para NetApp ONTAP	112
Cree un rol de IAM y AWS Secret	115
Instale Trident	121
Configure el backend de almacenamiento	128
Configure una clase de almacenamiento y la RVP	137
Despliegue la aplicación de muestra	142
Configure el complemento Trident EKS en un clúster EKS	143
Cree back-ends con kubectl	146
TridentBackendConfig	147
Descripción general de los pasos	148
Paso 1: Cree un secreto de Kubernetes	148
Paso 2: Cree la TridentBackendConfig CR	150
Paso 3: Compruebe el estado del TridentBackendConfig CR	150
(Opcional) Paso 4: Obtener más detalles	151
Gestionar back-ends	153

Realice la gestión del entorno de administración con kubectl	153
Realizar la administración de back-end con trimentctl	154
Pasar entre las opciones de administración del back-end	156

Configurar y gestionar back-ends

Configurar los back-ends

Un back-end define la relación entre Trident y un sistema de almacenamiento. Indica a Trident cómo se comunica con ese sistema de almacenamiento y cómo debe aprovisionar volúmenes a partir de él.

Trident ofrece automáticamente pools de almacenamiento de back-ends que coincidan con los requisitos definidos por una clase de almacenamiento. Aprenda a configurar el back-end para el sistema de almacenamiento.

- ["Configure un back-end de Azure NetApp Files"](#)
- ["Configura un back-end de Google Cloud NetApp Volumes"](#)
- ["Configure un back-end de NetApp HCI o SolidFire"](#)
- ["Configure un back-end con controladores NAS ONTAP o Cloud Volumes ONTAP"](#)
- ["Configurar un back-end con controladores SAN ONTAP o Cloud Volumes ONTAP"](#)
- ["Utiliza Trident con Amazon FSx para NetApp ONTAP"](#)

Azure NetApp Files

Configure un back-end de Azure NetApp Files

Puede configurar Azure NetApp Files como backend de Trident. Puede asociar volúmenes NFS y SMB con un back-end de Azure NetApp Files. Trident también admite la gestión de credenciales mediante identidades administradas para clústeres de Azure Kubernetes Services (AKS).

Información del controlador de Azure NetApp Files

Trident proporciona los siguientes controladores de almacenamiento de Azure NetApp Files para comunicarse con el clúster. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
azure-netapp-files	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	nfs, smb

Consideraciones

- El servicio Azure NetApp Files no admite volúmenes de menos de 50 GiB. Trident crea automáticamente volúmenes de 50 GiB si se solicita un volumen más pequeño.
- Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.

Identities administradas para AKS

Trident es compatible con "identidades administradas"clústeres de Azure Kubernetes Services. Para aprovechar la gestión de credenciales optimizada que ofrecen las identidades gestionadas, debe tener:

- Un clúster de Kubernetes puesto en marcha mediante AKS
- Identidades gestionadas configuradas en el clúster de kubernetes de AKS
- Trident instalado que incluye el `cloudProvider` para especificar "Azure".

Operador de Trident

Para instalar Trident con el operador Trident, edite `tridentorchestrator_cr.yaml` en `cloudProvider "Azure"` . Por ejemplo:

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

Timón

En el siguiente ejemplo se instalan conjuntos de Trident `cloudProvider` en Azure mediante la variable de entorno `$CP` :

```
helm install trident trident-operator-100.2506.0.tgz --create
--namespace --namespace <trident-namespace> --set cloudProvider=$CP
```

`tridentctl`

En el siguiente ejemplo se instala Trident y se establece el `cloudProvider` indicador en Azure:

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

Identidad de nube para AKS

La identidad en la nube permite que los pods de Kubernetes accedan a los recursos de Azure autenticándose como identidad de carga de trabajo, en lugar de proporcionar credenciales explícitas de Azure.

Para aprovechar la identidad de la nube en Azure, debes tener:

- Un clúster de Kubernetes puesto en marcha mediante AKS

- Identidad de carga de trabajo y emisor de oidc configurados en el clúster de Kubernetes de AKS
- Trident instalado que incluye `cloudProvider` para "Azure" especificar y `cloudIdentity` especificar la identidad de la carga de trabajo

Operador de Trident

Para instalar Trident mediante el operador Trident, edite `tridentorchestrator_cr.yaml` en Establecer `cloudProvider` en "Azure" y establezca `cloudIdentity` en `azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx`.

Por ejemplo:

```
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
```

Timón

Establezca los valores para los indicadores **cloud-provider (CP)** y **cloud-identity (CI)** utilizando las siguientes variables de entorno:

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

En el siguiente ejemplo, se instala Trident y se establece `cloudProvider` en Azure mediante la variable de entorno `$CP` y se establece el `cloudIdentity` uso de la variable de entorno `$CI` :

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

<code>tridentctl</code>

Establezca los valores para los indicadores **cloud provider** y **cloud identity** utilizando las siguientes variables de entorno:

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

En el siguiente ejemplo se instala Trident y se establece el `cloud-provider` indicador en `$CP`, y `cloud-identity` en `$CI`:

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

Prepárese para configurar un back-end de Azure NetApp Files

Antes de configurar el back-end de Azure NetApp Files, debe asegurarse de que se cumplan los siguientes requisitos.

Requisitos previos para volúmenes NFS y SMB

Si utiliza Azure NetApp Files por primera vez o en una ubicación nueva, es necesario realizar alguna configuración inicial para configurar Azure NetApp Files y crear un volumen NFS. Consulte ["Azure: Configure Azure NetApp Files y cree un volumen NFS"](#).

Para configurar y utilizar un ["Azure NetApp Files"](#) back-end, necesita lo siguiente:



- `subscriptionID`, `tenantID`, `clientID`, `location`, y `clientSecret` Son opcionales cuando se utilizan identidades administradas en un clúster AKS.
- `tenantID`, `clientID`, y `clientSecret` Son opcionales cuando se utiliza una identidad de nube en un clúster de AKS.

- Un pool de capacidad. Consulte ["Microsoft: Cree un pool de capacidad para Azure NetApp Files"](#).
- Una subred delegada en Azure NetApp Files. Consulte ["Microsoft: Delege una subred en Azure NetApp Files"](#).
- `subscriptionID` Desde una suscripción de Azure con Azure NetApp Files habilitado.
- `tenantID`, `clientID`, y `clientSecret` desde una ["Registro de aplicaciones"](#) En Azure Active Directory con permisos suficientes para el servicio Azure NetApp Files. El registro de aplicaciones debe usar:
 - El rol propietario o Colaborador ["Predefinidos por Azure"](#).
 - A ["Rol Colaborador personalizado"](#) en el nivel de suscripción (`assignableScopes`) con los siguientes permisos que están limitados solo a lo que Trident requiere. Después de crear el rol personalizado, ["Asigne el rol mediante el portal de Azure"](#).


```
{
  "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": []
  }
]
}

```

- Azure location que contiene al menos uno ["subred delegada"](#). A partir de Trident 22.01, la location parámetro es un campo obligatorio en el nivel superior del archivo de configuración del back-end. Los valores de ubicación especificados en los pools virtuales se ignoran.
- Para usar Cloud Identity, obtén el client ID desde a ["identidad gestionada asignada por el usuario"](#) Y especifique ese ID en azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.

Requisitos adicionales para volúmenes SMB

Para crear un volumen de SMB, debe tener lo siguiente:

- Active Directory configurado y conectado a Azure NetApp Files. Consulte ["Microsoft: Cree y gestione conexiones de Active Directory para Azure NetApp Files"](#).
- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2022. Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto Trident que contiene sus credenciales de Active Directory para que Azure NetApp Files pueda autenticarse en Active Directory. Para generar secreto smbcreds:

```

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

```

- Proxy CSI configurado como servicio de Windows. Para configurar un csi-proxy, consulte ["GitHub: Proxy CSI"](#) o ["GitHub: Proxy CSI para Windows"](#) Para nodos Kubernetes que se ejecutan en Windows.

Opciones y ejemplos de configuración del back-end de Azure NetApp Files

Obtenga más información sobre las opciones de configuración de back-end NFS y SMB para Azure NetApp Files y revise los ejemplos de configuración.

Opciones de configuración del back-end

Trident utiliza la configuración de back-end (subred, red virtual, nivel de servicio y ubicación) para crear volúmenes de Azure NetApp Files en los pools de capacidad que están disponibles en la ubicación solicitada y coincidir con el nivel de servicio y la subred solicitados.

Los back-ends de Azure NetApp Files proporcionan estas opciones de configuración.

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	"azure-netapp-files"
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre del controlador + "_" + caracteres aleatorios
subscriptionID	El ID de suscripción de su suscripción de Azure Opcional cuando se activan identidades gestionadas en un clúster de AKS.	
tenantID	El ID de inquilino de un registro de aplicación Opcional cuando se utilizan identidades gestionadas o identidad de nube en un clúster de AKS.	
clientID	El ID de cliente de un registro de aplicación Opcional cuando se utilizan identidades gestionadas o identidad de nube en un clúster de AKS.	
clientSecret	El secreto de cliente de un registro de aplicaciones Opcional cuando se utilizan identidades gestionadas o identidad de nube en un clúster de AKS.	
serviceLevel	Uno de Standard, Premium, o. Ultra	"" (aleatorio)

Parámetro	Descripción	Predeterminado
location	Nombre de la ubicación de Azure donde se crearán los nuevos volúmenes Opcional cuando se activan identidades gestionadas en un clúster de AKS.	
resourceGroups	Lista de grupos de recursos para filtrar los recursos detectados	"" (sin filtro)
netappAccounts	Lista de cuentas de NetApp para filtrar los recursos detectados	"" (sin filtro)
capacityPools	Lista de pools de capacidad para filtrar los recursos detectados	"" (sin filtro, aleatorio)
virtualNetwork	Nombre de una red virtual con una subred delegada	""
subnet	Nombre de una subred delegada a. Microsoft.Netapp/volumes	""
networkFeatures	Puede que el conjunto de funciones de vnet para un volumen sea Basic o Standard. Las funciones de red no están disponibles en todas las regiones y es posible que tengan que activarse en una suscripción. Especificando networkFeatures cuando la funcionalidad no está habilitada, hace que no se pueda realizar el aprovisionamiento del volumen.	""
nfsMountOptions	Control preciso de las opciones de montaje NFS. Ignorada para volúmenes de SMB. Para montar volúmenes con NFS versión 4.1, incluya nfsvers=4 En la lista de opciones de montaje delimitadas por comas para elegir NFS v4.1. Las opciones de montaje establecidas en una definición de clase de almacenamiento anulan las opciones de montaje establecidas en la configuración de back-end.	"nfsvers=3"
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)

Parámetro	Descripción	Predeterminado
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo: <code>\{"api": false, "method": true, "discovery": true\}</code> . No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo
nasType	Configure la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o nulo. El valor predeterminado es nulo en volúmenes de NFS.	<code>nfs</code>
supportedTopologies	Representa una lista de regiones y zonas soportadas por este backend. Para obtener más información, consulte "Utilice Topología CSI" .	
qosType	Representa el tipo de QoS: Automático o Manual.	Auto
maxThroughput	Establece el rendimiento máximo permitido en MiB/seg. Compatible solo con grupos de capacidad de QoS manuales.	4 MiB/sec



Para obtener más información sobre las funciones de red, consulte ["Configure las funciones de red para un volumen de Azure NetApp Files"](#).

Permisos y recursos necesarios

Si recibe un error que indica que no se han encontrado pools de capacidad al crear una RVP, es probable que el registro de la aplicación no tenga los permisos y recursos necesarios (subred, red virtual, pool de capacidad) asociados. Si DEBUG está habilitado, Trident registrará los recursos de Azure detectados al crear el backend. Compruebe que se está utilizando un rol adecuado.

Los valores para `resourceGroups`, `netappAccounts`, `capacityPools`, `virtualNetwork`, y `subnet` puede especificarse utilizando nombres cortos o completos. En la mayoría de las situaciones, se recomiendan nombres completos, ya que los nombres cortos pueden coincidir con varios recursos con el mismo nombre.



Si la red virtual (vNet) se encuentra en un grupo de recursos diferente al de la cuenta de almacenamiento de Azure NetApp Files (ANF), especifique el grupo de recursos para la red virtual al configurar la lista de grupos de recursos para el back-end.

La `resourceGroups`, `netappAccounts`, y `capacityPools` los valores son filtros que restringen el conjunto de recursos detectados a los disponibles en este back-end de almacenamiento y pueden especificarse en cualquier combinación de estos. Los nombres completos siguen este formato:

Tipo	Formato
Grupo de recursos	<resource group>
Cuenta de NetApp	<resource group>/<netapp account>
Pool de capacidad	<resource group>/<netapp account>/<capacity pool>
Red virtual	<resource group>/<virtual network>
Subred	<resource group>/<virtual network>/<subnet>

Aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento de volúmenes predeterminado especificando las siguientes opciones en una sección especial del archivo de configuración. Consulte [Configuraciones de ejemplo](#) para obtener más detalles.

Parámetro	Descripción	Predeterminado
exportRule	Reglas de exportación de volúmenes nuevos. exportRule Debe ser una lista separada por comas con cualquier combinación de direcciones IPv4 o subredes IPv4 en notación CIDR. Ignorada para volúmenes de SMB.	"0.0.0.0/0"
snapshotDir	Controla la visibilidad del directorio .snapshot	"True" para NFSv4 "false" para NFSv3
size	El tamaño predeterminado de los volúmenes nuevos	"100 G"
unixPermissions	Los permisos unix de nuevos volúmenes (4 dígitos octal). Ignorada para volúmenes de SMB.	"" (función de vista previa, requiere incluir en la lista blanca de suscripciones)

Configuraciones de ejemplo

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.

Configuración mínima

Ésta es la configuración mínima absoluta del back-end. Con esta configuración, Trident detecta todas sus cuentas de NetApp, pools de capacidad y subredes delegadas en Azure NetApp Files en la ubicación configurada, y coloca volúmenes nuevos en uno de esos pools y subredes de forma aleatoria. Dado que `nasType` se omite, `nfs` se aplica el valor predeterminado y el back-end se aprovisionará para los volúmenes de NFS.

Esta configuración es ideal cuando solo se está empezando a usar Azure NetApp Files y probando cosas, pero en la práctica va a querer proporcionar un ámbito adicional para los volúmenes que aprovisiona.

```
---
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 administradas para AKS

Esta configuración de backend omite `subscriptionID`, `tenantID`, `clientID`, y `clientSecret`, que son opcionales cuando se utilizan identidades gestionadas.

```
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
```


Identidad de nube para AKS

Esta configuración de backend omite `tenantID`, `clientID`, y `clientSecret`, que son opcionales cuando se utiliza una identidad de nube.

```
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
```

Configuración de niveles de servicio específica con filtros de pools de capacidad

Esta configuración de backend coloca los volúmenes en la ubicación de Azure `eastus` en un `Ultra` pool de capacidad. Trident detecta automáticamente todas las subredes delegadas en Azure NetApp Files en esa ubicación y coloca un volumen nuevo en una de ellas de forma aleatoria.

```
---
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
```

Ejemplo de backend con grupos de capacidad de QoS manuales

Esta configuración de backend coloca volúmenes en Azure `eastus` Ubicación con pools de capacidad QoS manuales.

```
---
version: 1
storageDriverName: azure-netapp-files
backendName: anfl
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
```

Configuración avanzada

Esta configuración de back-end reduce aún más el alcance de la ubicación de volúmenes en una única subred y también modifica algunos valores predeterminados de aprovisionamiento de volúmenes.

```
---
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"
```

Configuración de pool virtual

Esta configuración back-end define varios pools de almacenamiento en un único archivo. Esto resulta útil cuando hay varios pools de capacidad que admiten diferentes niveles de servicio y desea crear clases de almacenamiento en Kubernetes que representan estos. Se utilizaron etiquetas de pools virtuales para diferenciar los pools según 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
```

Configuración de topologías admitidas

Trident facilita el aprovisionamiento de volúmenes para cargas de trabajo según regiones y zonas de disponibilidad. El `supportedTopologies` bloque en esta configuración de backend se utiliza para proporcionar una lista de regiones y zonas por backend. Los valores de región y zona especificados aquí deben coincidir con los valores de región y zona de las etiquetas de cada nodo de clúster de Kubernetes. Estas regiones y zonas representan la lista de valores permitidos que se pueden proporcionar en una clase de almacenamiento. Para las clases de almacenamiento que contienen un subconjunto de las regiones y zonas proporcionadas en un backend, Trident crea volúmenes en la región y zona mencionadas. Para obtener más información, consulte ["Utilice Topología 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
```

Definiciones de clases de almacenamiento

Lo siguiente `StorageClass` las definiciones hacen referencia a los pools de almacenamiento anteriores.

Definiciones de ejemplo mediante `parameter.selector` campo

Uso `parameter.selector` puede especificar para cada una de ellas `StorageClass` el pool virtual que se utiliza para alojar un volumen. Los aspectos definidos en el pool elegido serán el volumen.

```

---
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

```

Definiciones de ejemplo de volúmenes SMB

Uso `nasType`, `node-stage-secret-name`, y `node-stage-secret-namespace`, Puede especificar un volumen SMB y proporcionar las credenciales necesarias de Active Directory.

Configuración básica en el espacio de nombres predeterminado

```
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"
```

Uso de diferentes secretos por espacio de nombres

```
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}
```

Uso de diferentes secretos por volumen

```
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` Filtra los pools que admiten volúmenes SMB. `nasType: nfs` o `nasType: null` Filtros para pools NFS.

Cree el back-end

Después de crear el archivo de configuración del back-end, ejecute el siguiente comando:

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

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede ejecutar de nuevo el comando `create`.

NetApp Volumes para Google Cloud

Configura un back-end de Google Cloud NetApp Volumes

Ahora puede configurar Google Cloud NetApp Volumes como back-end para Trident. Puede adjuntar volúmenes de NFS y SMB a través de un back-end de Google Cloud NetApp Volumes.

Detalles del controlador de Google Cloud NetApp Volumes

Trident proporciona `google-cloud-netapp-volumes` el controlador para comunicarse con el clúster. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
<code>google-cloud-netapp-volumes</code>	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	<code>nfs</code> , <code>smb</code>

Identidad de nube para GKE

La identidad de cloud permite a los pods de Kubernetes acceder a los recursos de Google Cloud autenticándose como identidad de carga de trabajo en lugar de proporcionando credenciales explícitas de Google Cloud.

Para aprovechar la identidad de la nube en Google Cloud, debes tener:

- Un clúster de Kubernetes puesto en marcha mediante GKE.
- Identidad de carga de trabajo configurada en el cluster de GKE y el servidor de metadatos de GKE

configurado en los pools de nodos.

- Una cuenta de servicio de GCP con el rol NetApp Volumes Admin de Google Cloud (roles/NetApp.admin) o un rol personalizado.
- Trident instalado que incluye el cloudProvider para especificar «GCP» y cloudIdentity especificando la nueva cuenta de servicio de GCP. A continuación se muestra un ejemplo.

Operador de Trident

Para instalar Trident mediante el operador Trident, edite `tridentorchestrator_cr.yaml` en Establecer `cloudProvider` en "GCP" y establezca `cloudIdentity` en `iam.gke.io/gcp-service-account: cloudvolumes-admin-sa@mygcpproject.iam.gserviceaccount.com`.

Por ejemplo:

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

Timón

Establezca los valores para los indicadores **cloud-provider (CP)** y **cloud-identity (CI)** utilizando las siguientes variables de entorno:

```
export CP="GCP"
export ANNOTATION="'iam.gke.io/gcp-service-account: cloudvolumes-admin-
sa@mygcpproject.iam.gserviceaccount.com'"
```

En el siguiente ejemplo se instala Trident y se establece `cloudProvider` en GCP mediante la variable de entorno `$CP` y se establece el `cloudIdentity` uso de la variable de entorno `$ANNOTATION`:

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

<code>tridentctl</code>

Establezca los valores para los indicadores **cloud provider** y **cloud identity** utilizando las siguientes variables de entorno:

```
export CP="GCP"
export ANNOTATION="'iam.gke.io/gcp-service-account: cloudvolumes-admin-
sa@mygcpproject.iam.gserviceaccount.com'"
```

En el siguiente ejemplo se instala Trident y se establece el `cloud-provider` indicador en `$CP`, y `cloud-identity` en `$ANNOTATION`:

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

Prepárate para configurar un back-end de Google Cloud NetApp Volumes

Para poder configurar el back-end de Google Cloud NetApp Volumes, debe asegurarse de que se cumplan los siguientes requisitos.

Requisitos previos para volúmenes de NFS

Si utiliza Google Cloud NetApp Volumes por primera vez o en una ubicación nueva, es necesario tener alguna configuración inicial para configurar volúmenes de Google Cloud NetApp y crear un volumen NFS. Consulte ["Antes de empezar"](#).

Asegúrate de disponer de lo siguiente antes de configurar el back-end de Google Cloud NetApp Volumes:

- Una cuenta de Google Cloud configurada con el servicio NetApp Volumes de Google Cloud. Consulte ["NetApp Volumes para Google Cloud"](#).
- Número de proyecto de tu cuenta de Google Cloud. Consulte ["Identificación de proyectos"](#).
- Una cuenta de servicio de Google Cloud con el rol Administrador de volúmenes de NetApp (roles/netapp.admin). Consulte ["Funciones y permisos de Identity and Access Management"](#).
- Archivo de claves de API para tu cuenta de GCNV. Consulte ["Cree una clave de cuenta de servicio"](#).
- Un pool de almacenamiento. Consulte ["Información general sobre pools de almacenamiento"](#).

Para obtener más información acerca de cómo configurar el acceso a volúmenes de Google Cloud NetApp, consulte ["Configure el acceso a Google Cloud NetApp Volumes"](#).

Opciones de configuración y ejemplos de back-end de Google Cloud NetApp Volumes

Obtén más información sobre las opciones de configuración del back-end para Google Cloud NetApp Volumes y revisa los ejemplos de configuración.

Opciones de configuración del back-end

Cada back-end aprovisiona volúmenes en una única región de Google Cloud. Para crear volúmenes en otras regiones, se pueden definir back-ends adicionales.

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	El valor de storageDriverName debe especificarse como «google-cloud-netapp-Volumes».

Parámetro	Descripción	Predeterminado
backendName	(Opcional) Nombre personalizado del back-end de almacenamiento	Nombre de controlador + "_ " + parte de la clave de API
storagePools	Parámetro opcional que se utiliza para especificar pools de almacenamiento para la creación del volumen.	
projectNumber	Número de proyecto de cuenta de Google Cloud. El valor está disponible en la página de inicio del portal de Google Cloud.	
location	La ubicación de Google Cloud donde Trident crea volúmenes de GCNV. Al crear clústeres de Kubernetes entre regiones, los volúmenes creados en un location se pueden usar en cargas de trabajo programadas en nodos de varias regiones de Google Cloud. El tráfico entre regiones conlleva un coste adicional.	
apiKey	La clave de la API para la cuenta de servicio de Google Cloud con netapp.admin el rol. Incluye el contenido en formato JSON del archivo de clave privada de una cuenta de servicio de Google Cloud (copiado literal en el archivo de configuración de back-end). apiKey`Debe incluir pares clave-valor para las siguientes claves`type:,,,project_idclient_emailclient_id,,auth_uritoken_uriauth_provider_x509_cert_url,yclient_x509_cert_url.	
nfsMountOptions	Control preciso de las opciones de montaje NFS.	"nfsvers=3"
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor.	"" (no se aplica de forma predeterminada)
serviceLevel	El nivel de servicio de un pool de almacenamiento y sus volúmenes. Los valores son flex, standard, premium, o extreme.	
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
network	La red de Google Cloud utilizada para los volúmenes GCNV.	
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api": false, "method": true}. No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo
nasType	Configure la creación de volúmenes NFS o SMB. Las opciones son nfs, smb o nulo. El valor predeterminado es nulo en volúmenes de NFS.	nfs

Parámetro	Descripción	Predeterminado
supportedTopologies	Representa una lista de regiones y zonas soportadas por este backend. Para obtener más información, consulte "Utilice Topología CSI" . Por ejemplo: supportedTopologies: - topology.kubernetes.io/region: asia-east1 topology.kubernetes.io/zone: asia-east1-a	

Opciones de aprovisionamiento de volúmenes

Es posible controlar el aprovisionamiento de volúmenes predeterminado en la `defaults` sección del archivo de configuración.

Parámetro	Descripción	Predeterminado
exportRule	Las reglas de exportación de nuevos volúmenes. Debe ser una lista separada por comas de cualquier combinación de direcciones IPv4.	"0.0.0.0/0"
snapshotDir	Acceso a la <code>.snapshot</code> directorio	"True" para NFSv4 "false" para NFSv3
snapshotReserve	Porcentaje de volumen reservado para las Snapshot	" (aceptar valor por defecto de 0)
unixPermissions	Los permisos unix de nuevos volúmenes (4 dígitos octal).	""

Configuraciones de ejemplo

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.

Configuración mínima

Ésta es la configuración mínima absoluta del back-end. Con esta configuración, Trident detecta todos sus pools de almacenamiento delegados a volúmenes de Google Cloud NetApp en la ubicación configurada y coloca volúmenes nuevos en uno de esos pools de forma aleatoria. Dado que `nasType` se omite, `nfs` se aplica el valor predeterminado y el back-end se aprovisionará para los volúmenes de NFS.

Esta configuración es ideal cuando solo vas a empezar a usar Google Cloud NetApp Volumes e intentarlo, pero en la práctica probablemente necesites proporcionar un ámbito adicional para los volúmenes que aprovisionas.

```

---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: f2cb6ed6d7cc10c453f7d3406fc700c5df0ab9ec
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    XsYg6gyxy4zq7OlwWgLwGa==
    -----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

```

Configuración para volúmenes 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
```




```

---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: f2cb6ed6d7cc10c453f7d3406fc700c5df0ab9ec
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    XsYg6gyxy4zq7OlwWgLwGa==
    -----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

```

Configuración de pool virtual

Esta configuración de backend define varios pools virtuales en un único archivo. Los pools virtuales se definen en `storage` la sección. Son útiles cuando tienes varios pools de almacenamiento que admiten diferentes niveles de servicio y deseas crear clases de almacenamiento en Kubernetes que las representen. Las etiquetas de pools virtuales se utilizan para diferenciar los pools. Por ejemplo, en el ejemplo que aparece a continuación `performance`, se utiliza la etiqueta `y` `serviceLevel` el tipo para diferenciar los pools virtuales.

También puede configurar algunos valores predeterminados para que sean aplicables a todos los pools virtuales y sobrescribir los valores predeterminados de los pools virtuales individuales. En el siguiente ejemplo, `snapshotReserve` y `exportRule` sirven como valores predeterminados para todos los pools virtuales.

Para obtener más información, consulte ["Pools virtuales"](#).

```
---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: f2cb6ed6d7cc10c453f7d3406fc700c5df0ab9ec
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    XsYg6gyxy4zq7OlwWgLwGa==
    -----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

```

Identidad de nube para GKE

```

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

```

Configuración de topologías admitidas

Trident facilita el aprovisionamiento de volúmenes para cargas de trabajo según regiones y zonas de disponibilidad. El `supportedTopologies` bloque en esta configuración de backend se utiliza para proporcionar una lista de regiones y zonas por backend. Los valores de región y zona especificados aquí deben coincidir con los valores de región y zona de las etiquetas de cada nodo de clúster de Kubernetes. Estas regiones y zonas representan la lista de valores permitidos que se pueden proporcionar en una clase de almacenamiento. Para las clases de almacenamiento que contienen un subconjunto de las regiones y zonas proporcionadas en un backend, Trident crea volúmenes en la región y zona mencionadas. Para obtener más información, consulte ["Utilice Topología 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
```

El futuro

Después de crear el archivo de configuración del back-end, ejecute el siguiente comando:

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

Para verificar que el backend se ha creado correctamente, ejecute el siguiente comando:

```
kubectl get tridentbackendconfig
```

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

Si la creación del back-end falla, algo está mal con la configuración del back-end. Puede describir el backend con el `kubectl get tridentbackendconfig <backend-name>` comando o ver los logs para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puede suprimir el backend y ejecutar el comando `create` de nuevo.

Definiciones de clases de almacenamiento

La siguiente es una definición básica `StorageClass` que hace referencia al backend anterior.

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

Ejemplo de definiciones usando el `parameter.selector` campo:

Mediante el uso `parameter.selector` se puede especificar para cada uno `StorageClass` de los "pool virtual" que se utiliza para alojar un volumen. Los aspectos definidos en el pool elegido serán el volumen.

```

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 obtener más información sobre las clases de almacenamiento, consulte ["Cree una clase de almacenamiento"](#).

Definiciones de ejemplo de volúmenes SMB

Con `nasType`, `node-stage-secret-name` y `node-stage-secret-namespace`, puede especificar un volumen SMB y proporcionar las credenciales de Active Directory necesarias. Se puede utilizar cualquier usuario/contraseña de Active Directory con permisos o sin permisos para el secreto de etapa de nodos.

Configuración básica en el espacio de nombres predeterminado

```
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"
```

Uso de diferentes secretos por espacio de nombres

```
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}
```

Uso de diferentes secretos por volumen

```
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` Filtra los pools que admiten volúmenes SMB. `nasType: nfs` o `nasType: null` Filtros para pools NFS.

Ejemplo de definición de PVC

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

Para verificar si la RVP está vinculada, ejecute el siguiente comando:

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

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

Configure un back-end de NetApp HCI o SolidFire

Aprende a crear y usar un back-end de Element con tu instalación de Trident.

Detalles del controlador de elementos

Trident proporciona `solidfire-san` el controlador de almacenamiento para comunicarse con el clúster. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

```
`solidfire-san`El controlador de almacenamiento admite los modos de
volumen _FILE_ y _BLOCK_. Para el `Filesystem` volumeMode, Trident crea un
volumen y crea un sistema de archivos. El tipo de sistema de archivos se
especifica mediante StorageClass.
```

Controlador	Protocolo	Modo VolumeMode	Modos de acceso compatibles	Sistemas de archivos compatibles
solidfire-san	ISCSI	Bloque	RWO, ROX, RWX, RWOP	No hay sistema de archivos. Dispositivo de bloque RAW.
solidfire-san	ISCSI	Sistema de archivos	RWO, RWOP	xfs, ext3, ext4

Antes de empezar

Necesitarás lo siguiente antes de crear un backend de elemento.

- Es un sistema de almacenamiento compatible que ejecuta el software Element.
- Credenciales a un usuario administrador del clúster o inquilino de HCI de NetApp/SolidFire que puede gestionar volúmenes.
- Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Consulte ["información de preparación del nodo de trabajo"](#).

Opciones de configuración del back-end

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	Siempre «SolidFire-san»
backendName	Nombre personalizado o el back-end de almacenamiento	«SolidFire_» + dirección IP de almacenamiento (iSCSI)
Endpoint	MVIP para el clúster de SolidFire con credenciales de inquilino	
SVIP	La dirección IP y el puerto de almacenamiento (iSCSI)	
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes.	""
TenantName	Nombre de inquilino que se va a usar (creado si no se encuentra)	
InitiatorIFace	Restringir el tráfico de iSCSI a una interfaz de host específica	"predeterminado"
UseCHAP	Utilice CHAP para autenticar iSCSI. Trident utiliza CHAP.	verdadero
AccessGroups	Lista de ID de grupos de acceso que se van a usar	Busca el ID de un grupo de acceso llamado Trident.

Parámetro	Descripción	Predeterminado
Types	Especificaciones de calidad de servicio	
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {«api»:false, «method»:true}	nulo



No utilizar `debugTraceFlags` a menos que esté solucionando problemas y necesite un volcado de registro detallado.

Ejemplo 1: Configuración de back-end para `solidfire-san` controlador con tres tipos de volumen

Este ejemplo muestra un archivo de back-end mediante autenticación CHAP y modelado de tres tipos de volúmenes con garantías de calidad de servicio específicas. Lo más probable es que, a continuación, defina clases de almacenamiento para consumir cada una de ellas mediante el `IOPS` parámetro de clase de almacenamiento.

```

---
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

```

Ejemplo 2: Configuración de clase de almacenamiento y de entorno de administración para solidfire-san controlador con pools virtuales

En este ejemplo, se muestra el archivo de definición del back-end configurado con pools virtuales junto con StorageClasses que les devuelve referencia.

Las etiquetas de copias de Trident están presentes en un pool de almacenamiento en el LUN de almacenamiento back-end en el momento del aprovisionamiento. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

En el archivo de definición de backend de ejemplo que se muestra a continuación, se establecen valores predeterminados específicos para todos los grupos de almacenamiento, que establecen el `type` En Silver. Los pools virtuales se definen en la `storage` sección. En este ejemplo, algunos pools de almacenamiento establecen su propio tipo, y algunos pools anulan los valores predeterminados definidos anteriormente.

```

---
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

```

Las siguientes definiciones de StorageClass se refieren a los pools virtuales anteriores. Con el

`parameters.selector` Field, cada clase de almacenamiento llama a qué pools virtuales se pueden utilizar para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

El primer `StorageClass` (`solidfire-gold-four`) se asignará al primer pool virtual. Este es el único pool que ofrece rendimiento de oro con `A Volume Type QoS` de Oro. The Last `StorageClass` (`solidfire-silver`) llama a cualquier pool de almacenamiento que ofrece un rendimiento óptimo. Trident decidirá qué pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

```
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

```

Obtenga más información

- ["Los grupos de acceso de volúmenes"](#)

Unidades SAN de ONTAP

Información general del controlador de SAN de ONTAP

Obtenga información sobre la configuración de un back-end de ONTAP con controladores SAN de ONTAP y Cloud Volumes ONTAP.

Información sobre el controlador de SAN de ONTAP

Trident proporciona los siguientes controladores de almacenamiento SAN para comunicarse con el clúster de ONTAP. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-san	SCSI iSCSI sobre FC	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar
ontap-san	SCSI iSCSI sobre FC	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	xfs, ext3, ext4
ontap-san	NVMe/TCP Consulte Consideraciones adicionales para NVMe/TCP.	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-san	NVMe/TCP Consulte Consideraciones adicionales para NVMe/TCP .	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	xfs, ext3, ext4
ontap-san-economy	ISCSI	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin procesar
ontap-san-economy	ISCSI	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen del sistema de archivos.	xfs, ext3, ext4



- Uso `ontap-san-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)".
- Uso `ontap-nas-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)" y la `ontap-san-economy` no se puede utilizar el conductor.
- No utilizar `ontap-nas-economy` si prevé la necesidad de protección de datos, recuperación ante desastres o movilidad.
- NetApp no recomienda el uso de crecimiento automático de FlexVol en todos los controladores de ONTAP, excepto ONTAP-san. Como solución alternativa, Trident admite el uso de la reserva Snapshot y escala los volúmenes de FlexVol en consecuencia.

Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente utilizando el usuario del clúster o `vsadmin` un usuario de SVM, `admin` o bien como usuario con un nombre distinto que tenga el mismo rol. Para puestas en marcha de Amazon FSx para NetApp ONTAP, Trident espera ejecutarse como administrador de ONTAP o SVM, utilizando el usuario del clúster `fsxadmin` o un `vsadmin` usuario de SVM, o como un usuario con un nombre distinto que tenga el mismo rol. `fsxadmin` El usuario es un sustituto limitado para el usuario administrador del clúster.



Si se usa `limitAggregateUsage` el parámetro, se requieren permisos de administrador del clúster. Cuando se usa Amazon FSx para NetApp ONTAP con Trident, el `limitAggregateUsage` parámetro no funcionará con `vsadmin` las cuentas de usuario y `fsxadmin` La operación de configuración generará un error si se especifica este parámetro.

Si bien es posible crear un rol más restrictivo dentro de ONTAP que puede utilizar un controlador Trident, no lo recomendamos. La mayoría de las nuevas versiones de Trident denominan API adicionales que se tendrían

que tener en cuenta, por lo que las actualizaciones son complejas y propensas a errores.

Consideraciones adicionales para NVMe/TCP

Trident admite el protocolo expres de memoria no volátil (NVMe) mediante `ontap-san` el controlador que se incluye:

- IPv6
- Snapshots y clones de volúmenes NVMe
- Cambiar el tamaño de un volumen NVMe
- Se importa un volumen NVMe que se creó fuera de Trident para que su ciclo de vida se pueda gestionar mediante Trident
- Multivía nativa de NVMe
- Cierre correcto o sin complicaciones de los K8s nodos (24,06)

Trident no admite:

- DH-HMAC-CHAP compatible de forma nativa con NVMe
- Rutas múltiples del asignador de dispositivos (DM)
- Cifrado LUKS



NVMe solo es compatible con las API REST de ONTAP y no con ONTAPI (ZAPI).

Prepárese para configurar el back-end con los controladores SAN de ONTAP

Conozca los requisitos y las opciones de autenticación para configurar un back-end de ONTAP con controladores SAN de ONTAP.

Requisitos

Para todos los backends de ONTAP, Trident requiere que se asigne al menos un agregado al SVM.



"Sistemas ASA r2" Se diferencian de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento. En los sistemas ASA r2, se utilizan zonas de disponibilidad de almacenamiento en lugar de agregados. Referirse a ["este"](#) Artículo de la base de conocimientos sobre cómo asignar agregados a SVM en sistemas ASA r2.

Recuerde que también puede ejecutar más de un controlador y crear clases de almacenamiento que señalen a uno o a otro. Por ejemplo, puede configurar un `san-dev` clase que utiliza `ontap-san` controlador y a `san-default` clase que utiliza `ontap-san-economy` uno.

Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Consulte ["Prepare el nodo de trabajo"](#) para obtener más detalles.

Autentique el backend de ONTAP

Trident ofrece dos modos de autenticación de un backend ONTAP.

- Basado en credenciales: El nombre de usuario y la contraseña de un usuario ONTAP con los permisos requeridos. Se recomienda utilizar un rol de inicio de sesión de seguridad predefinido, como `admin o`.

vsadmin Garantizar la máxima compatibilidad con versiones de ONTAP.

- Basado en certificado: Trident también puede comunicarse con un clúster de ONTAP mediante un certificado instalado en el back-end. Aquí, la definición de backend debe contener valores codificados en Base64 del certificado de cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

Puede actualizar los back-ends existentes para moverse entre métodos basados en credenciales y basados en certificados. Sin embargo, solo se admite un método de autenticación a la vez. Para cambiar a un método de autenticación diferente, debe eliminar el método existente de la configuración del back-end.



Si intenta proporcionar **tanto credenciales como certificados**, la creación de backend fallará y se producirá un error en el que se haya proporcionado más de un método de autenticación en el archivo de configuración.

Habilite la autenticación basada en credenciales

Trident requiere que las credenciales se comuniquen con un administrador de SVM o con el ámbito del clúster para que se comunique con el back-end de ONTAP. Se recomienda hacer uso de roles estándar, predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad con futuras versiones de ONTAP que podrían exponer API de funciones que podrán utilizarse en futuras versiones de Trident. Puede crearse y utilizarse un rol de inicio de sesión de seguridad personalizado con Trident, pero no se recomienda.

Una definición de backend de ejemplo tendrá este aspecto:

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"
}
```

Tenga en cuenta que la definición de backend es el único lugar en el que las credenciales se almacenan en

texto sin formato. Una vez creado el back-end, los nombres de usuario y las contraseñas se codifican con Base64 y se almacenan como secretos de Kubernetes. La creación o actualización de un backend es el único paso que requiere conocimiento de las credenciales. Por tanto, es una operación de solo administración que deberá realizar el administrador de Kubernetes o almacenamiento.

Habilitar la autenticación basada en certificados

Los back-ends nuevos y existentes pueden utilizar un certificado y comunicarse con el back-end de ONTAP. Se necesitan tres parámetros en la definición de backend.

- **ClientCertificate:** Valor codificado en base64 del certificado de cliente.
- **ClientPrivateKey:** Valor codificado en base64 de la clave privada asociada.
- **TrustedCACertificate:** Valor codificado en base64 del certificado de CA de confianza. Si se utiliza una CA de confianza, se debe proporcionar este parámetro. Esto se puede ignorar si no se utiliza ninguna CA de confianza.

Un flujo de trabajo típico implica los pasos siguientes.

Pasos

1. Genere una clave y un certificado de cliente. Al generar, establezca el nombre común (CN) en el usuario de ONTAP para autenticarse como.

```
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. Añada un certificado de CA de confianza al clúster ONTAP. Es posible que ya sea gestionado por el administrador de almacenamiento. Ignore si no se utiliza ninguna CA de confianza.

```
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 el certificado y la clave de cliente (desde el paso 1) en el clúster ONTAP.

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



Después de ejecutar este comando, ONTAP solicita la introducción del certificado. Pega el contenido del archivo `k8senv.pem` generado en el paso 1, luego ingresa `END` para completar la instalación.

4. Confirme los compatibilidad con el rol de inicio de sesión de seguridad ONTAP `cert` método de autenticación.

```
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. Probar la autenticación mediante un certificado generado. Reemplace <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre de 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 certificados, claves y certificados de CA de confianza con Base64.

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

7. Cree un backend utilizando los valores obtenidos del paso 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 |
+-----+-----+-----+-----+
+-----+-----+

```

Actualice los métodos de autenticación o gire las credenciales

Puede actualizar un back-end existente para utilizar un método de autenticación diferente o para rotar sus credenciales. Esto funciona de las dos maneras: Los back-ends que utilizan nombre de usuario/contraseña se pueden actualizar para usar certificados. Los back-ends que utilizan certificados pueden actualizarse a nombre de usuario/contraseña. Para ello, debe eliminar el método de autenticación existente y agregar el nuevo método de autenticación. A continuación, utilice el archivo backend.json actualizado que contiene los parámetros necesarios para ejecutarse `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 |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online | 9 |
+-----+-----+-----+
+-----+-----+
```



Cuando gira contraseñas, el administrador de almacenamiento debe actualizar primero la contraseña del usuario en ONTAP. A esto le sigue una actualización de back-end. Al rotar certificados, se pueden agregar varios certificados al usuario. A continuación, el back-end se actualiza para usar el nuevo certificado, siguiendo el cual se puede eliminar el certificado antiguo del clúster de ONTAP.

La actualización de un back-end no interrumpe el acceso a los volúmenes que se han creado ni afecta a las conexiones de volúmenes realizadas después. Una actualización de back-end correcta indica que Trident puede comunicarse con el back-end de ONTAP y manejar operaciones de volumen futuras.

Crear rol de ONTAP personalizado para Trident

Puede crear un rol de clúster de ONTAP con un Privileges mínimo de modo que no tenga que utilizar el rol de administrador de ONTAP para realizar operaciones en Trident. Cuando incluye el nombre de usuario en una configuración de back-end de Trident, Trident utiliza el rol de clúster de ONTAP que creó para realizar las operaciones.

Consulte "[Generador de roles personalizados de Trident](#)" para obtener más información sobre la creación de roles personalizados de Trident.

Con la CLI de ONTAP

1. Cree un rol nuevo mediante el siguiente comando:

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

2. Cree un nombre de usuario para el usuario de 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. Asignar el rol al usuario:

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

Mediante System Manager

Realice los pasos siguientes en ONTAP System Manager:

1. **Crear un rol personalizado:**

- a. Para crear un rol personalizado a nivel de clúster, seleccione **Cluster > Settings**.

(O) Para crear un rol personalizado en el nivel de SVM, seleccione **Almacenamiento > Storage VMs > required svm > Settings > Users and Roles**.

- b. Seleccione el icono de flecha (→) junto a **Usuarios y roles**.

- c. Seleccione **+Agregar** en **Roles**.

- d. Defina las reglas para el rol y haga clic en **Guardar**.

2. **Asignar el rol al usuario de Trident:** + Realizar los siguientes pasos en la página **Usuarios y Roles**:

- a. Seleccione Agregar icono **+** en **Usuarios**.

- b. Seleccione el nombre de usuario requerido y seleccione un rol en el menú desplegable para **Rol**.

- c. Haga clic en **Guardar**.

Consulte las siguientes páginas si quiere más información:

- ["Roles personalizados para la administración de ONTAP"](#) o. ["Definir funciones personalizadas"](#)
- ["Trabajar con roles y usuarios"](#)

Autenticar conexiones con CHAP bidireccional

Trident puede autenticar sesiones iSCSI con CHAP bidireccional para `ontap-san` los controladores y `ontap-san-economy`. Esto requiere la activación de `useCHAP` la opción en la definición de backend. Cuando se establece en `true`, Trident configura la seguridad del iniciador predeterminado de la SVM como CHAP bidireccional y establece el nombre de usuario y los secretos del archivo back-end. NetApp recomienda utilizar CHAP bidireccional para autenticar las conexiones. Consulte la siguiente configuración de ejemplo:

```

---
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

```



La useCHAP Parameter es una opción booleana que solo se puede configurar una vez. De forma predeterminada, se establece en FALSE. Después de configurarlo en true, no puede establecerlo en false.

Además de useCHAP=true, la chapInitiatorSecret, chapTargetInitiatorSecret, chapTargetUsername, y. chapUsername los campos deben incluirse en la definición del backend. Los secretos se pueden cambiar después de crear un back-end ejecutando `tridentctl update`.

Cómo funciona

Al configurarse useCHAP en true, el administrador de almacenamiento le ordena a Trident que configure CHAP en el back-end de almacenamiento. Esto incluye lo siguiente:

- Configuración de CHAP en la SVM:
 - Si el tipo de seguridad de iniciador predeterminado de la SVM es none (establecido de forma predeterminada) y no hay LUN preexistentes ya presentes en el volumen, Trident establecerá el tipo de seguridad predeterminado en CHAP y continuará configurando el iniciador CHAP y el nombre de usuario y los secretos de destino.
 - Si la SVM contiene LUN, Trident no habilitará CHAP en la SVM. De este modo se garantiza que no se restrinja el acceso a las LUN que ya están presentes en la SVM.
- Configurar el iniciador de CHAP, el nombre de usuario y los secretos de destino; estas opciones deben especificarse en la configuración del back-end (como se muestra más arriba).

Después de crear el backend, Trident crea un CRD correspondiente `tridentbackend` y almacena los secretos CHAP y nombres de usuario como secretos de Kubernetes. Todos los VP que crea Trident en este back-end se montarán y conectarán mediante CHAP.

Rotar credenciales y actualizar backends

Para actualizar las credenciales de CHAP, se deben actualizar los parámetros de CHAP en `backend.json` archivo. Para ello, será necesario actualizar los secretos CHAP y utilizar el `tridentctl update` comando para reflejar estos cambios.



Al actualizar los secretos CHAP para un backend, debe utilizar `tridentctl` para actualizar el backend. No actualice las credenciales en el clúster de almacenamiento mediante la interfaz de línea de comandos de ONTAP o ONTAP System Manager, ya que Trident no podrá recoger estos cambios.

```
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-4378-8a33-1a472ffbeeb5c |
online |        7 |
+-----+-----+-----+-----+
+-----+-----+
```

Las conexiones existentes no se verán afectadas; seguirán activas si las credenciales se actualizan mediante Trident en la SVM. Las nuevas conexiones utilizan las credenciales actualizadas y las conexiones existentes siguen activas. Al desconectar y volver a conectar los VP antiguos, se utilizarán las credenciales actualizadas.

Opciones y ejemplos de configuración DE SAN ONTAP

Aprenda a crear y utilizar controladores SAN de ONTAP con su instalación de Trident. Esta sección proporciona ejemplos de configuración de backend y detalles para la asignación de back-ends a StorageClasses.

["Sistemas ASA r2"](#) Se diferencian de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento. Estas variaciones afectan al uso de ciertos parámetros, tal como se indica.

["Obtenga más información sobre las diferencias entre los sistemas ASA r2 y otros sistemas ONTAP"](#).




Solo el `ontap-san` El controlador (con protocolos iSCSI, NVMe/TCP y FC) es compatible con los sistemas ASA r2.


En la configuración del backend de Trident , no es necesario especificar que su sistema sea ASA r2. Cuando selecciona `ontap-san` como el `storageDriverName` Trident detecta automáticamente el ASA r2 u otros sistemas ONTAP . Algunos parámetros de configuración del backend no son aplicables a los sistemas ASA r2, como se indica en la tabla siguiente.


Opciones de configuración del back-end

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	<code>ontap-san</code> o <code>ontap-san-economy</code>
<code>backendName</code>	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + «_» + LIF de datos
<code>managementLIF</code>	<p>La dirección IP de un clúster o una LIF de gestión de SVM.</p> <p>Se puede especificar un nombre de dominio completo (FQDN).</p> <p>Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code> como .</p> <p>Para una conmutación de sitios MetroCluster fluida, consulte Ejemplo de MetroCluster.</p> <div>  <p>Si utiliza las credenciales «vsadmin», <code>managementLIF</code> debe ser la de la SVM; si utiliza credenciales «admin», <code>managementLIF</code> debe ser la del clúster.</p> </div>	«10.0.0.1», «[2001:1234:abcd::fefe]»
<code>dataLIF</code>	<p>Dirección IP de LIF de protocolo. Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code> como . No especifique para iSCSI. Trident utiliza "Asignación de LUN selectiva de ONTAP" para detectar las LIF iSCSI necesarias para establecer una sesión de rutas múltiples. Se genera una advertencia si <code>dataLIF</code> se define explícitamente. Omitir para MetroCluster. Consulte la Ejemplo de MetroCluster.</p>	Derivado del SVM

Parámetro	Descripción	Predeterminado
svm	Máquina virtual de almacenamiento que usar Omitir para MetroCluster. Ver Ejemplo de MetroCluster .	Derivado si una SVM managementLIF está especificado
useCHAP	Use CHAP para autenticar iSCSI para los controladores SAN de ONTAP [Boolean]. Establezca como true para que Trident configure y utilice CHAP bidireccional como la autenticación predeterminada para la SVM especificada en el back-end. Consulte "Prepárese para configurar el back-end con los controladores SAN de ONTAP" para obtener más información. No compatible con FCP o NVMe/TCP.	false
chapInitiatorSecret	Secreto CHAP del iniciador. Obligatorio si useCHAP=true	""
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
chapTargetInitiatorSecret	Secreto CHAP del iniciador de destino. Obligatorio si useCHAP=true	""
chapUsername	Nombre de usuario entrante. Obligatorio si useCHAP=true	""
chapTargetUsername	Nombre de usuario de destino. Obligatorio si useCHAP=true	""
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados.	""
username	Nombre de usuario necesario para comunicarse con el clúster ONTAP . Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulte "Autenticar Trident en un SVM backend mediante credenciales de Active Directory" .	""
password	Contraseña necesaria para comunicarse con el clúster ONTAP . Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulte "Autenticar Trident en un SVM backend mediante credenciales de Active Directory" .	""
svm	Máquina virtual de almacenamiento que usar	Derivado si una SVM managementLIF está especificado

Parámetro	Descripción	Predeterminado
storagePrefix	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede modificar más adelante. Para actualizar este parámetro, deberá crear un nuevo backend.	trident
aggregate	<p>Agregado para el aprovisionamiento (opcional; si se establece, se debe asignar a la SVM). Para el <code>ontap-nas-flexgroup</code> controlador, esta opción se ignora. Si no se asigna, cualquiera de los agregados disponibles puede usarse para aprovisionar un volumen FlexGroup.</p> <div>  <p>Cuando el agregado se actualiza en SVM, se actualiza automáticamente en Trident sondeando SVM sin tener que reiniciar la controladora Trident. Cuando se haya configurado un agregado específico en Trident para aprovisionar volúmenes, si se cambia el nombre de este agregado o se saca de la SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar el agregado por uno presente en la SVM o quitarlo por completo para que el back-end vuelva a estar en línea.</p> </div> <p>No especificar para sistemas ASA r2.</p>	""
limitAggregateUsage	Error al aprovisionar si el uso supera este porcentaje. Si estás usando un backend de Amazon FSx for NetApp ONTAP, no especifiques <code>limitAggregateUsage</code> . El proporcionado <code>fsxadmin</code> y <code>vsadmin</code> no contiene los permisos necesarios para recuperar el uso de agregados y limitarlo mediante Trident. No especificar para sistemas ASA r2.	"" (no se aplica de forma predeterminada)
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor. Además, restringe el tamaño máximo de los volúmenes que gestiona para las LUN.	" (no se aplica por defecto)
lunsPerFlexvol	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]	100
debugTraceFlags	<p>Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {«api»:false, «method»:true}</p> <p>No lo utilice a menos que esté solucionando problemas y necesite un volcado de log detallado.</p>	null

Parámetro	Descripción	Predeterminado
useREST	<p>Parámetro booleano para utilizar las API REST de ONTAP .</p> <div> <p><code>`useREST`</code> Cuando se establece en <code>`true`</code> Trident utiliza las API REST de ONTAP para comunicarse con el backend; cuando se configura en <code>`false`</code> Trident utiliza llamadas ONTAPI (ZAPI) para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 y versiones posteriores. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>`ontapi`</code> solicitud. Esto se satisface mediante lo predefinido <code>`vsadmin`</code> y <code>`cluster-admin`</code> roles. A partir de la versión Trident 24.06 y ONTAP 9.15.1 o posterior, <code>`useREST`</code> está configurado para <code>`true`</code> por defecto; cambiar <code>`useREST`</code> a <code>`false`</code> para utilizar llamadas ONTAPI (ZAPI).</p> </div> <p><code>`useREST`</code> está totalmente calificado para NVMe/TCP.</p> <div>  <p>NVMe solo es compatible con las API REST de ONTAP y no con ONTAPI (ZAPI).</p> </div> <p>Si se especifica, configúrelo siempre en <code>true</code> para sistemas ASA r2.</p>	<p><code>true</code> Para ONTAP 9.15.1 o posterior, de lo contrario <code>false</code>.</p>
sanType	<p>Utilice para seleccionar <code>iscsi</code> para iSCSI, <code>nvme</code> para NVMe/TCP o <code>fc</code> para SCSI over Fibre Channel (FC).</p>	<p><code>iscsi</code> si está en blanco</p>

Parámetro	Descripción	Predeterminado
formatOptions	<p>Puede <code>formatOptions</code> usarse para especificar argumentos de línea de comandos para <code>mkfs</code> el comando, que se aplicará cada vez que se formatee un volumen. Esto permite formatear el volumen según sus preferencias. Asegúrese de especificar las opciones <code>formatOptions</code> similares a las de los comandos <code>mkfs</code>, excluyendo la ruta del dispositivo. Ejemplo: «-E nodiscard»</p> <p>Compatible con <code>ontap-san</code> y <code>ontap-san-economy</code> Controladores con protocolo iSCSI. Además, compatible con sistemas ASA r2 cuando se utilizan los protocolos iSCSI y NVMe/TCP.</p>	
limitVolumePoolSize	Tamaño máximo de FlexVol solicitable al usar LUN en back-end económico de ONTAP-san.	"" (no se aplica de forma predeterminada)
denyNewVolumePools	Restringe <code>ontap-san-economy</code> los back-ends para que no creen nuevos volúmenes de FlexVol para contener sus LUN. Solo se utilizan los FlexVols preexistentes para aprovisionar nuevos VP.	

Recomendaciones para utilizar formatOptions

Trident recomienda las siguientes opciones para agilizar el proceso de formateo:

- **-E nodiscard (ext3, ext4):** No intente descartar bloques en el momento de `mkfs` (descartar bloques inicialmente es útil en dispositivos de estado sólido y almacenamiento disperso/de aprovisionamiento ligero). Esto reemplaza la opción obsoleta "-K" y es aplicable a los sistemas de archivos ext3 y ext4.
- **-K (xfs):** No intente descartar bloques en el momento de `mkfs`. Esta opción es aplicable al sistema de archivos xfs.

Autenticar Trident en un SVM backend mediante credenciales de Active Directory

Puede configurar Trident para autenticarse en un SVM de backend usando credenciales de Active Directory (AD). Antes de que una cuenta de AD pueda acceder a la SVM, debe configurar el acceso del controlador de dominio de AD al clúster o SVM. Para la administración de un clúster con una cuenta de AD, debe crear un túnel de dominio. Referirse a ["Configurar el acceso al controlador de dominio de Active Directory en ONTAP"](#) Para más detalles.

pasos

1. Configurar los ajustes del Sistema de nombres de dominio (DNS) para un SVM de backend:

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

2. Ejecute el siguiente comando para crear una cuenta de computadora para la SVM en Active Directory:

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

3. Utilice este comando para crear un usuario o grupo de AD para administrar el clúster o SVM

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

4. En el archivo de configuración del backend de Trident , configure el username y password parámetros al nombre de usuario o grupo de AD y la contraseña, respectivamente.

Opciones de configuración de back-end para el aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento predeterminado utilizando estas opciones en la `defaults` sección de la configuración. Para ver un ejemplo, vea los ejemplos de configuración siguientes.

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para las LUN	"verdadero" Si se especifica, configúrelo en true para sistemas ASA r2.
spaceReserve	Modo de reserva de espacio; «ninguno» (fino) o «volumen» (grueso). Empezar a none para sistemas ASA r2.	ninguno
snapshotPolicy	Política de Snapshot para utilizar. Empezar a none para sistemas ASA r2.	ninguno
qosPolicy	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento. Usar grupos de políticas de QoS con Trident requiere ONTAP 9 Intersight 8 o posterior. Debe usar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido aplica el techo máximo para el rendimiento total de todas las cargas de trabajo.	""
adaptiveQosPolicy	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	""
snapshotReserve	Porcentaje de volumen reservado para snapshots. No especificar para sistemas ASA r2.	«0» si snapshotPolicy no es "ninguno", de lo contrario
splitOnClone	Divida un clon de su elemento principal al crearlo	"falso"
encryption	Habilite el cifrado de volúmenes de NetApp (NVE) en el nuevo volumen; los valores predeterminados son false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster. Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Trident será habilitado NAE. Para obtener más información, consulte: "Cómo funciona Trident con NVE y NAE" .	"falso" Si se especifica, configúrelo en true para sistemas ASA r2.

Parámetro	Descripción	Predeterminado
luksEncryption	Active el cifrado LUKS. Consulte "Usar la configuración de clave unificada de Linux (LUKS)" .	"" Establecer en false para sistemas ASA r2.
tieringPolicy	Política de niveles para utilizar "ninguno" No especificar para sistemas ASA r2.	
nameTemplate	Plantilla para crear nombres de volúmenes personalizados.	""

Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los valores predeterminados 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'
```



Para todos los volúmenes creados con `ontap-san` el controlador, Trident añade un 10 % de capacidad adicional al FlexVol para acomodar los metadatos del LUN. La LUN se aprovisionará con el tamaño exacto que el usuario solicite en la RVP. Trident agrega un 10 % a FlexVol (se muestra como tamaño disponible en ONTAP). Los usuarios obtienen ahora la cantidad de capacidad utilizable que soliciten. Este cambio también impide que las LUN se conviertan en de solo lectura a menos que se utilice completamente el espacio disponible. Esto no se aplica a `ontap-san-economy`.

Para los back-ends que definen `snapshotReserve`, Trident calcula el tamaño de los volúmenes de la siguiente manera:


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

El 1.1 es el 10 por ciento adicional que Trident agrega al FlexVol para acomodar los metadatos del LUN. Para `snapshotReserve` = 5%, y la solicitud de PVC = 5 GiB, el tamaño total del volumen es 5,79 GiB y el tamaño disponible es 5,5 GiB. El `volume show` El comando debería mostrar resultados similares a este ejemplo:

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.

En la actualidad, el cambio de tamaño es la única manera de utilizar el nuevo cálculo para un volumen existente.

Ejemplos de configuración mínima

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.



Si usa Amazon FSx en NetApp ONTAP con Trident, NetApp le recomienda que especifique nombres de DNS para las LIF en lugar de direcciones IP.

Ejemplo de SAN ONTAP

Se trata de una configuración básica que utiliza el `ontap-san` controlador.

```
---
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>
```

Ejemplo de MetroCluster

Puede configurar el backend para evitar tener que actualizar manualmente la definición de backend después del switchover y el switchover durante ["Replicación y recuperación de SVM"](#).

Para una conmutación de sitios y una conmutación de estado sin problemas, especifique la SVM con managementLIF y omita svm los parámetros. Por ejemplo:

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

Ejemplo de economía de SAN ONTAP

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

Ejemplo de autenticación basada en certificados

En este ejemplo de configuración básica `clientCertificate`, `clientPrivateKey`, y `trustedCACertificate` (Opcional, si se utiliza una CA de confianza) se completan en `backend.json`. Y tome los valores codificados base64 del certificado de cliente, la clave privada y el certificado de CA de confianza, 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
```

Ejemplos de CHAP bidireccional

Estos ejemplos crean un backend con useCHAP establezca en true.

Ejemplo de CHAP de SAN de ONTAP

```
---  
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>
```

Ejemplo de CHAP de economía de SAN 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>
```

Ejemplo de NVMe/TCP

Debe tener una SVM configurada con NVMe en el back-end de ONTAP. Esta es una configuración de back-end básica 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
```

Ejemplo de SCSI sobre FC (FCP)

Debe tener una SVM configurada con FC en el back-end de ONTAP. Esta es una configuración de back-end básica 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
```

Ejemplo de configuración de backend con 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}}"
```

Ejemplo de formatOptions para el controlador 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
```

Ejemplos de back-ends con pools virtuales

En estos archivos de definición de backend de ejemplo, se establecen valores predeterminados específicos para todos los pools de almacenamiento, como `spaceReserve` en ninguno, `spaceAllocation` en falso, y `encryption` en falso. Los pools virtuales se definen en la sección de almacenamiento.

Trident establece las etiquetas de aprovisionamiento en el campo de comentarios. En las copias FlexVol volume Trident se establecen comentarios Todas las etiquetas presentes en un pool virtual para el volumen de almacenamiento durante el aprovisionamiento. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

En estos ejemplos, algunos de los pools de almacenamiento establecen sus propios `spaceReserve`, `spaceAllocation`, y `encryption` y algunos pools sustituyen los valores predeterminados.

Ejemplo de SAN ONTAP




```

---
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"

```

Ejemplo de economía de SAN 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>
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"
```

Ejemplo 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"
```

Asigne los back-ends a StorageClass

Las siguientes definiciones de StorageClass hacen referencia a la [Ejemplos de back-ends con pools virtuales](#). Con el `parameters.selector` Cada StorageClass llama la atención sobre qué pools virtuales pueden usarse para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

- La `protection-gold` StorageClass se asignará al primer pool virtual del `ontap-san` back-end. Este es el único pool que ofrece protección de nivel Gold.

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

- La `protection-not-gold` StorageClass se asignará al segundo y tercer pool virtual en `ontap-san` back-end. Estos son los únicos pools que ofrecen un nivel de protección distinto del oro.

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

- La `app-mysqldb` StorageClass se asignará al tercer pool virtual en `ontap-san-economy` back-end. Este es el único pool que ofrece configuración de pool de almacenamiento para la aplicación de tipo `mysqldb`.

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

- La `protection-silver-creditpoints-20k` StorageClass se asignará al segundo pool virtual de `ontap-san` back-end. Este es el único pool que ofrece protección de nivel plata y 20000 puntos 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"
```

- La `creditpoints-5k` StorageClass se asignará al tercer pool virtual en `ontap-san` backend y cuarto pool virtual en `ontap-san-economy` back-end. Estas son las únicas ofertas de grupo con 5000 puntos de crédito.

```

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

```

- La my-test-app-sc StorageClass se asignará al testAPP pool virtual en el ontap-san conductor con sanType: nvme. Esta es la única oferta de pool 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"

```

Trident decidirá qué pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

Unidades NAS de ONTAP

Información general del controlador NAS de ONTAP

Obtenga información sobre la configuración de un back-end de ONTAP con controladores NAS de ONTAP y Cloud Volumes ONTAP.

Información del controlador NAS de ONTAP

Trident proporciona los siguientes controladores de almacenamiento NAS para comunicarse con el clúster de ONTAP. Los modos de acceso admitidos son: *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-nas	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	« », nfs, smb

Controlador	Protocolo	VolumeMo de	Modos de acceso compatibles	Sistemas de archivos compatibles
ontap-nas-economy	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	« », nfs, smb
ontap-nas-flexgroup	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	« », nfs, smb



- Uso `ontap-san-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)".
- Uso `ontap-nas-economy` solo si se espera que el número de uso de volúmenes persistentes sea superior a "[Límites de volumen ONTAP compatibles](#)" y la `ontap-san-economy` no se puede utilizar el conductor.
- No utilizar `ontap-nas-economy` si prevé la necesidad de protección de datos, recuperación ante desastres o movilidad.
- NetApp no recomienda el uso de crecimiento automático de FlexVol en todos los controladores de ONTAP, excepto ONTAP-san. Como solución alternativa, Trident admite el uso de la reserva Snapshot y escala los volúmenes de FlexVol en consecuencia.

Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente utilizando el usuario del clúster o `vsadmin` un usuario de SVM, `admin` o bien como usuario con un nombre distinto que tenga el mismo rol.

Para puestas en marcha de Amazon FSx para NetApp ONTAP, Trident espera ejecutarse como administrador de ONTAP o SVM, utilizando el usuario del clúster `fsxadmin` o un `vsadmin` usuario de SVM, o como un usuario con un nombre distinto que tenga el mismo rol. `fsxadmin` El usuario es un sustituto limitado para el usuario administrador del clúster.



Si se usa `limitAggregateUsage` el parámetro, se requieren permisos de administrador del clúster. Cuando se usa Amazon FSx para NetApp ONTAP con Trident, el `limitAggregateUsage` parámetro no funcionará con `vsadmin` las cuentas de usuario y `fsxadmin` La operación de configuración generará un error si se especifica este parámetro.

Si bien es posible crear un rol más restrictivo dentro de ONTAP que puede utilizar un controlador Trident, no lo recomendamos. La mayoría de las nuevas versiones de Trident denominan API adicionales que se tendrían que tener en cuenta, por lo que las actualizaciones son complejas y propensas a errores.

Prepárese para configurar un back-end con controladores NAS de ONTAP

Conozca los requisitos, las opciones de autenticación y las políticas de exportación para configurar un backend de ONTAP con controladores NAS de ONTAP.

A partir de la versión 25.10, NetApp Trident es compatible con "[Sistema de almacenamiento NetApp AFX](#)". Los sistemas de almacenamiento NetApp AFX se diferencian de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento.



Solo el `ontap-nas` El controlador (con protocolo NFS) es compatible con los sistemas AFX; el protocolo SMB no es compatible.

En la configuración del backend de Trident , no es necesario especificar que su sistema sea AFX. Cuando selecciona `ontap-nas` como el `storageDriverName` Trident detecta automáticamente los sistemas AFX.

Requisitos

- Para todos los backends de ONTAP, Trident requiere que se asigne al menos un agregado al SVM.
- Puede ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, puede configurar una clase Gold que utilice `ontap-nas` Controlador y clase Bronze que utiliza `ontap-nas-economy` uno.
- Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas NFS adecuadas. Consulte ["aquí"](#) para obtener más detalles.
- Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows. Consulte [Prepárese para aprovisionar los volúmenes de SMB](#) para obtener más información.

Autentique el backend de ONTAP

Trident ofrece dos modos de autenticación de un backend ONTAP.

- Basado en Credenciales: Este modo requiere permisos suficientes para el backend de ONTAP. Se recomienda utilizar una cuenta asociada con un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin` Garantizar la máxima compatibilidad con versiones de ONTAP.
- Basado en certificado: Este modo requiere un certificado instalado en el back-end para que Trident se comunique con un clúster de ONTAP. Aquí, la definición de backend debe contener valores codificados en Base64 del certificado de cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

Puede actualizar los back-ends existentes para moverse entre métodos basados en credenciales y basados en certificados. Sin embargo, solo se admite un método de autenticación a la vez. Para cambiar a un método de autenticación diferente, debe eliminar el método existente de la configuración del back-end.



Si intenta proporcionar **tanto credenciales como certificados**, la creación de backend fallará y se producirá un error en el que se haya proporcionado más de un método de autenticación en el archivo de configuración.

Habilite la autenticación basada en credenciales

Trident requiere que las credenciales se comuniquen con un administrador de SVM o con el ámbito del clúster para que se comunique con el back-end de ONTAP. Se recomienda hacer uso de roles estándar, predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad con futuras versiones de ONTAP que podrían exponer API de funciones que podrán utilizarse en futuras versiones de Trident. Puede crearse y utilizarse un rol de inicio de sesión de seguridad personalizado con Trident, pero no se recomienda.

Una definición de backend de ejemplo tendrá este aspecto:

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"
  }
}
```

Tenga en cuenta que la definición de backend es el único lugar en el que las credenciales se almacenan en texto sin formato. Una vez creado el back-end, los nombres de usuario y las contraseñas se codifican con Base64 y se almacenan como secretos de Kubernetes. La creación/mejora de un backend es el único paso que requiere conocimiento de las credenciales. Por tanto, es una operación de solo administración que deberá realizar el administrador de Kubernetes o almacenamiento.

Habilite la autenticación basada en certificados

Los back-ends nuevos y existentes pueden utilizar un certificado y comunicarse con el back-end de ONTAP. Se necesitan tres parámetros en la definición de backend.

- ClientCertificate: Valor codificado en base64 del certificado de cliente.
- ClientPrivateKey: Valor codificado en base64 de la clave privada asociada.
- TrustedCACertificate: Valor codificado en base64 del certificado de CA de confianza. Si se utiliza una CA de confianza, se debe proporcionar este parámetro. Esto se puede ignorar si no se utiliza ninguna CA de confianza.

Un flujo de trabajo típico implica los pasos siguientes.

Pasos

1. Genere una clave y un certificado de cliente. Al generar, establezca el nombre común (CN) en el usuario de ONTAP para autenticarse como.

```
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. Añada un certificado de CA de confianza al clúster ONTAP. Es posible que ya sea gestionado por el administrador de almacenamiento. Ignore si no se utiliza ninguna CA de confianza.

```
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 el certificado y la clave de cliente (desde el paso 1) en el clúster 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 los compatibilidad con el rol de inicio de sesión de seguridad ONTAP cert método de autenticación.

```
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. Probar la autenticación mediante un certificado generado. Reemplace <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre de SVM. Debe asegurarse de que la LIF tiene su política de servicio establecida en 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 certificados, claves y certificados de CA de confianza con Base64.

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

7. Cree un backend utilizando los valores obtenidos del paso 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
NasBackend	ontap-nas	98e19b74-aec7-4a3d-8dcf-128e5033b214

Actualice los métodos de autenticación o gire las credenciales

Puede actualizar un back-end existente para utilizar un método de autenticación diferente o para rotar sus credenciales. Esto funciona de las dos maneras: Los back-ends que utilizan nombre de usuario/contraseña se pueden actualizar para usar certificados. Los back-ends que utilizan certificados pueden actualizarse a nombre de usuario/contraseña. Para ello, debe eliminar el método de autenticación existente y agregar el nuevo método de autenticación. A continuación, utilice el archivo backend.json actualizado que contiene los parámetros necesarios para ejecutarse `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
NasBackend	ontap-nas	98e19b74-aec7-4a3d-8dcf-128e5033b214



Cuando gira contraseñas, el administrador de almacenamiento debe actualizar primero la contraseña del usuario en ONTAP. A esto le sigue una actualización de back-end. Al rotar certificados, se pueden agregar varios certificados al usuario. A continuación, el back-end se actualiza para usar el nuevo certificado, siguiendo el cual se puede eliminar el certificado antiguo del clúster de ONTAP.

La actualización de un back-end no interrumpe el acceso a los volúmenes que se han creado ni afecta a las conexiones de volúmenes realizadas después. Una actualización de back-end correcta indica que Trident puede comunicarse con el back-end de ONTAP y manejar operaciones de volumen futuras.

Crear rol de ONTAP personalizado para Trident

Puede crear un rol de clúster de ONTAP con un Privileges mínimo de modo que no tenga que utilizar el rol de administrador de ONTAP para realizar operaciones en Trident. Cuando incluye el nombre de usuario en una configuración de back-end de Trident, Trident utiliza el rol de clúster de ONTAP que creó para realizar las operaciones.

Consulte "[Generador de roles personalizados de Trident](#)" para obtener más información sobre la creación de roles personalizados de Trident.

Con la CLI de ONTAP

1. Cree un rol nuevo mediante el siguiente comando:

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

2. Cree un nombre de usuario para el usuario de 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. Asignar el rol al usuario:

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

Mediante System Manager

Realice los pasos siguientes en ONTAP System Manager:

1. **Crear un rol personalizado:**

- a. Para crear un rol personalizado a nivel de clúster, seleccione **Cluster > Settings**.

(O) Para crear un rol personalizado en el nivel de SVM, seleccione **Almacenamiento > Storage VMs > required svm > Settings > Users and Roles**.

- b. Seleccione el icono de flecha (→) junto a **Usuarios y roles**.

- c. Seleccione **+Agregar** en **Roles**.

- d. Defina las reglas para el rol y haga clic en **Guardar**.

2. **Asignar el rol al usuario de Trident:** + Realizar los siguientes pasos en la página **Usuarios y Roles**:

- a. Seleccione Agregar icono **+** en **Usuarios**.

- b. Seleccione el nombre de usuario requerido y seleccione un rol en el menú desplegable para **Rol**.

- c. Haga clic en **Guardar**.

Consulte las siguientes páginas si quiere más información:

- ["Roles personalizados para la administración de ONTAP"](#) o. ["Definir funciones personalizadas"](#)
- ["Trabajar con roles y usuarios"](#)

Gestione las políticas de exportación de NFS

Trident utiliza políticas de exportación de NFS para controlar el acceso a los volúmenes que aprovisiona.

Trident proporciona dos opciones al trabajar con políticas de exportación:

- Trident puede gestionar de manera dinámica la política de exportación; en este modo de funcionamiento,

el administrador de almacenamiento especifica una lista de bloques CIDR que representan direcciones IP admisibles. Trident agrega IP de nodo aplicables que se encuentran en estos rangos a la política de exportación de forma automática en el momento de la publicación. Como alternativa, cuando no se especifica ningún CIDR, todas las IP de unidifusión de ámbito global que se encuentran en el nodo en el que se publica el volumen se agregarán a la política de exportación.

- Los administradores de almacenamiento pueden crear una normativa de exportación y añadir reglas manualmente. Trident utiliza la política de exportación predeterminada a menos que se especifique otro nombre de política de exportación en la configuración.

Gestione de forma dinámica políticas de exportación

Trident proporciona la capacidad de gestionar dinámicamente políticas de exportación para back-ends de ONTAP. De este modo, el administrador de almacenamiento puede especificar un espacio de direcciones permitido para las IP de nodos de trabajo, en lugar de definir reglas explícitas de forma manual. Simplifica en gran medida la gestión de políticas de exportación; las modificaciones de la política de exportación ya no requieren intervención manual en el clúster de almacenamiento. Además, esto ayuda a restringir el acceso al clúster de almacenamiento solo a los nodos de trabajador que se montan volúmenes y que tienen IP en el rango especificado, lo que permite una gestión automatizada y precisa.



No utilice la traducción de direcciones de red (NAT) cuando utilice políticas de exportación dinámicas. Con NAT, el controlador de almacenamiento ve la dirección NAT de frontend y no la dirección de host IP real, por lo que el acceso se denegará cuando no se encuentre ninguna coincidencia en las reglas de exportación.

Ejemplo

Hay dos opciones de configuración que deben utilizarse. He aquí un ejemplo de definición 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
```



Al usar esta función, debe asegurarse de que la unión raíz de la SVM tenga una política de exportación creada previamente con una regla de exportación que permite el bloque CIDR de nodo (como la política de exportación predeterminada). Siga siempre las prácticas recomendadas por NetApp para dedicar una SVM para Trident.

A continuación se ofrece una explicación del funcionamiento de esta función utilizando el ejemplo anterior:

- `autoExportPolicy` se establece en `true`. Esto indica que Trident crea una política de exportación para cada volumen provisionado con este back-end para `svm1` la SVM y administra la adición y eliminación de

reglas mediante `autoExportCIDRs` bloques de direcciones. Hasta que un volumen se conecta a un nodo, el volumen usa una política de exportación vacía sin reglas para evitar el acceso no deseado a ese volumen. Cuando se publica un volumen en un nodo, Trident crea una política de exportación con el mismo nombre que el `qtree` subyacente que contiene la IP de nodo en el bloque CIDR especificado. Estas IP también se agregarán a la política de exportación utilizada por la FlexVol volume principal

- Por ejemplo:

- UUID de backend `403b5326-8482-40dB-96d0-d83fb3f4daec`
- `autoExportPolicy` establezca en `true`
- prefijo de almacenamiento `trident`
- PVC UUID `a79bcf5f-7b6d-4a40-9876-e2551f159c1c`
- el `qtree` denominado `Trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` crea una política de exportación para la FlexVol llamada `trident-403b5326-8482-40db96d0-d83fb3f4daec`, una política de exportación para el `qtree` llamado `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` y una política de exportación vacía denominada `trident_empty` en la SVM. Las reglas de la política de exportación de FlexVol serán un superconjunto de reglas contenidas en las políticas de exportación de `qtree`. La política de exportación vacía será reutilizada por cualquier volumen que no esté asociado.

- `autoExportCIDRs` contiene una lista de bloques de direcciones. Este campo es opcional y se establece de forma predeterminada en `["0.0.0.0/0", "":"/0"]`. Si no se define, Trident agrega todas las direcciones unicast de ámbito global que se encuentran en los nodos de trabajo con publicaciones.

En este ejemplo, `192.168.0.0/24` se proporciona el espacio de la dirección. Esto indica que las IP de nodo de Kubernetes que se encuentran dentro de este rango de direcciones con publicaciones se agregarán a la política de exportación que crea Trident. Cuando Trident registra un nodo en el que se ejecuta, recupera las direcciones IP del nodo y las comprueba con respecto a los bloques de direcciones proporcionados en `autoExportCIDRs`. En el momento de la publicación, después de filtrar las IP, Trident crea las reglas de política de exportación para las IP del cliente para el nodo en el que está publicando.

Puede actualizar `autoExportPolicy` y `autoExportCIDRs` para los back-ends después de crearlos. Puede añadir CIDR nuevos para un back-end que se gestiona o elimina automáticamente CIDR existentes. Tenga cuidado al eliminar CIDR para asegurarse de que las conexiones existentes no se hayan caído. También puede optar por desactivar `autoExportPolicy` para un back-end y caer en una política de exportación creada manualmente. Esto requerirá establecer la `exportPolicy` parámetro en la configuración del back-end.

Después de que Trident cree o actualice un backend, puede comprobar el backend utilizando `tridentctl` o el CRD correspondiente `tridentbackend`:

```
./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
```

Cuando se elimina un nodo, Trident comprueba todas las políticas de exportación para eliminar las reglas de acceso correspondientes al nodo. Al eliminar esta IP de nodo de las políticas de exportación de los back-ends gestionados, Trident evita los montajes no autorizados, a menos que un nuevo nodo del clúster reutilice esta IP.

Para los back-ends existentes anteriormente, al actualizar el backend con `tridentctl update backend` se garantiza que Trident administre las políticas de exportación automáticamente. Esto crea dos nuevas políticas de exportación llamadas después del UUID del back-end y el nombre de `qtree` cuando son necesarias. Los volúmenes presentes en el back-end utilizarán las políticas de exportación recién creadas después de desmontarlas y montarlas de nuevo.



Si se elimina un back-end con políticas de exportación gestionadas automáticamente, se eliminará la política de exportación creada de forma dinámica. Si se vuelve a crear el back-end, se trata como un nuevo back-end y dará lugar a la creación de una nueva política de exportación.

Si se actualiza la dirección IP de un nodo activo, debe reiniciar el pod de Trident en el nodo. A continuación, Trident actualizará la política de exportación de los back-ends que gestiona para reflejar este cambio de IP.

Prepárese para aprovisionar los volúmenes de SMB

Con un poco de preparación adicional, puede aprovisionar volúmenes SMB con `ontap-nas` de windows



Debe configurar tanto los protocolos NFS como SMB/CIFS en la SVM para crear `ontap-nas-economy` un volumen SMB para los clústeres de ONTAP en las instalaciones. Si no se configura ninguno de estos protocolos, se producirá un error en la creación del volumen de SMB.



autoExportPolicy No es compatible con los volúmenes de SMB.

Antes de empezar

Para poder aprovisionar volúmenes de SMB, debe tener lo siguiente.

- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2022. Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto Trident que contiene sus credenciales de Active Directory. Para generar secreto smbcreds:

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

- Proxy CSI configurado como servicio de Windows. Para configurar un csi-proxy, consulte ["GitHub: Proxy CSI"](#) o ["GitHub: Proxy CSI para Windows"](#) Para nodos Kubernetes que se ejecutan en Windows.

Pasos

1. Para la ONTAP en las instalaciones, puede crear un recurso compartido de SMB, o bien Trident puede crearlo para usted.



Los recursos compartidos de SMB se requieren para Amazon FSx para ONTAP.

Puede crear recursos compartidos de administrador de SMB de una de dos formas mediante el ["Consola de administración de Microsoft"](#) Complemento carpetas compartidas o uso de la CLI de ONTAP. Para crear los recursos compartidos de SMB mediante la CLI de ONTAP:

- a. Si es necesario, cree la estructura de ruta de acceso de directorio para el recurso compartido.

La `vserver cifs share create` comando comprueba la ruta especificada en la opción `-path` durante la creación del recurso compartido. Si la ruta especificada no existe, el comando falla.

- b. Cree un recurso compartido de SMB asociado con la SVM especificada:

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

- c. Compruebe que se ha creado el recurso compartido:

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



Consulte ["Cree un recurso compartido de SMB"](#) para obtener todos los detalles.

2. Al crear el back-end, debe configurar lo siguiente para especificar volúmenes de SMB. Para obtener información sobre todas las opciones de configuración del entorno de administración de ONTAP, consulte

"Opciones y ejemplos de configuración de FSX para ONTAP".

Parámetro	Descripción	Ejemplo
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado mediante la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP; un nombre para permitir que Trident cree el recurso compartido de SMB; o bien puede dejar el parámetro en blanco para evitar el acceso de recurso compartido común a los volúmenes. Este parámetro es opcional para ONTAP en las instalaciones. Este parámetro es necesario para los back-ends de Amazon FSx para ONTAP y no puede estar en blanco.	smb-share
nasType	Debe establecer en smb. Si es nulo, el valor predeterminado es <code>nfs</code> .	smb
securityStyle	Estilo de seguridad para nuevos volúmenes. Debe estar configurado en ntfs o. mixed Para volúmenes SMB.	ntfs o. mixed Para volúmenes de SMB
unixPermissions	Modo para volúmenes nuevos. Se debe dejar vacío para volúmenes SMB.	""

Habilitar SMB seguro

A partir de la versión 25.06, NetApp Trident admite el aprovisionamiento seguro de volúmenes SMB creados mediante `ontap-nas` y `ontap-nas-economy` Backends. Al habilitar SMB seguro, se puede proporcionar acceso controlado a los recursos compartidos de SMB para usuarios y grupos de usuarios de Active Directory (AD) mediante listas de control de acceso (ACL).

Puntos que debe recordar

- Importador `ontap-nas-economy` Los volúmenes no son compatibles.
- Solo se admiten clones de solo lectura. `ontap-nas-economy` volúmenes.
- Si SMB seguro está habilitado, Trident ignorará el recurso compartido SMB mencionado en el backend.
- La actualización de la anotación de PVC, la anotación de la clase de almacenamiento y el campo `backend` no actualiza la ACL del recurso compartido SMB.
- La ACL de recurso compartido SMB especificada en la anotación del PVC clonado tendrá prioridad sobre las del PVC de origen.
- Asegúrese de proporcionar usuarios de AD válidos al habilitar SMB seguro. Los usuarios no válidos no se añadirán a la ACL.
- Si proporciona el mismo usuario de AD en el backend, la clase de almacenamiento y PVC con diferentes permisos, la prioridad de permisos será: PVC, clase de almacenamiento y luego backend.
- SMB seguro es compatible con `ontap-nas` importaciones de volumen gestionadas y no aplicable a importaciones de volumen no gestionadas.

Pasos

1. Especifique `adAdminUser` en `TridentBackendConfig` como se muestra en el siguiente ejemplo:

```

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. Añade la anotación en la clase de almacenamiento.

Añade el `trident.netapp.io/smbShareAdUser` Anotación a la clase de almacenamiento para habilitar SMB seguro sin fallos. El valor de usuario especificado para la anotación `trident.netapp.io/smbShareAdUser` debe ser el mismo que el nombre de usuario especificado en el `smbcreds` `secreto`. es `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. Cree una PVC.

El siguiente ejemplo crea una 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

```

Opciones y ejemplos de configuración NAS de ONTAP

Aprenda a crear y utilizar controladores NAS de ONTAP con su instalación de Trident. Esta sección proporciona ejemplos de configuración de backend y detalles para la asignación de back-ends a StorageClasses.

A partir de la versión 25.10, NetApp Trident es compatible con ["Sistemas de almacenamiento NetApp AFX"](#) . Los sistemas de almacenamiento NetApp AFX se diferencian de otros sistemas basados en ONTAP(ASA, AFF y FAS) en la implementación de su capa de almacenamiento.



Solo el `ontap-nas` El controlador (con protocolo NFS) es compatible con los sistemas NetApp AFX; el protocolo SMB no es compatible.


En la configuración del backend de Trident , no es necesario especificar que su sistema sea un sistema de almacenamiento NetApp AFX. Cuando selecciona `ontap-nas` como el `storageDriverName` Trident detecta automáticamente el sistema de almacenamiento AFX. Algunos parámetros de configuración del backend no son aplicables a los sistemas de almacenamiento AFX, como se indica en la tabla siguiente.


Opciones de configuración del back-end


Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Predeterminado
version		Siempre 1

Parámetro	Descripción	Predeterminado
storageDriveName	<p>Nombre del controlador de almacenamiento</p> <div>  <p>Para sistemas NetApp AFX, solo ontap-nas está soportado.</p> </div>	ontap-nas, , ontap-nas-economy o. ontap-nas-flexgroup
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + «_» + LIF de datos
managementLIF	<p>Dirección IP de un clúster o una LIF de gestión de SVM Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555] como . Para una conmutación de sitios MetroCluster fluida, consulte Ejemplo de MetroCluster.</p>	«10.0.0.1», «[2001:1234:abcd::fefe]»
dataLIF	<p>Dirección IP de LIF de protocolo. NetApp recomienda especificar dataLIF. Si no se proporciona, Trident recupera las LIF de datos de la SVM. Puede especificar un nombre de dominio completo (FQDN) que se utilice para las operaciones de montaje de NFS, lo que permite crear un DNS por turnos para equilibrar la carga en varias LIF de datos. Se puede cambiar después del ajuste inicial. Consulte . Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555] como . Omitir para MetroCluster. Consulte la Ejemplo de MetroCluster.</p>	Dirección especificada o derivada de la SVM, si no se especifica (no recomendada)
svm	<p>Máquina virtual de almacenamiento que usar</p> <p>Omitir para MetroCluster. Ver Ejemplo de MetroCluster.</p>	Derivado si una SVM managementLIF está especificado
autoExportPolicy	Habilite la creación y actualización automática de la política de exportación [Boolean]. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	falso
autoExportCIDRs	Lista de CIDRs para filtrar las IP del nodo de Kubernetes contra cuando autoExportPolicy se habilita. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	[«0.0.0/0», «:/0»]
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""

Parámetro	Descripción	Predeterminado
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados	""
username	Nombre de usuario para conectarse al clúster/SVM. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulte "Autenticar Trident en un SVM backend mediante credenciales de Active Directory" .	
password	Contraseña para conectarse al cluster/SVM. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulte "Autenticar Trident en un SVM backend mediante credenciales de Active Directory" .	
storagePrefix	<p>El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede actualizar después de configurarlo</p> <div>  <p>Al utilizar ONTAP-nas-economy y un prefijo de almacenamiento con 24 caracteres o más, los qtrees no tendrán el prefijo de almacenamiento incrustado, pero estarán en el nombre del volumen.</p> </div>	«trident»

Parámetro	Descripción	Predeterminado
aggregate	<p>Agregado para el aprovisionamiento (opcional; si se establece, se debe asignar a la SVM). Para el <code>ontap-nas-flexgroup</code> controlador, esta opción se ignora. Si no se asigna, cualquiera de los agregados disponibles puede usarse para aprovisionar un volumen FlexGroup.</p> <div>  <p>Cuando el agregado se actualiza en SVM, se actualiza automáticamente en Trident sondeando SVM sin tener que reiniciar la controladora Trident. Cuando se haya configurado un agregado específico en Trident para aprovisionar volúmenes, si se cambia el nombre de este agregado o se saca de la SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar el agregado por uno presente en la SVM o quitarlo por completo para que el back-end vuelva a estar en línea.</p> </div> <p>No especificar para sistemas de almacenamiento AFX.</p>	""
limitAggregateUsage	<p>Fallará el aprovisionamiento si el uso supera este porcentaje. No se aplica a Amazon FSx para ONTAP. No especificar para sistemas de almacenamiento AFX.</p>	"" (no se aplica de forma predeterminada)

Parámetro	Descripción	Predeterminado
Lista de Agregados de Flexgroup	<p>Lista de agregados para el aprovisionamiento (opcional; si se ha definido, debe asignarse a la SVM). Todos los agregados asignados a la SVM se usan para aprovisionar un volumen FlexGroup. Compatible con el controlador de almacenamiento ONTAP-nas-FlexGroup.</p> <div>  <p>Cuando la lista de agregados se actualiza en SVM, la lista se actualiza automáticamente en Trident sondeando la SVM sin tener que reiniciar la controladora Trident. Cuando se configuró una lista de agregado específica en Trident para aprovisionar volúmenes, si se cambia el nombre de la lista de agregados o se sale de SVM, el back-end se moverá al estado Failed en Trident mientras se sondea el agregado de SVM. Debe cambiar la lista de agregados por una que esté presente en la SVM o quitarla por completo para que el back-end vuelva a estar en línea.</p> </div>	""
limitVolumeSize	Fallará el aprovisionamiento si el tamaño de volumen solicitado supera este valor.	" (no se aplica por defecto)
debugTraceFlags	<p>Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {«api»:false, «method»:true}</p> <p>No utilizar debugTraceFlags a menos que esté solucionando problemas y necesite un volcado de registro detallado.</p>	nulo
nasType	Configure la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o nulo. Si se establece en nulo, se utilizarán volúmenes NFS por defecto. Si se especifica, siempre se establecerá en <code>nfs</code> para sistemas de almacenamiento AFX.	<code>nfs</code>

Parámetro	Descripción	Predeterminado
nfsMountOptions	Lista de opciones de montaje NFS separadas por comas. Las opciones de montaje para los volúmenes persistentes de Kubernetes se especifican normalmente en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident volverá a utilizar las opciones de montaje especificadas en el archivo de configuración del back-end de almacenamiento. Si no se especifican opciones de montaje en la clase almacenamiento o el archivo de configuración, Trident no definirá ninguna opción de montaje en un volumen persistente asociado.	""
qtreesPerFlexvol	El número máximo de qtrees por FlexVol debe estar comprendido entre [50, 300]	«200»
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado mediante la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP; un nombre para permitir que Trident cree el recurso compartido de SMB; o bien puede dejar el parámetro en blanco para evitar el acceso de recurso compartido común a los volúmenes. Este parámetro es opcional para ONTAP en las instalaciones. Este parámetro es necesario para los back-ends de Amazon FSx para ONTAP y no puede estar en blanco.	smb-share
useREST	Parámetro booleano para utilizar las API REST de ONTAP. <code>useREST</code> Cuando se configura para <code>true</code> Trident utiliza las API REST de ONTAP para comunicarse con el backend; cuando se configura en <code>false</code> Trident utiliza llamadas ONTAPI (ZAPI) para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 y versiones posteriores. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontapi</code> solicitud. Esto se satisface mediante lo predefinido. <code>vsadmin</code> y <code>cluster-admin</code> roles. A partir de la versión Trident 24.06 y ONTAP 9.15.1 o posterior, <code>useREST</code> está configurado para <code>true</code> por defecto; cambiar <code>useREST</code> a <code>false</code> para utilizar llamadas ONTAPI (ZAPI). Si se especifica, siempre se establecerá en <code>true</code> para sistemas de almacenamiento AFX.	<code>true</code> Para ONTAP 9.15.1 o posterior, de lo contrario <code>false</code> .
limitVolumePoolSize	Tamaño máximo de FlexVol que se puede solicitar cuando se utilizan qtrees en el back-end económico de ONTAP-nas.	"" (no se aplica de forma predeterminada)
denyNewVolumePools	Restringe <code>ontap-nas-economy</code> los back-ends de la creación de nuevos volúmenes de FlexVol para contener sus Qtrees. Solo se utilizan los FlexVols preexistentes para aprovisionar nuevos VP.	

Parámetro	Descripción	Predeterminado
adAdminUser	Usuario o grupo de usuarios administradores de Active Directory con acceso total a los recursos compartidos SMB. Utilice este parámetro para otorgar derechos de administrador al recurso compartido SMB con control total.	

Opciones de configuración de back-end para el aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento predeterminado utilizando estas opciones en la `defaults` sección de la configuración. Para ver un ejemplo, vea los ejemplos de configuración siguientes.

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para Qtrees	verdadero
spaceReserve	Modo de reserva de espacio; «ninguno» (fino) o «volumen» (grueso)	ninguno
snapshotPolicy	Política de Snapshot que se debe usar	ninguno
qosPolicy	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	""
adaptiveQosPolicy	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento. no admitido por ontap-nas-Economy.	""
snapshotReserve	Porcentaje de volumen reservado para las Snapshot	«0» si snapshotPolicy no es "ninguno", de lo contrario
splitOnClone	Divida un clon de su elemento principal al crearlo	"falso"
encryption	Habilite el cifrado de volúmenes de NetApp (NVE) en el nuevo volumen; los valores predeterminados son false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster. Si NAE está habilitado en el back-end, cualquier volumen aprovisionado en Trident será habilitado NAE. Para obtener más información, consulte: "Cómo funciona Trident con NVE y NAE" .	"falso"
tieringPolicy	Política de organización en niveles para utilizar ninguna	
unixPermissions	Modo para volúmenes nuevos	«777» para volúmenes NFS; vacío (no aplicable) para volúmenes SMB
snapshotDir	Controla el acceso al .snapshot directorio	"True" para NFSv4 "false" para NFSv3

Parámetro	Descripción	Predeterminado
exportPolicy	Política de exportación que se va a utilizar	"predeterminado"
securityStyle	Estilo de seguridad para nuevos volúmenes. Compatibilidad con NFS mixed y.. unix estilos de seguridad. SMB admite mixed y.. ntfs estilos de seguridad.	El valor predeterminado de NFS es unix. La opción predeterminada de SMB es ntfs.
nameTemplate	Plantilla para crear nombres de volúmenes personalizados.	""



Usar grupos de políticas de QoS con Trident requiere ONTAP 9 Intersight 8 o posterior. Debe usar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido aplica el techo máximo para el rendimiento total de todas las cargas de trabajo.

Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los valores predeterminados 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 y ontap-nas-flexgroups Trident ahora utiliza un nuevo cálculo para garantizar que el FlexVol tenga el tamaño correcto con el porcentaje de snapshotReserve y el PVC. Cuando el usuario solicita

un PVC, Trident crea el FlexVol original con más espacio mediante el nuevo cálculo. Este cálculo garantiza que el usuario reciba el espacio de escritura que solicitó en el PVC, y no menos espacio del que solicitó. Antes de la versión v21.07, cuando el usuario solicitaba un PVC (por ejemplo, 5 GiB), con el snapshotReserve al 50 %, obtenía solo 2,5 GiB de espacio de escritura. Esto se debe a que lo que el usuario solicitó fue el volumen completo y snapshotReserve es un porcentaje de eso. Con Trident 21.07, lo que el usuario solicita es el espacio de escritura y Trident define el snapshotReserve número como porcentaje del volumen total. Esto no se aplica a `ontap-nas-economy`. Vea el siguiente ejemplo para ver cómo funciona

El cálculo es el siguiente:

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

Para snapshotReserve = 50% y la solicitud de PVC = 5 GiB, el tamaño total del volumen es $5/0.5 = 10$ GiB y el tamaño disponible es 5 GiB, que es lo que el usuario solicitó en la solicitud de PVC. `volume show` El comando debería mostrar resultados similares a este ejemplo:

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.

Los backends existentes de instalaciones anteriores aprovisionarán volúmenes como se explicó anteriormente al actualizar Trident. Para los volúmenes creados antes de la actualización, debe redimensionarlos para que se observe el cambio. Por ejemplo, un PVC de 2 GiB con snapshotReserve=50. Anteriormente, se generó un volumen que proporciona 1 GiB de espacio de escritura. Por ejemplo, al redimensionar el volumen a 3 GiB, la aplicación obtiene 3 GiB de espacio de escritura en un volumen de 6 GiB.

Ejemplos de configuración mínima

Los ejemplos siguientes muestran configuraciones básicas que dejan la mayoría de los parámetros en los valores predeterminados. Esta es la forma más sencilla de definir un back-end.



Si utiliza Amazon FSX en ONTAP de NetApp con Trident, la recomendación es especificar nombres DNS para las LIF en lugar de direcciones IP.

Ejemplo de economía NAS de ONTAP

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

Ejemplo de FlexGroup NAS de ONTAP

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

Ejemplo de MetroCluster

Puede configurar el backend para evitar tener que actualizar manualmente la definición de backend después del switchover y el switchover durante ["Replicación y recuperación de SVM"](#).

Para obtener una conmutación de sitios y una conmutación de estado sin problemas, especifique la SVM con managementLIF y omita la dataLIF y.. svm parámetros. Por ejemplo:

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

Ejemplo de volúmenes de 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
```

Ejemplo de autenticación basada en certificados

Este es un ejemplo de configuración de backend mínima. `clientCertificate`, `clientPrivateKey`, y `trustedCACertificate` (Opcional, si se utiliza una CA de confianza) se completan en `backend.json` Y tome los valores codificados base64 del certificado de cliente, la clave privada y el certificado de CA de confianza, 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_
```

Ejemplo de política de exportación automática

En este ejemplo, se muestra cómo puede indicar a Trident que utilice políticas de exportación dinámicas para crear y gestionar la política de exportación automáticamente. Esto funciona igual para `ontap-nas-economy` los controladores y `ontap-nas-flexgroup`

```
---
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
```

Ejemplo de direcciones IPv6

Este ejemplo muestra managementLIF Uso de una dirección 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
```

Ejemplo de Amazon FSx para ONTAP mediante volúmenes de bloque de mensajes del servidor

La smbShare El parámetro es obligatorio para FSx para ONTAP mediante volúmenes de bloque de mensajes del servidor.

```
---
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_
```

Ejemplo de configuración de backend con 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}}"
```

Ejemplos de back-ends con pools virtuales

En los archivos de definición de backend de ejemplo que se muestran a continuación, se establecen valores predeterminados específicos para todos los pools de almacenamiento, como `spaceReserve` en ninguno, `spaceAllocation` en falso, y `encryption` en falso. Los pools virtuales se definen en la sección de almacenamiento.

Trident establece las etiquetas de aprovisionamiento en el campo de comentarios. Los comentarios se establecen en FlexVol for ontap-nas o FlexGroup para ontap-nas-flexgroup. Trident copia todas las etiquetas presentes en un pool virtual en el volumen de almacenamiento durante el aprovisionamiento. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

En estos ejemplos, algunos de los pools de almacenamiento establecen sus propios `spaceReserve`, `spaceAllocation`, y `encryption` y algunos pools sustituyen los valores predeterminados.

Ejemplo de NAS de ONTAP

```
---
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"
```

```
---
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"
```

Ejemplo de economía NAS de ONTAP

```
---
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"
```

Asigne los back-ends a StorageClass

Las siguientes definiciones de StorageClass se refieren a [Ejemplos de back-ends con pools virtuales](#). Con el `parameters.selector` Cada StorageClass llama la atención sobre qué pools virtuales pueden usarse para alojar un volumen. El volumen tendrá los aspectos definidos en el pool virtual elegido.

- La `protection-gold` StorageClass se asignará al primer y segundo pool virtual del `ontap-nas-flexgroup` back-end. Estos son los únicos pools que ofrecen protección de nivel Gold.

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

- La `protection-not-gold` StorageClass se asignará al tercer y cuarto pool virtual del `ontap-nas-flexgroup` back-end. Estos son los únicos pools que ofrecen un nivel de protección distinto al Gold.

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

- La `app-mysqldb` StorageClass se asignará al cuarto pool virtual del `ontap-nas` back-end. Este es el único pool que ofrece configuración de pool de almacenamiento para la aplicación de tipo `mysqldb`.

```

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

```

- T. protection-silver-creditpoints-20k StorageClass se asignará al tercer pool virtual del ontap-nas-flexgroup back-end. Este es el único pool que ofrece protección de nivel plata y 20000 puntos 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"

```

- La creditpoints-5k StorageClass se asignará al tercer pool virtual del ontap-nas backend y segundo pool virtual en ontap-nas-economy back-end. Estas son las únicas ofertas de grupo con 5000 puntos de crédito.

```

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

```

Trident decidirá qué pool virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

Actualizar dataLIF tras la configuración inicial

Puede cambiar la LIF de datos después de la configuración inicial. Para ello, ejecute el siguiente comando para proporcionar el nuevo archivo JSON de back-end con dataLIF actualizado.

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



Si los RVP están conectados a uno o varios POD, debe desactivar todos los POD correspondientes y a continuación volver a eliminarlos para que el nuevo LIF de datos entre en vigor.

Ejemplos de PYMES seguras

Configuración del backend con el controlador 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
```

Configuración del backend con el controlador 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

```

Configuración de backend con pool de almacenamiento

```

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

```

Ejemplo de clase de almacenamiento con controlador 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

```



Asegúrese de agregar annotations Para habilitar SMB seguro. El SMB seguro no funciona sin las anotaciones, independientemente de la configuración establecida en el backend o PVC.

Ejemplo de clase de almacenamiento con controlador 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

```

Ejemplo de PVC con un solo usuario de 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
```

Ejemplo de PVC con múltiples usuarios 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

```

Amazon FSX para ONTAP de NetApp

Utiliza Trident con Amazon FSx para NetApp ONTAP

"Amazon FSX para ONTAP de NetApp" Es un servicio AWS totalmente gestionado que permite a los clientes iniciar y ejecutar sistemas de archivos con tecnología del sistema operativo de almacenamiento ONTAP de NetApp. FSX para ONTAP le permite aprovechar las funciones, el rendimiento y las funcionalidades administrativas de NetApp con las que ya está familiarizado, a la vez que aprovecha la simplicidad, la agilidad, la seguridad y la escalabilidad de almacenar datos en AWS. FSX para ONTAP es compatible con las funciones del sistema de archivos ONTAP y las API de administración.

Puede integrar su sistema de archivos de Amazon FSx para NetApp ONTAP con Trident para garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) puedan aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

Un sistema de archivos es el recurso principal de Amazon FSx, similar a un clúster de ONTAP en las instalaciones. En cada SVM, se pueden crear uno o varios volúmenes, que son contenedores de datos que almacenan los archivos y las carpetas en el sistema de archivos. Con Amazon FSx para NetApp ONTAP se proporcionará como un sistema de archivos gestionado en la nube. El nuevo tipo de sistema de archivos se llama **ONTAP** de NetApp.

Al usar Trident con Amazon FSx para NetApp ONTAP, puedes garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) puedan aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

Requisitos

Además "[Requisitos de Trident](#)" de , para integrar FSx para ONTAP con Trident, necesita:

- Un clúster de Amazon EKS existente o un clúster de Kubernetes autogestionado con `kubectl` instalado.
- Un sistema de archivos Amazon FSx para NetApp ONTAP y una máquina virtual de almacenamiento (SVM) a la que se puede acceder desde los nodos de trabajo del clúster.
- Nodos de trabajo preparados para "[NFS o iSCSI](#)".



Asegúrese de seguir los pasos de preparación de nodos necesarios para Amazon Linux y Ubuntu "[Imágenes de máquina de Amazon](#)" (AMI) en función del tipo de IAM EKS.

Consideraciones

- Volúmenes SMB:
 - Se admiten los volúmenes de SMB mediante el `ontap-nas` sólo conductor.
 - Los volúmenes SMB no son compatibles con el complemento Trident EKS.
 - Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows. Consulte "[Prepárese para aprovisionar los volúmenes de SMB](#)" para obtener más información.
- Antes de Trident 24,02, Trident no podía eliminar los volúmenes creados en el sistema de archivos Amazon FSx que tenían habilitados los backups automáticos. Para evitar este problema en Trident 24,02 o posterior, especifique `fsxFilesystemID`, `aws`, `apiKey` `aws` `apiRegion` y `aws secretKey` en el archivo de configuración de backend para AWS FSx for ONTAP.



Si especifica un rol de IAM en Trident, puede omitir la especificación de los `apiRegion` campos , `apiKey` y `secretKey` en Trident de forma explícita. Para obtener más información, consulte "[Opciones y ejemplos de configuración de FSX para ONTAP](#)".

Uso simultáneo del controlador Trident SAN/iSCSI y EBS-CSI

Si planea usar controladores `ontap-san` (por ejemplo, iSCSI) con AWS (EKS, ROSA, EC2 o cualquier otra instancia), la configuración de múltiples rutas requerida en los nodos podría entrar en conflicto con el controlador CSI de Amazon Elastic Block Store (EBS). Para garantizar que las funciones de rutas múltiples funcionen sin interferir con los discos EBS en el mismo nodo, debe excluir EBS en su configuración de rutas múltiples. Este ejemplo muestra una `multipath.conf` archivo que incluye las configuraciones Trident requeridas mientras excluye los discos EBS de las rutas múltiples:

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

Autenticación

Trident ofrece dos modos de autenticación.

- Basado en credenciales (recomendado): Almacena las credenciales de forma segura en AWS Secrets Manager. Puede usar el `fsxadmin` usuario del sistema de archivos o del `vsadmin` usuario configurado para la SVM.



Trident espera ejecutarse como `vsadmin` usuario de SVM o como usuario con un nombre distinto que tenga el mismo rol. Amazon FSx para NetApp ONTAP tiene un `fsxadmin` usuario que sustituye de forma limitada al usuario del clúster de ONTAP `admin`. Recomendamos encarecidamente utilizar `vsadmin` con Trident.

- Basado en certificado: Trident se comunicará con la SVM en su sistema de archivos FSx a través de un certificado instalado en su SVM.

Para obtener más información sobre cómo habilitar la autenticación, consulte la autenticación del tipo de controlador:

- ["Autenticación NAS de ONTAP"](#)
- ["Autenticación SAN ONTAP"](#)

Imágenes de máquina de Amazon probadas (AMI)

El clúster EKS admite varios sistemas operativos, pero AWS ha optimizado ciertas imágenes de máquinas de Amazon (AMI) para contenedores y EKS. Las siguientes AMI se han probado con NetApp Trident 25.02.

IAM	NAS	Economía NAS	ISCSI	Economía iSCSI
AL2023_x86_64_STANDARD	Sí	Sí	Sí	Sí
AL2_x86_64	Sí	Sí	Sí*	Sí*
BOTTLEROCKET_x86_64	Sí**	Sí	NO DISPONIBLE	NO DISPONIBLE
AL2023_ARM_64_STANDARD	Sí	Sí	Sí	Sí
AL2_ARM_64	Sí	Sí	Sí*	Sí*

BOTTLEROCKET_A RM_64	Sí**	Sí	NO DISPONIBLE	NO DISPONIBLE
-------------------------	------	----	---------------	---------------

- * No se puede eliminar el PV sin reiniciar el nodo
- ** No funciona con NFSv3 con Trident versión 25.02.



Si su AMI deseado no aparece aquí, no significa que no sea compatible; simplemente significa que no se ha probado. Esta lista sirve como guía para las AMI que se sabe que funcionan.

Pruebas realizadas con:

- Versión de EKS: 1.32
- Método de instalación: Helm 25.06 y como complemento de AWS 25.06
- Para NAS, se probaron tanto NFSv3 como NFSv4,1.
- Para SAN solo se probó iSCSI, no NVMe-oF.

Pruebas realizadas:

- Crear: Clase de almacenamiento, pvc, pod
- Eliminar: Pod, pvc (normal, qtree/lun: Economía, NAS con backup de AWS)

Obtenga más información

- ["Documentación de Amazon FSX para ONTAP de NetApp"](#)
- ["Publicación del blog en Amazon FSX para ONTAP de NetApp"](#)

Cree un rol de IAM y AWS Secret

Puede configurar los pods de Kubernetes para acceder a los recursos de AWS mediante la autenticación como un rol de AWS IAM en lugar de proporcionar credenciales de AWS explícitas.



Para autenticarse mediante un rol de AWS IAM, debe tener un clúster de Kubernetes implementado mediante EKS.

Crear secreto de AWS Secrets Manager

Como Trident emitirá API con un Vserver FSx para gestionar el almacenamiento por usted, necesitará credenciales para hacerlo. La forma segura de pasar esas credenciales es a través de un secreto de AWS Secrets Manager. Por lo tanto, si aún no tiene uno, deberá crear un secreto de AWS Secrets Manager que contenga las credenciales de la cuenta vsadmin.

En este ejemplo, se crea un secreto de AWS Secrets Manager para almacenar las credenciales de Trident CSI:

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

Crear política de IAM

Trident también necesita permisos de AWS para ejecutarse correctamente. Por lo tanto, debe crear una política que proporcione a Trident los permisos que necesita.

Los siguientes ejemplos crean una política de IAM mediante la CLI de AWS:

```
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"
```

Ejemplo de Política JSON:

```

{
  "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"
}

```

Crear una identidad de pod o un rol de IAM para la asociación de cuentas de servicio (IRSA)

Puede configurar una cuenta de servicio de Kubernetes para que asuma un rol de AWS Identity and Access Management (IAM) con EKS Pod Identity o un rol de IAM para la asociación de cuentas de servicio (IRSA). Cualquier pod configurado para usar la cuenta de servicio podrá acceder a cualquier servicio de AWS al que el rol tenga permisos de acceso.

Identidad de pod

Las asociaciones de identidad de pod de Amazon EKS brindan la capacidad de administrar credenciales para sus aplicaciones, de manera similar a la forma en que los perfiles de instancia de Amazon EC2 proporcionan credenciales a las instancias de Amazon EC2.

Instalar Pod Identity en tu clúster EKS:

Puede crear una identidad de Pod a través de la consola de AWS o usando el siguiente comando de AWS CLI:

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

Para obtener más información, consulte ["Configurar el agente de identidad de pod de Amazon EKS"](#).

Crear trust-relationship.json:

Cree el archivo trust-relationship.json para permitir que la entidad de servicio de EKS asuma este rol para la identidad del pod. A continuación, cree un rol con esta política de confianza:

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

archivo trust-relationship.json:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "pods.eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
```

Adjuntar la política de rol al rol de IAM:

Adjunte la política de rol del paso anterior al rol de IAM que se creó:

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

Crear una asociación de identidad de pod:

Cree una asociación de identidad de pod entre el rol de IAM y la cuenta de servicio 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
```

Rol de IAM para la asociación de cuentas de servicio (IRSA)

Usando la AWS CLI:

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

archivo 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"
        }
      }
    }
  ]
}
```

Actualice los siguientes valores en el `trust-relationship.json` archivo:

- **<account_id>** - Su ID de cuenta de AWS
- **<oidc_provider>** - El OIDC de su clúster EKS. Puede obtener `oidc_provider` ejecutando:

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

Adjuntar el rol de IAM con la política de IAM:

Una vez creado el rol, adjunte la política (que se creó en el paso anterior) al rol mediante este comando:

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

Verificar que el proveedor de OICD está asociado:

Verifique que su proveedor de OIDC está asociado al clúster. Puede verificarlo con este comando:

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

Si la salida está vacía, utilice el siguiente comando para asociar IAM OIDC al cluster:

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

Si está usando **eksctl**, utilice el siguiente ejemplo para crear una función de IAM para una cuenta de servicio en 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 optimiza la gestión del almacenamiento de Amazon FSx para NetApp ONTAP en Kubernetes para que sus desarrolladores y administradores se centren en la puesta en marcha de aplicaciones.

Puede instalar Trident mediante uno de los siguientes métodos:

- Timón
- Complemento EKS

Si desea utilizar la funcionalidad Snapshot, instale el complemento del controlador de instantáneas CSI. Consulte ["Habilite la funcionalidad Snapshot para volúmenes CSI"](#) si desea obtener más información.

Instale Trident a través del timón

Identidad de pod

1. Añada el repositorio Helm de Trident:

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

2. Instale Trident utilizando el siguiente ejemplo:

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

Puede utilizar `helm list` el comando para revisar detalles de instalación como nombre, espacio de nombres, gráfico, estado, versión de la aplicación y número de revisión.

```
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		

Asociación de cuentas de servicio (IRSA)

1. Añada el repositorio Helm de Trident:

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

2. Establezca los valores para **proveedor de nube** y **identidad de nube**:

```
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
```

Puede utilizar `helm list` el comando para revisar detalles de instalación como nombre, espacio de nombres, gráfico, estado, versión de la aplicación y número de revisión.

```
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		

Si planea usar iSCSI, asegúrese de que esté habilitado en su equipo cliente. Si usa el sistema operativo de nodo de trabajo AL2023, puede automatizar la instalación del cliente iSCSI añadiendo el parámetro `node prep` en la instalación de Helm:



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

Instale Trident a través del complemento EKS

El complemento Trident EKS incluye los parches de seguridad más recientes, correcciones de errores y está validado por AWS para funcionar con Amazon EKS. El complemento EKS le permite garantizar de forma constante que sus clústeres de Amazon EKS sean seguros y estables y reducir la cantidad de trabajo que necesita para instalar, configurar y actualizar complementos.

Requisitos previos

Asegúrese de tener lo siguiente antes de configurar el complemento Trident para AWS EKS:

- Una cuenta de clúster de Amazon EKS con suscripción complementaria
- Permisos de AWS para AWS Marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Tipo de AMI: Amazon Linux 2 (AL2_x86_64) o Amazon Linux 2 Arm (AL2_ARM_64)
- Tipo de nodo: AMD o ARM
- Un sistema de archivos Amazon FSx para NetApp ONTAP existente

Habilite el complemento Trident para AWS

Consola de gestión

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, seleccione **Clusters**.
3. Seleccione el nombre del cluster para el que desea configurar el complemento CSI de NetApp Trident.
4. Seleccione **Add-ons** y luego seleccione **Get more add-ons**.
5. Siga estos pasos para seleccionar el complemento:
 - a. Desplácese hacia abajo hasta la sección **Complementos de AWS Marketplace** y escriba **"Trident"** en el cuadro de búsqueda.
 - b. Seleccione la casilla de verificación en la esquina superior derecha del cuadro Trident by NetApp.
 - c. Seleccione **Siguiente**.
6. En la página de configuración **Configure Selected add-ons**, haga lo siguiente:



Omite estos pasos si estás usando la asociación de identidad de pod.

- a. Seleccione la **Versión** que desea usar.
- b. Si utiliza la autenticación IRSA, asegúrese de establecer los valores de configuración disponibles en la configuración opcional:
 - Seleccione la **Versión** que desea usar.
 - Siga el **Esquema de configuración del complemento** y configure el parámetro **configurationValues** en la sección **Valores de configuración** en el rol-arn que creó en el paso anterior (el valor debe tener el siguiente formato):

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

+

Si selecciona Sustituir para el método de resolución de conflictos, una o más de las configuraciones del complemento existente se pueden sobrescribir con la configuración del complemento Amazon EKS. Si no habilita esta opción y existe un conflicto con la configuración existente, se producirá un error en la operación. Puede utilizar el mensaje de error resultante para solucionar el conflicto. Antes de seleccionar esta opción, asegúrese de que el complemento de Amazon EKS no gestiona la configuración que necesita para autogestionar.

7. Elija **Siguiente**.
8. En la página **Revisar y agregar**, seleccione **Crear**.

Una vez finalizada la instalación del complemento, verá el complemento instalado.

CLI DE AWS

1. Crea el add-on.json archivo:

Para la identidad del pod, utilice el siguiente formato:



Usa la

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

Para la autenticación de IRSA, utilice el siguiente 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"
  }
}
```



Reemplace <role ARN> por el ARN del rol que se creó en el paso anterior.

2. Instalar el complemento Trident EKS.

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

eksctl

El siguiente comando de ejemplo instala el complemento Trident EKS:

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

Actualice el complemento Trident EKS

Consola de gestión

1. Abra la consola de Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, seleccione **Clusters**.
3. Seleccione el nombre del cluster para el que desea actualizar el complemento CSI de NetApp Trident.
4. Seleccione la pestaña **Add-ons**.
5. Seleccione **Trident by NetApp** y luego seleccione **Editar**.
6. En la página **Configure Trident by NetApp**, haga lo siguiente:
 - a. Seleccione la **Versión** que desea usar.
 - b. Expanda la **Configuración opcional** y modifique según sea necesario.
 - c. Seleccione **Guardar cambios**.

CLI DE AWS

El siguiente ejemplo actualiza el complemento 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

- Compruebe la versión actual de su complemento FSxN Trident CSI. Sustituya my-cluster por el nombre del clúster.

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

Ejemplo de salida:

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'\"}			

- Actualice el complemento a la versión devuelta bajo ACTUALIZACIÓN DISPONIBLE en la salida del paso anterior.

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

Si elimina la `--force` opción y cualquiera de las configuraciones del complemento de Amazon EKS entra en conflicto con la configuración existente, la actualización del complemento de Amazon EKS falla; recibirá un mensaje de error que le ayudará a resolver el conflicto. Antes de especificar esta opción, asegúrese de que el complemento de Amazon EKS no gestiona la configuración que debe administrar, ya que dicha configuración se sobrescribe con esta opción. Para obtener más información acerca de otras opciones para esta configuración, consulte ["Complementos"](#). Para obtener más información sobre la gestión de campos de Amazon EKS Kubernetes, consulte ["Gestión del campo de Kubernetes"](#).

Desinstale/elimine el complemento Trident EKS

Tienes dos opciones para eliminar un complemento de Amazon EKS:

- **Preserve el software complementario en su clúster** – Esta opción elimina la administración de Amazon EKS de cualquier configuración. También elimina la posibilidad de que Amazon EKS le notifique las actualizaciones y actualice automáticamente el complemento de Amazon EKS después de iniciar una actualización. Sin embargo, conserva el software complementario en el clúster. Esta opción convierte el complemento en una instalación autogestionada, en lugar de un complemento de Amazon EKS. Con esta opción, no se produce tiempo de inactividad en el complemento. Conserve `--preserve` la opción en el comando para conservar el complemento.
- * Elimine el software complementario completamente de su clúster *: NetApp recomienda eliminar el complemento Amazon EKS de su clúster solo si no hay recursos en su clúster que dependan de él. Elimine `--preserve` la opción del `delete` comando para eliminar el complemento.



Si el complemento tiene una cuenta de IAM asociada, la cuenta de IAM no se elimina.

Consola de gestión

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, seleccione **Clusters**.
3. Seleccione el nombre del cluster para el que desea quitar el complemento CSI de NetApp Trident.
4. Seleccione la pestaña **Complementos** y luego seleccione **Trident by NetApp**.*
5. Seleccione **Quitar**.
6. En el cuadro de diálogo **Remove netapp_trident-operator confirmation**, haga lo siguiente:
 - a. Si desea que Amazon EKS deje de administrar la configuración del complemento, seleccione **Conservar en clúster**. Haga esto si desea conservar el software complementario en su clúster para que pueda gestionar todos los ajustes del complemento por su cuenta.
 - b. Introduzca **netapp_trident-operator**.
 - c. Seleccione **Quitar**.

CLI DE AWS

Reemplace `my-cluster` por el nombre del clúster y, a continuación, ejecute el siguiente comando.

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

eksctl

El siguiente comando desinstala el complemento Trident EKS:

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

Configure el backend de almacenamiento

Integración de controladores ONTAP SAN y NAS

Para crear un backend de almacenamiento, debe crear un archivo de configuración en formato JSON o YAML. El archivo debe especificar el tipo de almacenamiento que se desea (NAS o SAN), el sistema de archivos y SVM desde el que desea obtener el archivo y cómo se debe autenticar con él. El siguiente ejemplo muestra cómo definir el almacenamiento basado en NAS y cómo usar un secreto de AWS para almacenar las credenciales en la SVM que desea utilizar:

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"
    }
  }
}
```

Ejecute los siguientes comandos para crear y validar la configuración de backend de Trident (TBC):

- Cree la configuración de backend de Trident (TBC) desde el archivo yaml y ejecute el siguiente comando:

```
kubectl create -f backendconfig.yaml -n trident
```

```
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-nas created
```

- Validar que la configuración de backend de Trident (TBC) se ha creado correctamente:

```
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

FSX para ONTAP detalles del controlador

Puedes integrar Trident con Amazon FSx for NetApp ONTAP mediante los siguientes controladores:

- **ontap-san:** Cada VP aprovisionado es un LUN dentro de su propio volumen de Amazon FSx para NetApp ONTAP. Recomendado para almacenamiento en bloques.
- **ontap-nas:** Cada VP aprovisionado es un volumen completo de Amazon FSx para NetApp ONTAP. Recomendado para NFS y SMB.
- **ontap-san-economy:** Cada VP aprovisionado es un LUN con un número configurable de LUN por Amazon FSX para el volumen ONTAP de NetApp.
- **ontap-nas-economy:** Cada VP aprovisionado es un qtree, con un número configurable de qtrees por Amazon FSX para el volumen ONTAP de NetApp.
- **ontap-nas-flexgroup:** Cada VP aprovisionado es un Amazon FSX completo para el volumen ONTAP FlexGroup de NetApp.

Para obtener información detallada sobre el conductor, consulte ["Controladores de NAS"](#) y.. ["Controladores de SAN"](#).

Una vez creado el archivo de configuración, ejecute este comando para crearlo dentro de su EKS:

```
kubectl create -f configuration_file
```

Para verificar el estado, ejecute este comando:

```
kubectl get tbc -n trident
```

NAME	BACKEND NAME	BACKEND UUID
PHASE STATUS		
backend-fsx-ontap-nas	backend-fsx-ontap-nas	7a551921-997c-4c37-a1d1-f2f4c87fa629
Bound	Success	

Configuración avanzada de backend y ejemplos

Consulte la siguiente tabla para ver las opciones de configuración del back-end:

Parámetro	Descripción	Ejemplo
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + «_» + LIF de datos
managementLIF	Dirección IP de un clúster o una LIF de gestión de SVM Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si proporciona el fsxFilesystemID en aws el campo, no necesita proporcionar el managementLIF porque Trident recupera la información de la SVM managementLIF de AWS. Por lo tanto, debe proporcionar credenciales para un usuario en la SVM (por ejemplo: Vsadmin) y el usuario debe tener vsadmin el rol.	«10.0.0.1», «[2001:1234:abcd::fefe]»

Parámetro	Descripción	Ejemplo
dataLIF	Dirección IP de LIF de protocolo. Controladores NAS de ONTAP: NetApp recomienda especificar dataLIF. Si no se proporciona, Trident recupera las LIF de datos de la SVM. Puede especificar un nombre de dominio completo (FQDN) que se utilice para las operaciones de montaje de NFS, lo que permite crear un DNS por turnos para equilibrar la carga en varias LIF de datos. Se puede cambiar después del ajuste inicial. Consulte . Controladores SAN ONTAP: No se especifica para iSCSI. Trident utiliza asignación de LUN selectiva de ONTAP para descubrir las LIF iSCSI necesarias para establecer una sesión multivía. Se genera una advertencia si dataLIF se define explícitamente. Se puede configurar para utilizar direcciones IPv6 si Trident se instaló con el indicador IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	
autoExportPolicy	Habilite la creación y actualización automática de la política de exportación [Boolean]. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	false
autoExportCIDRs	Lista de CIDRs para filtrar las IP del nodo de Kubernetes contra cuando autoExportPolicy se habilita. Mediante las autoExportPolicy opciones y autoExportCIDRs, Trident puede gestionar automáticamente las políticas de exportación.	«[«0.0.0.0/0»::/0]»
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""

Parámetro	Descripción	Ejemplo
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados.	""
username	El nombre de usuario para conectarse al clúster o SVM. Se utiliza para autenticación basada en credenciales. Por ejemplo, vsadmin.	
password	La contraseña para conectarse al clúster o SVM. Se utiliza para autenticación basada en credenciales.	
svm	Máquina virtual de almacenamiento que usar	Derivado si se especifica una LIF de gestión de SVM.
storagePrefix	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede modificar una vez creada. Para actualizar este parámetro, deberá crear un nuevo backend.	trident
limitAggregateUsage	No especifique para Amazon FSx para NetApp ONTAP. El proporcionado fsxadmin y vsadmin no contiene los permisos necesarios para recuperar el uso de agregados y limitarlo mediante Trident.	No utilizar.
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor. También restringe el tamaño máximo de los volúmenes que gestiona para qtrees y LUN, y la qtreesPerFlexvol opción permite personalizar el número máximo de qtrees por FlexVol volume	"" (no se aplica de forma predeterminada)

Parámetro	Descripción	Ejemplo
<code>lunsPerFlexvol</code>	El número máximo de LUN por FlexVol volume debe estar comprendido entre [50, 200]. Solo SAN.	«100»
<code>debugTraceFlags</code>	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {«api»:false, «method»:true} No utilizar <code>debugTraceFlags</code> a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo
<code>nfsMountOptions</code>	Lista de opciones de montaje NFS separadas por comas. Las opciones de montaje para los volúmenes persistentes de Kubernetes se especifican normalmente en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident volverá a utilizar las opciones de montaje especificadas en el archivo de configuración del back-end de almacenamiento. Si no se especifican opciones de montaje en la clase almacenamiento o el archivo de configuración, Trident no definirá ninguna opción de montaje en un volumen persistente asociado.	""
<code>nasType</code>	Configure la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> , o nulo. Debe establecer en <code>smb</code> Para volúmenes SMB. el valor predeterminado es null en volúmenes NFS.	<code>nfs</code>
<code>qtreesPerFlexvol</code>	El número máximo de qtrees por FlexVol volume debe estar en el intervalo [50, 300]	"200"

Parámetro	Descripción	Ejemplo
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado con la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP, o bien un nombre para permitir que Trident cree el recurso compartido de SMB. Este parámetro es obligatorio para los back-ends de Amazon FSx para ONTAP.	smb-share
useREST	Parámetro booleano para usar las API DE REST de ONTAP. Cuando se establece en <code>true</code> , Trident utilizará las API REST DE ONTAP para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap</code> la aplicación. Esto se cumple con los roles predefinidos <code>vsadmin</code> y <code>cluster-admin</code> .	false
aws	Puedes especificar lo siguiente en el archivo de configuración de AWS FSx para ONTAP: - <code>fsxFileSystemID</code> : Especifique el ID del sistema de archivos AWS FSx. - <code>apiRegion</code> : Nombre de la región de la API de AWS. - <code>apiKey</code> : AWS API key. - <code>secretKey</code> : AWS clave secreta.	"" "" ""
credentials	Especifique las credenciales de FSX SVM para almacenarlas en AWS Secrets Manager. <code>name</code> - : Nombre de recurso de Amazon (ARN) del secreto, que contiene las credenciales de SVM. <code>type</code> - : Establecido en <code>awsarn</code> . Consulte "Cree un secreto de AWS Secrets Manager" si desea obtener más información.	

Opciones de configuración de back-end para el aprovisionamiento de volúmenes

Puede controlar el aprovisionamiento predeterminado utilizando estas opciones en la `defaults` sección de la configuración. Para ver un ejemplo, vea los ejemplos de configuración siguientes.

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para las LUN	true
spaceReserve	Modo de reserva de espacio; «ninguno» (fino) o «volumen» (grueso)	none
snapshotPolicy	Política de Snapshot que se debe usar	none
qosPolicy	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o back-end. Usar grupos de políticas de QoS con Trident requiere ONTAP 9 Intersight 8 o posterior. Debe usar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido aplica el techo máximo para el rendimiento total de todas las cargas de trabajo.	""
adaptiveQosPolicy	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o back-end. no admitido por ontap-nas-Economy.	""
snapshotReserve	Porcentaje de volumen reservado para las instantáneas «0»	snapshotPolicy`Si es `none, else
splitOnClone	Divida un clon de su elemento principal al crearlo	false
encryption	Habilite el cifrado de volúmenes de NetApp (NVE) en el nuevo volumen; los valores predeterminados son false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster. Si NAE está habilitado en el back-end, cualquier volumen provisionado en Trident será habilitado NAE. Para obtener más información, consulte: "Cómo funciona Trident con NVE y NAE" .	false

Parámetro	Descripción	Predeterminado
luksEncryption	Active el cifrado LUKS. Consulte "Usar la configuración de clave unificada de Linux (LUKS)" . Solo SAN.	""
tieringPolicy	Política de organización en niveles para utilizar <code>none</code>	
unixPermissions	Modo para volúmenes nuevos. Dejar vacío para volúmenes SMB.	""
securityStyle	Estilo de seguridad para nuevos volúmenes. Compatibilidad con NFS <code>mixed</code> y.. <code>unix</code> estilos de seguridad. SMB admite <code>mixed</code> y.. <code>ntfs</code> estilos de seguridad.	El valor predeterminado de NFS es <code>unix</code> . La opción predeterminada de SMB es <code>ntfs</code> .

aprovisionamiento de volúmenes SMB

Puede aprovisionar volúmenes SMB utilizando `ontap-nas` conductor. Antes de completar [Integración de controladores ONTAP SAN y NAS](#) Complete estos pasos: ["Prepárese para aprovisionar los volúmenes de SMB"](#).

Configure una clase de almacenamiento y la RVP

Configure un objeto `StorageClass` de Kubernetes y cree la clase de almacenamiento para indicar a Trident cómo se aprovisionan los volúmenes. Cree una reclamación de volumen persistente (RVP) que utilice el `StorageClass` de Kubernetes configurado para solicitar acceso al VP. A continuación, puede montar el VP en un pod.

Cree una clase de almacenamiento

Configurar un objeto de Kubernetes `StorageClass`

El ["Objeto de Kubernetes `StorageClass`"](#) El objeto identifica a Trident como el aprovisionador que se utiliza para esa clase y le indica cómo aprovisionar un volumen. Utilice este ejemplo para configurar `Storageclass` para volúmenes que utilizan NFS (consulte la sección Atributos de Trident a continuación para obtener la 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"
```

Utilice este ejemplo para configurar Storageclass para volúmenes que utilizan 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"
```

Para aprovisionar volúmenes de NFSv3 TB en AWS Bottlerocket, agregue el necesario `mountOptions` a la clase de almacenamiento:

```
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
```

Consulte el ["Objetos de Kubernetes y Trident"](#) para obtener más detalles sobre cómo interactúan las clases de almacenamiento con los `PersistentVolumeClaim` parámetros y para controlar la forma en que Trident aprovisiona los volúmenes.

Cree una clase de almacenamiento

Pasos

1. Este es un objeto de Kubernetes, así que use `kubectl` Para crear en Kubernetes.

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

2. Ahora deberías ver una clase de almacenamiento **basic-csi** tanto en Kubernetes como en Trident, y Trident debería haber descubierto los pools en el back-end.

```
kubectl get sc basic-csi
```

NAME	PROVISIONER	AGE
basic-csi	csi.trident.netapp.io	15h

Cree la RVP

Una "*Claim de volumen persistente*" (RVP) es una solicitud para acceder al volumen persistente en el clúster.

La RVP se puede configurar para solicitar almacenamiento de un determinado tamaño o modo de acceso. Mediante el StorageClass asociado, el administrador del clúster puede controlar mucho más que el tamaño de los volúmenes persistentes y el modo de acceso, como el rendimiento o el nivel de servicio.

Después de crear la RVP, puede montar el volumen en un pod.

Manifiestos de muestra

Manifiestos de muestra de PersistentVolumeClaim

Estos ejemplos muestran opciones básicas de configuración de PVC.

PVC con acceso RWX

Este ejemplo muestra una PVC básica con acceso RWX que está asociada con una clase de almacenamiento llamada `basic-csi`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-gold
```

Ejemplo de PVC usando iSCSI

Este ejemplo muestra un PVC básico para iSCSI con acceso RWO que está asociado con una StorageClass denominada `protection-gold`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: protection-gold
```

Crear PVC

Pasos

1. Cree la RVP.

```
kubectl create -f pvc.yaml
```

2. Verifique el estado de la RVP.

```
kubectl get pvc
```

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
pvc-storage	Bound	pv-name	2Gi	RWO		5m

Consulte el ["Objetos de Kubernetes y Trident"](#) para obtener más detalles sobre cómo interactúan las clases de almacenamiento con los `PersistentVolumeClaim` parámetros y para controlar la forma en que Trident aprovisiona los volúmenes.

Atributos de la Trident

Estos parámetros determinan qué pools de almacenamiento gestionados por Trident se deben utilizar para aprovisionar volúmenes de un determinado tipo.

Atributo	Tipo	Valores	Oferta	Solicitud	Admitido por
media 1	cadena	hdd, híbrido, ssd	Pool contiene medios de este tipo; híbrido significa ambos	Tipo de medios especificado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san y solidfire-san
AprovisionaciónTipo	cadena	delgado, grueso	El pool admite este método de aprovisionamiento	Método de aprovisionamiento o especificado	grueso: all ONTAP; thin: all ONTAP y solidfire-san
Tipo de backendType	cadena	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, azure-netapp-files, ontap-san-economy	Pool pertenece a este tipo de backend	Backend especificado	Todos los conductores
snapshot	bool	verdadero, falso	El pool admite volúmenes con Snapshot	Volumen con snapshots habilitadas	ontap-nas, ontap-san, solidfire-san
clones	bool	verdadero, falso	Pool admite el clonado de volúmenes	Volumen con clones habilitados	ontap-nas, ontap-san, solidfire-san

Atributo	Tipo	Valores	Oferta	Solicitud	Admitido por
cifrado	bool	verdadero, falso	El pool admite volúmenes cifrados	Volumen con cifrado habilitado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	int	entero positivo	El pool es capaz de garantizar IOPS en este rango	El volumen garantizado de estas IOPS	solidfire-san

Esta versión 1: No es compatible con sistemas ONTAP Select

Despliegue la aplicación de muestra

Cuando se crean la clase de almacenamiento y la RVP, puede montar el PV en un pod. Esta sección enumera el comando de ejemplo y la configuración para adjuntar el PV a un pod.

Pasos

1. Monte el volumen en un pod.

```
kubectl create -f pv-pod.yaml
```

Estos ejemplos muestran configuraciones básicas para conectar el PVC a un pod: **Configuración 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
```



Puede supervisar el progreso con `kubectl get pod --watch`.

2. Compruebe que el volumen está montado en `/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	

Ahora puede eliminar el Pod. La aplicación Pod ya no existirá, pero el volumen permanecerá.

```
kubectl delete pod pv-pod
```

Configure el complemento Trident EKS en un clúster EKS

NetApp Trident optimiza la gestión del almacenamiento de Amazon FSx para NetApp ONTAP en Kubernetes para que sus desarrolladores y administradores se centren en la puesta en marcha de aplicaciones. El complemento NetApp Trident EKS incluye los parches de seguridad más recientes, correcciones de errores y está validado por AWS para funcionar con Amazon EKS. El complemento EKS le permite garantizar de forma constante que sus clústeres de Amazon EKS sean seguros y estables y reducir la cantidad de trabajo que necesita para instalar, configurar y actualizar complementos.

Requisitos previos

Asegúrese de tener lo siguiente antes de configurar el complemento Trident para AWS EKS:

- Una cuenta de clúster de Amazon EKS con permisos para trabajar con complementos. Consulte ["Complementos de Amazon EKS"](#).
- Permisos de AWS para AWS Marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Tipo de AMI: Amazon Linux 2 (AL2_x86_64) o Amazon Linux 2 Arm (AL2_ARM_64)
- Tipo de nodo: AMD o ARM
- Un sistema de archivos Amazon FSx para NetApp ONTAP existente

Pasos

1. Asegúrese de crear el rol de IAM y el secreto de AWS para permitir que los pods de EKS accedan a los recursos de AWS. Para obtener instrucciones, consulte ["Cree un rol de IAM y AWS Secret"](#).

2. En tu clúster de Kubernetes de EKS, navega a la pestaña **Add-ons**.

tri-env-eks Refresh Delete cluster Upgrade version View dashboard

ⓘ End of standard support for Kubernetes version 1.30 is July 28, 2025. On that date, your cluster will enter the extended support period with additional fees. For more information, see the [pricing page](#). Upgrade now

▼ Cluster info [Info](#)

Status
✓ Active

Cluster health issues
✓ 0

Kubernetes version [Info](#)
1.30

Upgrade insights
✓ 0

Support period
ⓘ Standard support until July 28, 2025

Provider
EKS

Overview | Resources | Compute | Networking | **Add-ons 1** | Access | Observability | Update history | Tags

ⓘ New versions are available for 1 add-on. ×

Add-ons (3) [Info](#) View details Edit Remove Get more add-ons

Any categ... Any status 3 matches < 1 >

3. Vaya a **AWS Marketplace add-ons** y elija la categoría *storage*.


AWS Marketplace add-ons (1) Refresh

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. X < 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

4. Localice **NetApp Trident** y seleccione la casilla de verificación para el complemento Trident, y haga clic en **Siguiente**.

5. Elija la versión deseada del complemento.

Configure selected add-ons settings


Configure the add-ons for your cluster by selecting settings.

NetApp TridentRemove add-on

Listed by

Category

Status



storage

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

6. Configure los ajustes complementarios necesarios.

Review and add

Step 1: Select add-ons

[Edit](#)

Selected add-ons (1)

Find add-on

< 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 >

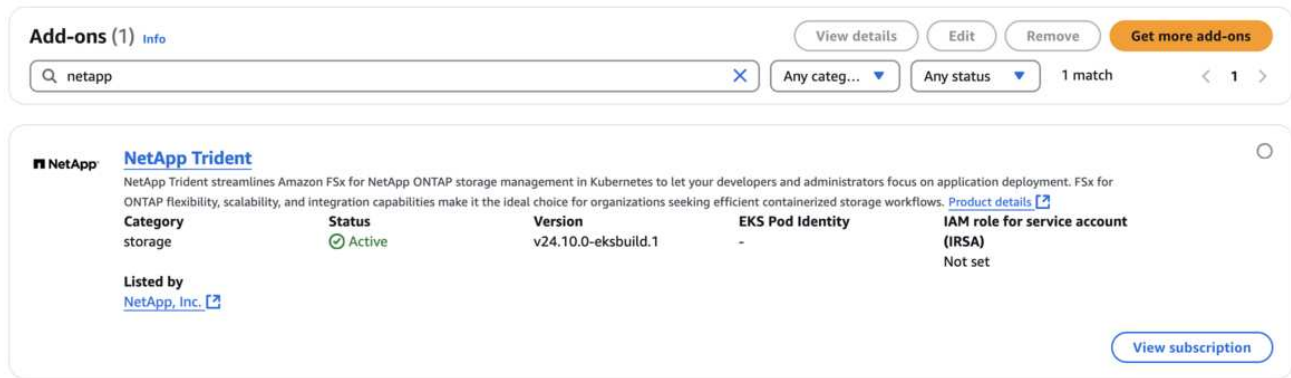
Add-on name	IAM role	Service account
No Pod Identity associations None of the selected add-on(s) have Pod Identity associations.		

[Cancel](#)[Previous](#)[Create](#)

7. Si está utilizando IRSA (roles de IAM para cuentas de servicio), consulte los pasos de configuración adicionales[aquí](#).

8. Seleccione **Crear**.

9. Compruebe que el estado del complemento es *Active*.



10. Ejecute el siguiente comando para comprobar que Trident está correctamente instalado en el clúster:

```
kubectl get pods -n trident
```

11. Continúe con la configuración y configure el back-end de almacenamiento. Para obtener más información, consulte "[Configure el backend de almacenamiento](#)".

Instale/desinstale el complemento Trident EKS mediante la interfaz de línea de comandos

Instale el complemento NetApp Trident EKS mediante la interfaz de línea de comandos:

El siguiente comando de ejemplo instala el complemento Trident EKS:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.0-eksbuild.1 (con una versión dedicada)
```

El siguiente comando de ejemplo instala el complemento Trident EKS versión 25.6.1:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.1-eksbuild.1 (con una versión dedicada)
```

El siguiente comando de ejemplo instala el complemento Trident EKS versión 25.6.2:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.2-eksbuild.1 (con una versión dedicada)
```

Desinstale el complemento NetApp Trident EKS mediante la interfaz de línea de comandos:

El siguiente comando desinstala el complemento Trident EKS:

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

Cree back-ends con kubectl

Un back-end define la relación entre Trident y un sistema de almacenamiento. Indica a Trident cómo se comunica con ese sistema de almacenamiento y cómo debe aprovisionar volúmenes a partir de él. Después de instalar Trident, el siguiente paso es crear un backend. La `TridentBackendConfig` definición de recursos personalizados (CRD) le permite crear y administrar backends de Trident directamente a través de la

interfaz de Kubernetes. Para ello, puede utilizar `kubectl` o la herramienta CLI equivalente para su distribución de Kubernetes.

TridentBackendConfig

`TridentBackendConfig` (`tbc`, `tbconfig` `tbackendconfig`) Es una interfaz CRD con nombre que permite gestionar los backends de Trident mediante `kubectl`. Los administradores de Kubernetes y de almacenamiento ahora pueden crear y gestionar back-ends directamente mediante la CLI de Kubernetes sin necesidad de una utilidad de línea de comandos dedicada (`tridentctl`).

Sobre la creación de un `TridentBackendConfig` objeto, sucede lo siguiente:

- Trident crea automáticamente un backend basado en la configuración que proporcione. Esto se representa internamente como un `TridentBackend` (`tbe`, `tridentbackend`) CR.
- El `TridentBackendConfig` está vinculado exclusivamente a una `TridentBackend` que fue creada por Trident.

Cada uno `TridentBackendConfig` mantiene una asignación de uno a uno con un `TridentBackend`. El primero es la interfaz que se ofrece al usuario para diseñar y configurar los back-ends. El segundo es cómo Trident representa el objeto back-end real.



`TridentBackend` Trident crea los CRS automáticamente. Usted **no debe** modificarlos. Si desea realizar actualizaciones en los back-ends, haga esto modificando el `TridentBackendConfig` objeto.

Consulte el siguiente ejemplo para ver el formato del `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
```

También puede echar un vistazo a los ejemplos de la ["instalador de trident"](#) directorio para configuraciones de ejemplo para la plataforma o servicio de almacenamiento que desee.

La `spec` toma parámetros de configuración específicos del back-end. En este ejemplo, el back-end utiliza el `ontap-san` controlador de almacenamiento y utiliza los parámetros de configuración que se tabulan aquí. Para obtener la lista de opciones de configuración para el controlador de almacenamiento deseado, consulte la ["información de configuración del back-end para el controlador de almacenamiento"](#).

La spec la sección también incluye `credentials` y `deletionPolicy` campos, que se introducen recientemente en `TridentBackendConfig` CR:

- `credentials`: Este parámetro es un campo obligatorio y contiene las credenciales utilizadas para autenticarse con el sistema/servicio de almacenamiento. Este juego debe ser un secreto de Kubernetes creado por el usuario. Las credenciales no se pueden pasar en texto sin formato y se producirá un error.
- `deletionPolicy`: Este campo define lo que debe suceder cuando `TridentBackendConfig` se ha eliminado. Puede ser necesario uno de los dos valores posibles:
 - `delete`: Esto resulta en la eliminación de ambos `TridentBackendConfig` CR y el back-end asociado. Este es el valor predeterminado.
 - `retain`: Cuando un `TridentBackendConfig` Se elimina la CR, la definición de backend seguirá estando presente y se puede gestionar con `tridentctl`. Establecimiento de la política de eliminación como `retain` permite a los usuarios degradar a una versión anterior (anterior a 21.04) y conservar los back-ends creados. El valor de este campo se puede actualizar después de un `TridentBackendConfig` se ha creado.



El nombre de un back-end se define mediante `spec.backendName`. Si no se especifica, el nombre del backend se establece en el nombre del `TridentBackendConfig` objeto (`metadata.name`). Se recomienda establecer explícitamente nombres de backend mediante `spec.backendName`.



Los back-ends que se crearon con `tridentctl` no tienen un objeto asociado `TridentBackendConfig`. Puede optar por gestionar dichos back-ends con `kubectl` creando una `TridentBackendConfig` CR. Se debe tener cuidado de especificar parámetros de configuración idénticos (`spec.backendName` como `, , , `spec.storagePrefix` spec.storageDriverName etc.). Trident enlazará automáticamente los recién creados TridentBackendConfig con el backend preexistente.`

Descripción general de los pasos

Para crear un nuevo back-end mediante `kubectl`, debe hacer lo siguiente:

1. Create a "**Secreto Kubernetes**". El secreto contiene las credenciales que Trident necesita para comunicarse con el clúster/servicio de almacenamiento.
2. Cree un `TridentBackendConfig` objeto. Este contiene detalles sobre el servicio/clúster de almacenamiento y hace referencia al secreto creado en el paso anterior.

Después de crear un backend, puede observar su estado utilizando `kubectl get tbc <tbc-name> -n <trident-namespace>` y recopile detalles adicionales.

Paso 1: Cree un secreto de Kubernetes

Cree un secreto que contenga las credenciales de acceso para el back-end. Esto es único para cada servicio/plataforma de almacenamiento. Veamos un ejemplo:

```
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 tabla resume los campos que deben incluirse en el secreto para cada plataforma de almacenamiento:

Descripción de campos secretos de la plataforma de almacenamiento	Secreto	Descripción de los campos
Azure NetApp Files	ID del Cliente	El ID de cliente de un registro de aplicación
Element (HCI/SolidFire de NetApp)	Extremo	MVIP para el clúster de SolidFire con credenciales de inquilino
ONTAP	nombre de usuario	Nombre de usuario para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales
ONTAP	contraseña	Contraseña para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales
ONTAP	ClientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados
ONTAP	ChapUsername	Nombre de usuario entrante. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy
ONTAP	InitichapatorSecret	Secreto CHAP del iniciador. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy

Descripción de campos secretos de la plataforma de almacenamiento	Secreto	Descripción de los campos
ONTAP	ChapTargetUsername	Nombre de usuario de destino. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy
ONTAP	ChapTargetInitiatorSecret	Secreto CHAP del iniciador de destino. Necesario si useCHAP=true. Para ontap-san y.. ontap-san-economy

El secreto creado en este paso será referenciado en el `spec.credentials` del `TridentBackendConfig` objeto creado en el paso siguiente.

Paso 2: Cree la `TridentBackendConfig` CR

Ya está listo para crear su `TridentBackendConfig` CR. En este ejemplo, un back-end que utiliza ontap-san el controlador se crea mediante `TridentBackendConfig` objeto mostrado a continuación:

```
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
```

Paso 3: Compruebe el estado del `TridentBackendConfig` CR

Ahora que creó la `TridentBackendConfig` CR, puede comprobar el estado. Consulte el siguiente ejemplo:

```
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	

Se ha creado un backend correctamente y se ha enlazado a TridentBackendConfig CR.

La fase puede tomar uno de los siguientes valores:

- **Bound:** La TridentBackendConfig CR está asociado con un backend, y ese backend contiene configRef establezca en la TridentBackendConfig UID de CR.
- **Unbound:** Representado usando "". La TridentBackendConfig el objeto no está enlazado a un back-end. Creadas recientemente TridentBackendConfig CRS se encuentra en esta fase de forma predeterminada. Tras cambiar la fase, no puede volver a «sin límites».
- **Deleting:** La TridentBackendConfig CR deletionPolicy se ha configurado para eliminar. Cuando la TridentBackendConfig La CR se elimina y pasa al estado de supresión.
 - Si no existen reclamaciones de volumen persistentes (RVP) en el back-end, si se elimina el Trident, tanto el TridentBackendConfig back-end como la TridentBackendConfig CR.
 - Si uno o más EVs están presentes en el backend, pasa a un estado de supresión. La TridentBackendConfig Posteriormente, CR también entra en fase de eliminación. El back-end y. TridentBackendConfig Se eliminan sólo después de que se hayan eliminado todas las EVs.
- **Lost:** El backend asociado con TridentBackendConfig La CR se eliminó accidental o deliberadamente y la TridentBackendConfig CR todavía tiene una referencia al backend eliminado. La TridentBackendConfig La CR puede ser eliminada independientemente de la deletionPolicy valor.
- **Unknown:** Trident no puede determinar el estado o la existencia del backend asociado al TridentBackendConfig CR. Por ejemplo, si el servidor API no responde o si falta el tridentbackends.trident.netapp.io CRD. Esto puede requerir intervención.

En esta fase, se ha creado un backend. Hay varias operaciones que se pueden realizar además, como ["actualizaciones back-end y eliminaciones backend"](#).

(Opcional) Paso 4: Obtener más detalles

Puede ejecutar el siguiente comando para obtener más información acerca de su entorno de administración:

```
kubectl -n trident get tbc backend-tbc-ontap-san -o wide
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
Bound	Success	

Además, también puede obtener un volcado YLMA/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 Contiene los backendName y el backendUUID del backend que se creó en respuesta a la TridentBackendConfig CR. El lastOperationStatus campo representa el estado de la última operación TridentBackendConfig del CR, que puede ser activada por el usuario (por ejemplo, el usuario cambió algo en spec) o activada por Trident (por ejemplo, durante los reinicios de Trident). Puede ser Success o Failed. phase Representa el estado de la relación entre TridentBackendConfig el CR y el backend. En el ejemplo anterior, phase tiene el valor bound, lo que significa que TridentBackendConfig el CR está asociado al backend.

Puede ejecutar el `kubectl -n trident describe tbc <tbc-cr-name>` comando para obtener detalles de los registros de eventos.



No puede actualizar ni eliminar un backend que contenga un archivo asociado `TridentBackendConfig` objeto con `tridentctl`. Comprender los pasos que implica cambiar entre `tridentctl` y `TridentBackendConfig`, ["ver aquí"](#).

Gestionar back-ends

Realice la gestión del entorno de administración con kubectl

Obtenga información sobre cómo realizar operaciones de administración de back-end mediante `kubectl`.

Eliminar un back-end

Al suprimir un `TridentBackendConfig`, indica a Trident que suprima/conserva los back-ends (según `deletionPolicy`). Para suprimir un backend, asegúrese de que `deletionPolicy` está definido como `DELETE`. Para suprimir sólo el `TridentBackendConfig`, asegúrese de que `deletionPolicy` está definido en `Retener`. Esto asegura que el backend todavía está presente y se puede gestionar mediante el uso `tridentctl`.

Ejecute el siguiente comando:

```
kubectl delete tbc <tbc-name> -n trident
```

Trident no elimina los secretos de Kubernetes que estaban en uso por `TridentBackendConfig`. El usuario de Kubernetes es responsable de limpiar los secretos. Hay que tener cuidado a la hora de eliminar secretos. Solo debe eliminar secretos si no los están utilizando los back-ends.

Ver los back-ends existentes

Ejecute el siguiente comando:

```
kubectl get tbc -n trident
```

También puede ejecutar `tridentctl get backend -n trident` o `tridentctl get backend -o yaml -n trident` obtener una lista de todos los back-ends que existen. Esta lista también incluirá los back-ends que se crearon con `tridentctl`.

Actualizar un back-end

Puede haber varias razones para actualizar un back-end:

- Las credenciales del sistema de almacenamiento han cambiado. Para actualizar las credenciales, se debe actualizar el secreto de Kubernetes utilizado en el `TridentBackendConfig` objeto. Trident actualizará automáticamente el backend con las últimas credenciales proporcionadas. Ejecute el siguiente comando para actualizar Kubernetes Secret:

```
kubectl apply -f <updated-secret-file.yaml> -n trident
```

- Es necesario actualizar los parámetros (como el nombre de la SVM de ONTAP que se está utilizando).
 - Puede actualizar `TridentBackendConfig` Objetos directamente a través de Kubernetes usando el siguiente comando:

```
kubectl apply -f <updated-backend-file.yaml>
```

- Como alternativa, puede realizar cambios en los existentes `TridentBackendConfig` CR con el siguiente comando:

```
kubectl edit tbc <tbc-name> -n trident
```



- Si falla una actualización de back-end, el back-end continúa en su última configuración conocida. Puede ver los registros para determinar la causa ejecutando `kubectl get tbc <tbc-name> -o yaml -n trident` o `kubectl describe tbc <tbc-name> -n trident`.
- Después de identificar y corregir el problema con el archivo de configuración, puede volver a ejecutar el comando `update`.

Realizar la administración de back-end con `tridentctl`

Obtenga información sobre cómo realizar operaciones de administración de back-end mediante `tridentctl`.

Cree un back-end

Después de crear un ["archivo de configuración del back-end"](#), ejecute el siguiente comando:

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

Si se produce un error en la creación del back-end, algo estaba mal con la configuración del back-end. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs -n trident
```

Después de identificar y corregir el problema con el archivo de configuración, simplemente puede ejecutar el `create` comando de nuevo.

Eliminar un back-end

Para suprimir un backend de Trident, haga lo siguiente:

1. Recupere el nombre del backend:

```
tridentctl get backend -n trident
```

2. Eliminar el back-end:

```
tridentctl delete backend <backend-name> -n trident
```



Si Trident ha aprovisionado volúmenes y snapshots a partir de este back-end que aún existen, al eliminar el back-end se evita que se aprovisionen nuevos volúmenes. El backend seguirá existiendo en estado de supresión.

Ver los back-ends existentes

Para ver los back-ends que Trident conoce, haga lo siguiente:

- Para obtener un resumen, ejecute el siguiente comando:

```
tridentctl get backend -n trident
```

- Para obtener todos los detalles, ejecute el siguiente comando:

```
tridentctl get backend -o json -n trident
```

Actualizar un back-end

Después de crear un nuevo archivo de configuración de back-end, ejecute el siguiente comando:

```
tridentctl update backend <backend-name> -f <backend-file> -n trident
```

Si falla la actualización del back-end, algo estaba mal con la configuración del back-end o intentó una actualización no válida. Puede ver los registros para determinar la causa ejecutando el siguiente comando:

```
tridentctl logs -n trident
```

Después de identificar y corregir el problema con el archivo de configuración, simplemente puede ejecutar el update comando de nuevo.

Identifique las clases de almacenamiento que utilizan un back-end

Este es un ejemplo del tipo de preguntas que puede responder con el JSON que `tridentctl` salidas para objetos backend. Utiliza la `jq` utilidad, que debe instalar.

```
tridentctl get backend -o json | jq '[.items[] | {backend: .name,
storageClasses: [.storage[].storageClasses] | unique}]'
```

Esto también se aplica a los back-ends que se crearon con el uso `TridentBackendConfig`.

Pasar entre las opciones de administración del back-end

Obtén información sobre las diferentes formas de administrar back-ends en Trident.

Opciones para gestionar back-ends

Con la introducción de `TridentBackendConfig`, los administradores ahora tienen dos formas únicas de administrar los back-ends. Esto plantea las siguientes preguntas:

- Pueden crearse back-ends con `tridentctl` administrarse con `TridentBackendConfig`?
- Pueden crearse back-ends con `TridentBackendConfig` se gestionan mediante `tridentctl`?

Gestione `tridentctl` con los back-ends `TridentBackendConfig`

En esta sección se describen los pasos necesarios para gestionar los back-ends creados con `tridentctl` Directamente mediante la interfaz de Kubernetes creando `TridentBackendConfig` objetos.

Esto se aplica a las siguientes situaciones:

- Back-ends preexistentes, que no tienen un `TridentBackendConfig` porque fueron creados con `tridentctl`.
- Nuevos back-ends que se crearon con `tridentctl`, mientras que otros `TridentBackendConfig` existen objetos.

En ambos escenarios, los back-ends seguirán presentes, con Trident programando volúmenes y operando en ellos. A continuación, los administradores tienen una de estas dos opciones:

- Siga utilizando `tridentctl` para gestionar los back-ends que se crearon con él.
- Enlazar los back-ends creados con `tridentctl` a un nuevo `TridentBackendConfig` objeto. Hacerlo significaría que se gestionarán los back-ends `kubectl` y no `tridentctl`.

Para administrar un back-end preexistente mediante `kubectl`, tendrá que crear un `TridentBackendConfig` que enlace con el backend existente. A continuación se ofrece una descripción general de cómo funciona:

1. Cree un secreto de Kubernetes. El secreto contiene las credenciales que Trident necesita para comunicarse con el clúster/servicio de almacenamiento.
2. Cree un `TridentBackendConfig` objeto. Este contiene detalles sobre el servicio/clúster de almacenamiento y hace referencia al secreto creado en el paso anterior. Se debe tener cuidado para especificar parámetros de configuración idénticos (como `spec.backendName`, `spec.storagePrefix`, `spec.storageDriverName`, y así sucesivamente). `spec.backendName` se debe establecer el nombre del backend existente.

Paso 0: Identificar el back-end

Para crear un `TridentBackendConfig` que se enlaza a un backend existente, necesitará obtener la configuración de backend. En este ejemplo, supongamos que se ha creado un back-end mediante la siguiente definición JSON:

```
tridentctl get backend ontap-nas-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE  | VOLUMES |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-nas-backend      | ontap-nas      | 52f2eb10-e4c6-4160-99fc-
96b3be5ab5d7 | online |          25 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

```
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"
      }
    }
  ]
}

```

Paso 1: Cree un secreto de Kubernetes

Cree un secreto que contenga las credenciales del back-end, como se muestra en este ejemplo:

```
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
```

Paso 2: Cree un `TridentBackendConfig` CR

El paso siguiente es crear un `TridentBackendConfig` CR que se enlazará automáticamente a la preexistente `ontap-nas-backend` (como en este ejemplo). Asegurarse de que se cumplen los siguientes requisitos:

- El mismo nombre de fondo se define en `spec.backendName`.
- Los parámetros de configuración son idénticos al backend original.
- Los pools virtuales (si están presentes) deben conservar el mismo orden que en el back-end original.
- Las credenciales se proporcionan a través de un secreto de Kubernetes, pero no en texto sin formato.

En este caso, el `TridentBackendConfig` tendrá este aspecto:

```
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

```

Paso 3: Compruebe el estado del TridentBackendConfig CR

Después del TridentBackendConfig se ha creado, su fase debe ser Bound. También debería reflejar el mismo nombre de fondo y UUID que el del back-end 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
Bound	Success	

#confirm that no new backends were created (i.e., TridentBackendConfig did not end up creating a new backend)

```
tridentctl get backend -n trident
```

NAME	STORAGE DRIVER	UUID
ontap-nas-backend	ontap-nas	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7
online	25	

El back-end se gestionará completamente mediante el tbc-ontap-nas-backend TridentBackendConfig objeto.

Gestione TridentBackendConfig con los back-ends tridentctl

`tridentctl` se puede utilizar para enumerar los back-ends que se crearon con `TridentBackendConfig`. Además, los administradores también pueden optar por gestionar completamente estos back-ends `tridentctl` eliminando `TridentBackendConfig` y eso seguro `spec.deletionPolicy` se establece en `retain`.

Paso 0: Identificar el back-end

Por ejemplo, supongamos que se ha creado el siguiente back-end mediante TridentBackendConfig:

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san	ontap-san-backend	81abcb27-ea63-49bb-b606-0a5315ac5f82

```
tridentctl get backend ontap-san-backend -n trident
```

NAME	STORAGE DRIVER	UUID
ontap-san-backend	ontap-san	81abcb27-ea63-49bb-b606-0a5315ac5f82

Desde la salida, se ve eso TridentBackendConfig Se ha creado correctamente y está enlazado a un backend [observe el UUID del backend].

Paso 1: Confirmar deletionPolicy **se establece en** retain

Echemos un vistazo al valor de deletionPolicy. Se debe establecer en retain. Esto garantiza que cuando se elimina un TridentBackendConfig CR, la definición de backend seguirá presente y se puede gestionar con tridentctl.

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-san	ontap-san-backend	81abcb27-ea63-49bb-b606-0a5315ac5f82

```
# 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
backend-tbc-ontap-san	ontap-san-backend	81abcb27-ea63-49bb-b606-0a5315ac5f82



No continúe con el siguiente paso a menos que `deletionPolicy` se establece en `retain`.

Paso 2: Elimine la `TridentBackendConfig` CR

El paso final es eliminar la `TridentBackendConfig` CR. Tras confirmar la `deletionPolicy` se establece en `retain`, puede utilizar `Adelante` con la eliminación:

```
kubect1 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 |
+-----+-----+
+-----+-----+-----+-----+
```

Tras la eliminación del `TridentBackendConfig` objeto, Trident simplemente lo elimina sin eliminar realmente el backend.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.