



Configura y gestiona backends

Trident

NetApp
October 29, 2026

Tabla de contenidos

Configura y gestiona backends	1
Configurar los backends de Trident	1
Azure NetApp Files	1
Configura un backend de Azure NetApp Files	1
Prepárate para configurar un backend de Azure NetApp Files	4
Opciones y ejemplos de configuración del backend de Azure NetApp Files	7
Google Cloud NetApp Volumes	18
Configura Google Cloud NetApp Volumes	18
Configura Google Cloud NetApp Volumes para cargas de trabajo SAN	22
Prepárate para configurar un backend de Google Cloud NetApp Volumes	28
Opciones y ejemplos de configuración del backend de Google Cloud NetApp Volumes	28
Configura la jerarquización automática para Google Cloud NetApp Volumes	39
Configura los grupos de almacenamiento en modo ONTAP de Google Cloud NetApp Volumes	42
Configura un backend de NetApp HCI o SolidFire	46
Detalles del controlador Element	46
Antes de empezar	47
Opciones de configuración del backend	47
Ejemplo 1: configuración de backend para <code>solidfire-san</code> driver con tres tipos de volumen	48
Ejemplo 2: configuración de backend y clase de almacenamiento para <code>`solidfire-san`</code> driver con grupos virtuales	48
Encuentra más información	51
Controladores SAN de ONTAP	51
Descripción general del controlador SAN de ONTAP	51
Prepárate para configurar el backend con controladores SAN de ONTAP	53
Opciones de configuración y ejemplos de ONTAP SAN	61
Controladores NAS de ONTAP	78
Descripción general del controlador NAS de ONTAP	78
Prepárate para configurar un backend con controladores ONTAP NAS	79
Opciones de configuración y ejemplos de ONTAP NAS	91
Utiliza la distribución equilibrada con los backends de ONTAP	112
Cómo funciona la asignación equilibrada	112
Requisitos	112
Valores por defecto	112
Opción de configuración	113
Asignación equilibrada con grupos virtuales	113
Ejemplos	113
Errores de validación del backend	114
Amazon FSx for NetApp ONTAP	114
Usa Trident con Amazon FSx for NetApp ONTAP	114
Crea un rol de IAM y un secreto de AWS	117
Instala Trident	122
Configurar una clase de almacenamiento	128
Configura un PVC	142

Implementa una aplicación	144
Implementa una aplicación de ejemplo	144
Configura el complemento Trident EKS en un clúster EKS	145
Crea backends con kubectl	148
TridentBackendConfig	149
Resumen de pasos	150
Paso 1: crea un secreto de Kubernetes	150
Paso 2: crea el `TridentBackendConfig`CR	152
Paso 3: verifica el estado de la `TridentBackendConfig`CR	152
(Opcional) Paso 4: obtén más detalles	153
Gestiona backends	154
Gestiona los backends de Trident con kubectl	154
Gestiona los backends de Trident con tridentctl	156
Elige un método de gestión del backend de Trident	157

Configura y gestiona backends

Configurar los backends de Trident

Un backend define la relación entre Trident y un sistema de almacenamiento. Le dice a Trident cómo comunicarse con ese sistema de almacenamiento y cómo Trident debe aprovisionar volúmenes desde él.

Trident ofrece automáticamente grupos de almacenamiento de backends que cumplen los requisitos definidos por una clase de almacenamiento. Aprende cómo configurar el backend para tu sistema de almacenamiento.

- ["Configura un backend de Azure NetApp Files"](#)
- ["Configura un backend de Google Cloud NetApp Volumes"](#)
- ["Configura un backend de NetApp HCI o SolidFire"](#)
- ["Configura un backend con controladores NAS ONTAP o Cloud Volumes ONTAP"](#)
- ["Configura un backend con controladores SAN ONTAP o Cloud Volumes ONTAP"](#)
- ["Usa Trident con Amazon FSx for NetApp ONTAP"](#)

Azure NetApp Files

Configura un backend de Azure NetApp Files

Usa Azure NetApp Files como backend para Trident. Este backend admite volúmenes NFS y SMB. Trident admite identidades gestionadas e identidad de carga de trabajo para clústeres de Azure Kubernetes Service (AKS).

Entornos cloud de Azure compatibles

Trident es compatible con los backends de Azure NetApp Files en varios entornos cloud de Azure.

Las nubes de Azure compatibles incluyen:

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

Cuando despliegues Trident o configures un backend de Azure NetApp Files, asegúrate de que Azure Resource Manager y los endpoints de autenticación coincidan con tu entorno de cloud de Azure.

Revisa el soporte del controlador de Azure NetApp Files

Trident proporciona el siguiente controlador de almacenamiento Azure NetApp Files.

Los modos de acceso admitidos incluyen *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX) y *ReadWriteOncePod* (RWOP).

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

Revisa las consideraciones

- Azure NetApp Files no admite volúmenes menores de 50 GiB. Trident crea un volumen de 50 GiB cuando se solicita un volumen menor.
- Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows.
- Las implementaciones de Azure NetApp Files en nubes Azure no comerciales requieren puntos finales de Azure Resource Manager y de autenticación específicos para cada nube. Asegúrate de que Trident y cualquier configuración de backend usen los puntos finales apropiados para tu entorno de nube Azure.

Usa identidades gestionadas para AKS

Trident es compatible con "identidades gestionadas" para clústeres AKS.

Si usas `tridentctl` para crear o gestionar backends de Azure NetApp Files, asegúrate de que esté configurado para el entorno de cloud de Azure correcto.

Para usar identidades gestionadas, debes tener:

- Un clúster de Kubernetes implementado mediante AKS
- Identidades gestionadas configuradas en el clúster de Kubernetes de AKS
- Trident instalado con `cloudProvider` configurado en "Azure"

Operador de Trident

Edita `tridentorchestrator_cr.yaml` y establece `cloudProvider` en "Azure".

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

Helm

El siguiente ejemplo instala Trident y configura `cloudProvider` usando la variable de entorno `$CP`:

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

`<code>tridentctl</code>`

El siguiente ejemplo instala Trident y establece la `cloud-provider` bandera en Azure:

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

Usa la identidad de carga de trabajo para AKS

La identidad de carga de trabajo permite que los pods de Kubernetes accedan a los recursos de Azure autenticándose como una identidad de carga de trabajo.

Si usas `tridentctl` para crear o gestionar backends de Azure NetApp Files, asegúrate de que esté configurado para el entorno de cloud de Azure correcto.

Para usar la identidad de carga de trabajo, debes tener:

- Un clúster de Kubernetes implementado mediante AKS
- Identidad de carga de trabajo y `oidc-issuer` configurados en el clúster AKS Kubernetes
- Trident instalado con `cloudProvider` configurado en "Azure" y `cloudIdentity` configurado en el valor de identidad de la carga de trabajo

Operador de Trident

Edita `tridentorchestrator_cr.yaml` y establece `cloudProvider` en "Azure". Establece `cloudIdentity` en `azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx`.

```
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-xxxxxxxxxx' # Edit
```

Helm

Establece los valores para las opciones **cloud-provider (CP)** y **cloud-identity (CI)** usando las siguientes variables de entorno:

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

El siguiente ejemplo instala Trident y establece `cloudProvider` usando `$CP` y establece `cloudIdentity` usando `$CI`:

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

`tridentctl`

Establece los valores para las banderas **cloud provider** y **cloud identity** usando las siguientes variables de entorno:

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

El siguiente ejemplo instala Trident y establece `cloud-provider` en `$CP` y `cloud-identity` en `$CI`:

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

Prepárate para configurar un backend de Azure NetApp Files

Antes de que puedas configurar tu backend de Azure NetApp Files, necesitas asegurarte de que se cumplan los siguientes requisitos.

Entornos cloud de Azure compatibles

Trident es compatible con los backends de Azure NetApp Files en varios entornos cloud de Azure.

Las nubes de Azure compatibles incluyen:

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

Cuando prepares tu entorno, asegúrate de que tu suscripción de Azure, la configuración de identidad y los recursos de Azure NetApp Files se creen en el entorno de cloud de Azure adecuado.

Requisitos previos para volúmenes NFS y SMB

Si estás usando Azure NetApp Files por primera vez o en una nueva ubicación, necesitas hacer una configuración inicial para preparar Azure NetApp Files y crear un volumen NFS. Consulta ["Azure: configura Azure NetApp Files y crea un volumen NFS"](#).

Para configurar y usar un ["Azure NetApp Files"](#) backend, necesitas lo siguiente:



- `subscriptionID`, `tenantID`, `clientID`, `location` y `clientSecret` son opcionales cuando usas identidades administradas en un clúster de AKS.

- `tenantID`, `clientID` y `clientSecret` son opcionales cuando usas una identidad en la nube en un clúster de AKS.
- Las implementaciones de Azure NetApp Files en nubes Azure no comerciales requieren puntos finales de Azure Resource Manager y de autenticación específicos para cada nube. Asegúrate de que Trident y cualquier configuración de backend usen los puntos finales apropiados para tu entorno de nube Azure.

- Un fondo de capacidad. Consulta ["Microsoft: crea un grupo de capacidad para Azure NetApp Files"](#).
- Una subred delegada a Azure NetApp Files. Consulta ["Microsoft: delega una subred a Azure NetApp Files"](#).
- `subscriptionID` desde una suscripción de Azure con Azure NetApp Files habilitado.
- `tenantID`, `clientID` y `clientSecret` de un ["Registro de la aplicación"](#) en Azure Active Directory con permisos suficientes para el servicio Azure NetApp Files. El registro de la aplicación debe usar una de las siguientes opciones:
 - El rol de Owner o Contributor ["predefinido por Azure"](#).
 - A ["rol de 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, ["asigna el rol usando el portal de Azure"](#).

▼ Rol de colaborador personalizado

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

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

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

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

          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",
        ]
      }
    ]
  }
}
```

```

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

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

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

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

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

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

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

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

```

- El Azure location que contiene al menos un ["subred delegada"](#). Desde Trident 22.01, el parámetro location es un campo obligatorio en el nivel superior del archivo de configuración del backend. Se ignoran los valores de ubicación especificados en los grupos virtuales.
- Para usar Cloud Identity, consigue el client ID de un ["identidad administrada asignada por el usuario"](#) y especifica ese ID en azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.

Requisitos adicionales para volúmenes SMB

Para crear un volumen SMB, debes tener:

- Active Directory configurado y conectado a Azure NetApp Files. Consulta ["Microsoft: crear y administrar conexiones de Active Directory para Azure NetApp Files"](#).
- Un clúster de Kubernetes con un nodo controlador Linux y al menos un nodo trabajador Windows que ejecuta Windows Server 2022. Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows.
- Al menos un secreto de Trident que contenga tus credenciales de Active Directory para que Azure NetApp Files pueda autenticarse en Active Directory. Para generar un secreto `smbcreds`:

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

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

Opciones y ejemplos de configuración del backend de Azure NetApp Files

Conoce las opciones de configuración de backend de NFS y SMB para Azure NetApp Files y revisa ejemplos de configuración.

Opciones de configuración del backend

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

Los backends de Azure NetApp Files proporcionan estas opciones de configuración.

Parámetro	Descripción	Predeterminado
<code>version</code>	Versión de configuración del backend.	Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	"azure-netapp-files"
<code>backendName</code>	Nombre personalizado para el backend de almacenamiento	Nombre del driver + "_" + caracteres aleatorios
<code>subscriptionID</code>	El identificador de suscripción de tu suscripción de Azure opcional cuando las identidades administradas están habilitadas en un clúster de AKS.	
<code>tenantID</code>	El ID del inquilino de un App Registration es opcional cuando se usan identidades administradas o identidad en la nube en un clúster de AKS.	

Parámetro	Descripción	Predeterminado
<code>clientID</code>	El ID de cliente de un registro de aplicación, opcional cuando se usan identidades administradas o identidad en la nube en un clúster de AKS.	
<code>clientSecret</code>	El secreto del cliente de un registro de aplicación es opcional cuando se usan identidades administradas o identidad en la nube en un clúster de AKS.	
<code>serviceLevel</code>	Uno de Standard, Premium o Ultra	"" (aleatorio)
<code>location</code>	Nombre de la ubicación de Azure donde se crearán los nuevos volúmenes Opcional cuando las identidades administradas están habilitadas en un clúster de AKS.	
<code>cloudConfiguration.cloudName</code>	Identifica el entorno de nube de Azure para el backend. Configúralo como <code>AzureGovernment</code> cuando uses Azure Government.	
<code>resourceGroups</code>	Lista de grupos de recursos para filtrar recursos descubiertos	[] (sin filtro)
<code>netappAccounts</code>	Lista de cuentas de NetApp para filtrar recursos descubiertos	[] (sin filtro)
<code>capacityPools</code>	Lista de grupos de capacidad para filtrar recursos descubiertos	[] (sin filtro, aleatorio)
<code>virtualNetwork</code>	Nombre de una red virtual con una subred delegada	""
<code>subnet</code>	Nombre de una subred delegada a <code>Microsoft.Netapp/volumes</code>	""
<code>networkFeatures</code>	Conjunto de funciones de VNet para un volumen, puede ser <code>Basic</code> o <code>Standard</code> . Network Features no está disponible en todas las regiones y podría tener que habilitarse en una suscripción. Especificar <code>networkFeatures</code> cuando la funcionalidad no está habilitada hace que falle el aprovisionamiento del volumen.	""

Parámetro	Descripción	Predeterminado
nfsMountOptions	Control detallado de las opciones de montaje de NFS. Ignorado para volúmenes SMB. Para montar volúmenes usando la versión de NFS 4.1, incluye <code>nfsvers=4</code> en la lista de opciones de montaje separadas por comas para elegir NFS v4.1. Las opciones de montaje establecidas en una definición de clase de almacenamiento reemplazan las opciones de montaje establecidas en la configuración de backend.	"nfsvers=3"
limitVolumeSize	Falla el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor	"" (no aplicado por defecto)
debugTraceFlags	Indicadores de depuración para utilizar cuando estés solucionando problemas. Ejemplo, <code>\{"api": false, "method": true, "discovery": true\}</code> . No uses esto a menos que estés resolviendo problemas y necesites un volcado detallado del registro.	null
nasType	Configura la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o <code>null</code> . Si lo configuras en <code>null</code> , se usarán volúmenes NFS por defecto.	nfs
supportedTopologies	Representa una lista de regiones y zonas compatibles con este backend. Para obtener más información, consulta "Usa la topología CSI" .	
qosType	Representa el tipo de QoS: automático o manual.	Automático
maxThroughput	Establece el rendimiento máximo permitido en MiB/s. Compatible solo con grupos de capacidad de QoS manual.	4 MiB/sec



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

Considera los entornos cloud de Azure (26.06)

A partir de la versión 26.06, Trident admite la creación y gestión de backends de Azure NetApp Files en varios entornos cloud de Azure.

Las nubes de Azure compatibles incluyen:

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

Cuando despliegas Trident o creas un backend de Azure NetApp Files, asegúrate de que Azure Resource Manager y los endpoints de autenticación coincidan con tu entorno de Azure cloud. Si los endpoints no coinciden, `tridentctl` no puede autenticarse y la creación del backend falla.

Para un backend de Azure Government, configura `cloudConfiguration.cloudName` en la configuración del backend:

```
cloudConfiguration:
  cloudName: AzureGovernment
```

Permisos y recursos necesarios

Si recibes el error "No capacity pools found" al crear un PVC, es probable que el registro de tu aplicación no tenga los permisos y recursos necesarios (subred, red virtual, capacity pool) asociados. Si la depuración está activada, Trident registra los recursos de Azure descubiertos cuando se crea el backend. Verifica que se esté usando un rol adecuado.

Los valores para `resourceGroups`, `netappAccounts`, `capacityPools`, `virtualNetwork` y `subnet` se pueden especificar usando nombres cortos o nombres completamente calificados. Se recomiendan los nombres completamente calificados en la mayoría de las situaciones, ya que los nombres cortos pueden coincidir con varios recursos con el mismo nombre.



Si la vNet está ubicada en un grupo de recursos diferente de la cuenta de almacenamiento de Azure NetApp Files (ANF), especifica el grupo de recursos para la red virtual mientras configuras la lista `resourceGroups` para el backend.

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

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

Aprovisionamiento de volumen

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

Parámetro	Descripción	Predeterminado
exportRule	Reglas de exportación para volúmenes nuevos. exportRule debe ser una lista separada por comas de cualquier combinación de direcciones IPv4 o subredes IPv4 en notación CIDR. Ignorado para volúmenes SMB.	"0.0.0.0/0"
snapshotDir	Acceso al .snapshot directorio	true, false (establecer explícitamente).
size	El tamaño predeterminado de los nuevos volúmenes	"100G"
unixPermissions	Los permisos unix de nuevos volúmenes (4 dígitos octales). Ignorado para volúmenes SMB.	"" (función de vista previa, requiere whitelisting en la suscripción)

Configuraciones de ejemplo

Los siguientes ejemplos muestran configuraciones básicas que dejan la mayoría de los parámetros en sus valores predeterminados. Esta es la forma más fácil de definir un backend.

▼ Configuración mínima

Esta es la configuración mínima absoluta del backend. Con esta configuración, Trident detecta todas tus cuentas NetApp, grupos de capacidad y subredes delegadas a Azure NetApp Files en la ubicación configurada, y coloca los nuevos volúmenes en uno de esos grupos y subredes aleatoriamente. Porque `nasType` se omite, la `nfs` configuración predeterminada se aplica y el backend aprovisionará volúmenes NFS.

Esta configuración es ideal cuando recién estás empezando a usar Azure NetApp Files y estás probando cosas, pero en la práctica vas a querer proporcionar un alcance adicional para los volúmenes que aprovisiones.

```
---
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 usas identidades administradas.

```
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 en la nube para AKS

Esta configuración de backend omite `tenantID`, `clientID` y `clientSecret`, que son opcionales cuando usas una identidad en la 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 específica del nivel de servicio con filtros de grupo de capacidad

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

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

▼ Ejemplo de backend con grupos de capacidad QoS manuales

Esta configuración de back-end coloca volúmenes en la `eastus` ubicación de Azure con grupos de capacidad de QoS manuales.

```
---
version: 1
storageDriverName: azure-netapp-files
backendName: anf1
location: eastus
labels:
  clusterName: test-cluster-1
  cloud: anf
  nasType: nfs
defaults:
  qosType: Manual
storage:
  - serviceLevel: Ultra
    labels:
      performance: gold
    defaults:
      maxThroughput: 10
  - serviceLevel: Premium
    labels:
      performance: silver
    defaults:
      maxThroughput: 5
  - serviceLevel: Standard
    labels:
```

```
performance: bronze
defaults:
  maxThroughput: 3
```

▼ Configuración avanzada

Esta configuración de backend reduce aún más el alcance de la ubicación del volumen a una sola subred, y también modifica algunos valores predeterminados de aprovisionamiento de volumen.

```
---
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 virtual pool

Esta configuración de backend define varios grupos de almacenamiento en un solo archivo. Esto es útil cuando tienes varios grupos de capacidad que admiten diferentes niveles de servicio y quieres crear clases de almacenamiento en Kubernetes que los representen. Se usaron etiquetas de grupo virtual para diferenciar los grupos 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 usa 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 en cada nodo del 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, consulta ["Usa la 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

Las siguientes `StorageClass` definiciones se refieren a los grupos de almacenamiento anteriores.

Ejemplos de definiciones usando `parameter.selector` field

Usando `parameter.selector` puedes especificar para cada `StorageClass` el pool virtual que se usa para alojar un volumen. El volumen tendrá los aspectos definidos en el pool elegido.

```

---
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 para volúmenes SMB

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

▼ 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"
```

▼ Usando 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}
```

▼ Usando 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`filtros para grupos que admiten volúmenes SMB.
`nasType: nfs o `nasType: null`filtros para grupos NFS.`

Crea el backend

Después de crear el archivo de configuración de backend, ejecuta el siguiente comando:

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

Si usas una nube Azure no comercial, asegúrate de que `tridentctl` esté configurado para usar los endpoints de Azure Resource Manager y autenticación para tu entorno de nube Azure. Si falla la creación del backend, revisa tu configuración del backend y mira los registros para ver cuál es la causa:

```
tridentctl logs
```

Después de identificar y corregir el problema con el archivo de configuración, puedes volver a ejecutar el comando `create`.

Google Cloud NetApp Volumes

Configura Google Cloud NetApp Volumes

Puedes configurar Google Cloud NetApp Volumes como backend para que Trident aprovisiona almacenamiento para cargas de trabajo de Kubernetes.

Descripción general

Trident es compatible con Google Cloud NetApp Volumes tanto para cargas de trabajo NAS (NFS y SMB) como en bloque (iSCSI).

- Las cargas de trabajo NAS utilizan el `google-cloud-netapp-volumes backend`
- Las cargas de trabajo en bloque (iSCSI) utilizan el `google-cloud-netapp-volumes-san backend`

Los volúmenes NAS proporcionan almacenamiento basado en archivos y se accede a ellos mediante protocolos NFS o SMB. Estos volúmenes admiten el acceso compartido a través de varios pods o nodos.

Los volúmenes en bloque proporcionan almacenamiento en bloque sin procesar y se accede a ellos como dispositivos iSCSI conectados a nodos Kubernetes. Estos volúmenes se utilizan cuando las aplicaciones requieren acceso a nivel de bloque.

Esto se aplica a los siguientes entornos:

- Trident 26.02 y posteriores
- Google Kubernetes Engine (GKE) o Red Hat OpenShift
- Pools de almacenamiento de Google Cloud NetApp Volumes

Para configurar el almacenamiento en bloque (iSCSI), consulta ["Configura el almacenamiento en bloque"](#)

(iSCSI)".

Prepárate para configurar

La identidad en la nube permite que las cargas de trabajo de Kubernetes accedan a los recursos de Google Cloud autenticándose como una identidad de carga de trabajo en vez de usar credenciales estáticas.

Para usar la identidad en la nube con Google Cloud NetApp Volumes, debes tener:

- Un clúster de Kubernetes desplegado usando Google Kubernetes Engine (GKE)
- Identidad de carga de trabajo habilitada en el clúster GKE y el servidor de metadatos habilitado en los grupos de nodos
- Una cuenta de servicio de Google Cloud con la función de Google Cloud NetApp Volumes Admin (roles/netapp.admin) o una función personalizada equivalente
- Trident instalado con el cloud provider establecido en GCP y la cloud identity annotation configurada

Operador de Trident

Para instalar Trident utilizando el operador Trident, edita `tridentorchestrator_cr.yaml`:

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

Helm

Establece el proveedor de la nube y la identidad de la nube al instalar Trident con Helm:

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

tridentctl

Instala Trident especificando el proveedor de la nube y la identidad de la nube:

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

```
-n trident
```

Configurar el almacenamiento NAS



Para los grupos de almacenamiento UNIFIED de Google Cloud NetApp Volumes, Trident aplica reglas de nomenclatura y validación específicas de UNIFIED durante las operaciones de volumen.

Al localizar un volumen, Trident puede evaluar múltiples variantes de nombre de volumen compatibles (por ejemplo, formatos de guion y guion bajo) para mejorar la fiabilidad de la importación y el descubrimiento.

Detalles del controlador

Trident proporciona el `google-cloud-netapp-volumes` controlador para aprovisionar almacenamiento NAS desde Google Cloud NetApp Volumes.

El controlador admite los siguientes modos de acceso:

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

Controlador	Protocolo	volumeMod e	Modos de acceso admitidos	Sistemas de archivos compatibles
google-cloud-netapp-volumes	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	nfs, smb

Configura un backend NAS Trident

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

Aprovisionar volúmenes NAS

Los volúmenes NAS se aprovisionan usando el `google-cloud-netapp-volumes` backend y son compatibles con los protocolos NFS y SMB.

StorageClass para volúmenes NFS

Para aprovisionar volúmenes NFS, establece `nasType` en `nfs`.

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

StorageClass para volúmenes SMB

Para aprovisionar volúmenes SMB, establece `nasType` en `smb` y proporciona las credenciales.

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

Ejemplo de PersistentVolumeClaim (RWX)

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: gcnv-nas-rwx
spec:
  accessModes:
    - ReadWriteMany
  resources:
```

```
requests:
  storage: 100Gi
storageClassName: gcnv-nfs
```

Ejemplo de PersistentVolumeClaim (RWO)

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



Los volúmenes NAS usan `volumeMode: Filesystem`.

Configura Google Cloud NetApp Volumes para cargas de trabajo SAN

Puedes configurar Trident para aprovisionar volúmenes de almacenamiento en bloque usando el protocolo iSCSI desde Google Cloud NetApp Volumes. Los volúmenes SAN se aprovisionan desde grupos de almacenamiento Flex Unified usando el controlador de almacenamiento `google-cloud-netapp-volumes-san`.



Este controlador está dedicado a cargas de trabajo en bloque y no es compatible con protocolos NAS.



El `google-cloud-netapp-volumes-san` backend es necesario para aprovisionar volúmenes de bloques iSCSI. El `google-cloud-netapp-volumes` backend admite solo protocolos NAS y no puede usarse para cargas de trabajo SAN.

Descripción general

Trident es compatible con las cargas de trabajo SAN (iSCSI) de Google Cloud NetApp Volumes mediante el controlador `google-cloud-netapp-volumes-san`.

Los volúmenes SAN se aprovisionan desde grupos de almacenamiento Flex Unified y se presentan a los nodos de Kubernetes como dispositivos de bloques iSCSI.

Esto se aplica a los siguientes entornos:

- Trident 26.02 y posteriores

- Google Kubernetes Engine (GKE) o Red Hat OpenShift
- Pools de almacenamiento unificado de Google Cloud NetApp Volumes Flex
- cargas de trabajo basadas en iSCSI

Pools de almacenamiento unificado Flex

Los grupos de almacenamiento de Flex Unified proporcionan almacenamiento en bloque mediante el protocolo iSCSI y son necesarios para el aprovisionamiento de SAN:

- Se admiten los pools REGIONALES de Flex Unified.
- Las agrupaciones de Flex Unified ZONAL son compatibles a partir de Trident 26.02.1.
- Solo se admite el nivel de servicio **Flex** para cargas de trabajo SAN.

Configura un backend SAN Trident

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

Crea un StorageClass

Después de configurar el backend SAN, crea un StorageClass que haga referencia al google-cloud-netapp-volumes-san driver.

El tipo de sistema de archivos se define en el StorageClass, no en el backend.

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

```
backendType: "google-cloud-netapp-volumes-san"
fsType: "ext4"
allowVolumeExpansion: true
```

Tipos de sistemas de archivos compatibles:

- ext4 (predeterminado)
- ext3
- xfs



El controlador SAN solo es compatible con el nivel de servicio Flex y no utiliza parámetros de backend específicos de NAS como `exportRule`, `unixPermissions`, `nasType`, `snapshotDir`, `nfsMountOptions` o configuraciones relacionadas con el tiering.

Provisiona volúmenes en bloque

ReadWriteOnce (RWO)

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

ReadWriteOncePod (RWOP)

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

ReadOnlyMany (ROX)

Un patrón común para ROX es clonar un volumen ReadWriteOnce existente y montar el clon como de solo lectura.

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

ReadWriteMany (RWX) — solo bloque en bruto

ReadWriteMany solo se admite cuando `volumeMode: Block`.

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

Comportamiento del volumen de bloques

Los volúmenes de bloques se aprovisionan como LUN iSCSI y se presentan a los nodos de Kubernetes como dispositivos de bloque.

Volúmenes en bloque:

- Usa el protocolo iSCSI
- Soporte para sistema de archivos y presentación de bloques sin procesar

- Están adjuntos y gestionados por Trident
- Soporta múltiples modos de acceso a Kubernetes

Modos de acceso

Los volúmenes en bloque aprovisionados por Trident admiten los siguientes modos de acceso:

- `ReadWriteOnce` (RWO)
- `ReadOnlyMany` (ROX)
- `ReadWriteOncePod` (RWOP)
- `ReadWriteMany` (RWX), compatible solo cuando `volumeMode: Block`

volumeMode comportamiento

El `volumeMode` campo controla cómo se expone un volumen de bloque:

- `Filesystem` Trident formatea y monta el volumen.
- `Block` Trident conecta el dispositivo y lo expone como un dispositivo de bloque sin procesar.

Operaciones compatibles

Los volúmenes en bloque aprovisionados usando el controlador `google-cloud-netapp-volumes-san` admiten:

- Crear
- Borrar
- Clonar
- Snapshot
- Cambiar tamaño
- Importar

Comportamiento de la sobreaprovisionamiento de GiB extra

Google Cloud NetApp Volumes los volúmenes en bloque incluyen una sobrecarga interna de metadatos. Esta sobrecarga reduce el tamaño del dispositivo visible desde el kernel en comparación con la capacidad provisionada.

Las pruebas muestran:

- Aproximadamente 300 KiB de sobrecarga en la creación inicial
- Hasta aproximadamente 107 MiB de sobrecarga después de un redimensionamiento

Porque Google Cloud NetApp Volumes acepta solo asignaciones de GiB enteros, Trident se asegura de que el tamaño utilizable del dispositivo siempre cumpla o supere la solicitud de PVC:

- Redondeando el tamaño solicitado al siguiente GiB entero
- Agregando un búfer adicional de 1 GiB

Ejemplo:

- Solicitud de PVC: 100 GiB
- Tamaño aprovisionado en Google Cloud NetApp Volumes: 101 GiB
- Espacio útil visible para la aplicación: al menos 100 GiB

Ejemplos de pods

Volumen de bloque montado en el sistema de archivos (RWO)

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

Dispositivo de bloque raw (RWX)

```
apiVersion: v1
kind: Pod
metadata:
  name: app-raw-rwx
spec:
  containers:
  - name: app
    image: ubuntu:22.04
    command: ["sleep", "infinity"]
    volumeDevices:
    - name: data
      devicePath: /dev/xda
  volumes:
  - name: data
    persistentVolumeClaim:
      claimName: gcnv-san-raw-rwx
```

Comportamiento de attach y mount

Para volúmenes SAN aprovisionados desde Google Cloud NetApp Volumes:

- Trident crea un Logical Unit Number (LUN) en un grupo de almacenamiento Flex Unified.
- Durante la publicación, Trident asigna el LUN a un grupo de hosts por nodo.
- Durante la puesta en escena del nodo, Trident:
 - Inicia sesión en el target iSCSI
 - Descubre el LUN
 - Configura multivía
- Si `volumeMode: Filesystem`, Trident formatea el dispositivo si es necesario y lo monta.
- Si `volumeMode: Block`, Trident conecta el dispositivo y lo expone directamente al pod sin formatear ni montar.



Los volúmenes de bloques SAN no proporcionan bloqueo distribuido ni coordinación de escritura. Cuando un volumen de bloques es accedido por varios nodos (ReadWriteMany con `volumeMode: Block`), la aplicación o el sistema de archivos debe gestionar la concurrencia.

Prepárate para configurar un backend de Google Cloud NetApp Volumes

Antes de que puedas configurar tu backend de Google Cloud NetApp Volumes, necesitas asegurarte de que se cumplan los siguientes requisitos.

Requisitos previos para volúmenes NFS o SMB

Si estás usando Google Cloud NetApp Volumes por primera vez o en una ubicación nueva, necesitas hacer una configuración inicial para configurar Google Cloud NetApp Volumes y crear un volumen NFS o SMB. Consulta ["Antes de empezar"](#).

Asegúrate de tener lo siguiente antes de configurar el backend de Google Cloud NetApp Volumes:

- Una cuenta de Google Cloud configurada con el servicio Google Cloud NetApp Volumes. Consulta ["Google Cloud NetApp Volumes"](#).
- Número de proyecto de tu cuenta de Google Cloud. Consulta ["Identificación de proyectos"](#).
- Una cuenta de servicio de Google Cloud con el rol de NetApp Volumes Admin (`roles/netapp.admin`). Consulta ["Roles y permisos de Identity and Access Management"](#).
- Archivo de clave API para tu cuenta GCNV. Consulta ["Crear una clave de cuenta de servicio"](#).
- Un grupo de almacenamiento. Consulta ["Descripción general de los storage pools"](#).

Para obtener más información sobre cómo configurar el acceso a Google Cloud NetApp Volumes, consulta ["Configura el acceso a Google Cloud NetApp Volumes"](#).

Opciones y ejemplos de configuración del backend de Google Cloud NetApp Volumes

Conoce las opciones de configuración de backend para Google Cloud NetApp Volumes y revisa ejemplos de configuración.

Opciones de configuración del backend

Cada backend aprovisiona volúmenes en una única región de Google Cloud. Para crear volúmenes en otras regiones, puedes definir backends adicionales.

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	El valor de <code>storageDriverName</code> debe especificarse como "google-cloud-netapp-volumes".
backendName	(Opcional) Nombre personalizado del backend de almacenamiento	Nombre del driver + "_" + parte de la clave API
storagePools	Parámetro opcional usado para especificar grupos de almacenamiento para la creación de volúmenes.	
projectNumber	Número de proyecto de la cuenta de Google Cloud. El valor se encuentra en la página de inicio del portal de Google Cloud.	
location	La ubicación de Google Cloud donde Trident crea volúmenes GCNV. Al crear clústeres de Kubernetes entre regiones, los volúmenes creados en un <code>location</code> se pueden usar en cargas de trabajo programadas en nodos de varias regiones de Google Cloud. El tráfico entre regiones tiene un costo adicional.	
apiKey	Clave API para la cuenta de servicio de Google Cloud con la <code>netapp.admin</code> función. Incluye el contenido en formato JSON del archivo de clave privada de una cuenta de servicio de Google Cloud (copiado textualmente en el archivo de configuración del backend). El <code>apiKey</code> debe incluir pares clave-valor para las siguientes claves: <code>type</code> , <code>project_id</code> , <code>client_email</code> , <code>client_id</code> , <code>auth_uri</code> , <code>token_uri</code> , <code>auth_provider_x509_cert_url</code> y <code>client_x509_cert_url</code> .	
nfsMountOptions	Control detallado de las opciones de montaje de NFS.	"nfsvers=3"
limitVolumeSize	Falla el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor.	"" (no aplicado por defecto)
serviceLevel	El nivel de servicio de un pool de almacenamiento y sus volúmenes. Los valores son <code>flex</code> , <code>standard</code> , <code>premium</code> o <code>extreme</code> .	
labels	Conjunto de etiquetas arbitrarias con formato JSON para aplicar en volúmenes	""
network	Red de Google Cloud utilizada para volúmenes GCNV.	

Parámetro	Descripción	Predeterminado
debugTraceFlags	Indicadores de depuración para utilizar cuando estés solucionando problemas. Ejemplo, {"api":false, "method":true}. No uses esto a menos que estés resolviendo problemas y necesites un volcado detallado del registro.	null
nasType	Configura la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o <code>null</code> . Si lo configuras en <code>null</code> , se usarán volúmenes NFS por defecto.	<code>nfs</code>
supportedTopologies	Representa una lista de regiones y zonas compatibles con este backend. Para obtener más información, consulta "Usa la topología CSI" . Por ejemplo: supportedTopologies: - topology.kubernetes.io/region: asia-east1 topology.kubernetes.io/zone: asia-east1-a	

Opciones de aprovisionamiento de volumen

Puedes controlar el aprovisionamiento de volúmenes predeterminados en la sección `defaults` del archivo de configuración.

Parámetro	Descripción	Predeterminado
exportRule	Las reglas de exportación para nuevos volúmenes. Debe ser una lista separada por comas de cualquier combinación de direcciones IPv4.	"0.0.0.0/0"
snapshotDir	Acceso al <code>.snapshot</code> directorio	<code>true</code> , <code>false</code> (el comportamiento por defecto puede variar. Establece explícitamente) <code>"false"</code> para NFSv3
snapshotReserve	Porcentaje de volumen reservado para instantáneas	"" (acepta el valor predeterminado de 0)
unixPermissions	Los permisos unix de nuevos volúmenes (4 dígitos octales).	""

Configuraciones de ejemplo

Los siguientes ejemplos muestran configuraciones básicas que dejan la mayoría de los parámetros en sus valores predeterminados. Esta es la forma más fácil de definir un backend.

▼ Configuración mínima

Esta es la configuración mínima absoluta del backend. Con esta configuración, Trident detecta todos tus grupos de almacenamiento delegados a Google Cloud NetApp Volumes en la ubicación configurada y coloca los nuevos volúmenes en uno de esos grupos aleatoriamente. Porque `nasType` se omite, la `nfs` configuración predeterminada se aplica y el backend aprovisionará volúmenes NFS.

Esta configuración es ideal cuando estás empezando a usar Google Cloud NetApp Volumes y probando

cosas, pero en la práctica podrías necesitar proporcionar un alcance adicional para los volúmenes que aprovisionas.



Reemplaza <id_value> y <key_value> con las credenciales de tu cuenta de servicio.

```
---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: "123455380079"
  location: europe-west6
  serviceLevel: premium
  apiKey:
    type: service_account
    project_id: my-gcnv-project
    client_email: myproject-prod@my-gcnv-project.iam.gserviceaccount.com
    client_id: "103346282737811234567"
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
    client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
  credentials:
    name: backend-tbc-gcnv-secret
```

▼ 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

```

▼ Configuración con filtro StoragePools

```

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

```

```

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

```

▼ Configuración de virtual pool

Esta configuración de backend define varios grupos virtuales en un solo archivo. Los grupos virtuales se definen en la `storage` sección. Son útiles cuando tienes varios grupos de almacenamiento que admiten diferentes niveles de servicio y quieres crear clases de almacenamiento en Kubernetes que los representen. Las etiquetas de los grupos virtuales se usan para diferenciarlos. Por ejemplo, en el ejemplo de abajo, la `performance` etiqueta y el `serviceLevel` tipo se usan para diferenciar los grupos virtuales.

También puedes establecer algunos valores predeterminados que se aplicarán a todos los grupos virtuales y sobrescribir esos valores predeterminados para grupos virtuales individuales. En el siguiente ejemplo, `snapshotReserve` y `exportRule` sirven como valores predeterminados para todos los grupos virtuales.

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

```

---
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque

```

```

stringData:
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----

---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: "123455380079"
  location: europe-west6
  apiKey:
    type: service_account
    project_id: my-gcnv-project
    client_email: myproject-prod@my-gcnv-project.iam.gserviceaccount.com
    client_id: "103346282737811234567"
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
    client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
  credentials:
    name: backend-tbc-gcnv-secret
  defaults:
    snapshotReserve: "10"
    exportRule: 10.0.0.0/24
  storage:
    - labels:
        performance: extreme
        serviceLevel: extreme
      defaults:
        snapshotReserve: "5"
        exportRule: 0.0.0.0/0
    - labels:
        performance: premium
        serviceLevel: premium
    - labels:
        performance: standard

```

```
serviceLevel: standard
```

▼ Identidad en la nube para GKE

Al instalar Trident con una identidad en la nube de GKE, los backends se autentican como una identidad de carga de trabajo y omiten el bloque `apiKey`. La identidad en la nube se configura de la misma manera para ambos controladores de Google Cloud NetApp Volumes. La única diferencia es el valor de `storageDriverName`: usa `google-cloud-netapp-volumes` para volúmenes NAS (NFS o SMB) y `google-cloud-netapp-volumes-san` para volúmenes SAN (iSCSI block).



La compatibilidad con identidades en la nube para el `google-cloud-netapp-volumes-san` driver requiere Trident 26.06 o una versión posterior. Los volúmenes SAN se aprovisionan desde los grupos de almacenamiento Flex Unified, así que configura `serviceLevel` en `flex`.

Controlador NAS (<code>google-cloud-netapp-volumes</code>)

```
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
```

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

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

▼ 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 usa 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 en cada nodo del 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, consulta ["Usa la 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
```

¿Qué sigue?

Después de crear el archivo de configuración de backend, ejecuta el siguiente comando:

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

Para verificar que el backend se haya creado correctamente, ejecuta 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 falla la creación del backend, algo anda mal con la configuración del backend. Puedes describir el backend usando el `kubectl get tridentbackendconfig <backend-name>` comando o 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, puedes eliminar el backend y ejecutar el comando create otra vez.

Definiciones de clases de almacenamiento

La siguiente es una `StorageClass` definición básica que se refiere al backend de arriba.

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

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

Usando `parameter.selector` puedes especificar para cada `StorageClass` el "pool virtual" que se utiliza para alojar un volumen. El volumen tendrá los aspectos definidos en el pool elegido.

```
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 más detalles sobre las clases de almacenamiento, consulta ["Crear una clase de almacenamiento"](#).

Definiciones de ejemplo para volúmenes SMB

Usando `nasType`, `node-stage-secret-name` y `node-stage-secret-namespace`, puedes especificar un volumen SMB y proporcionar las credenciales necesarias de Active Directory. Cualquier usuario/contraseña de Active Directory, con o sin permisos, puede usarse para el secreto de la etapa del nodo.

▼ 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"
```

▼ Usando 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}"
```

▼ Usando 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`filtros para grupos que admiten volúmenes SMB. `nasType: nfs o `nasType: null`filtros para grupos 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 el PVC está enlazado, ejecuta el siguiente comando:

```
kubect1 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	

Configura la jerarquización automática para Google Cloud NetApp Volumes

La clasificación automática se configura a través de los parámetros de backend de Trident y las anotaciones de PersistentVolumeClaim durante el aprovisionamiento de volúmenes. Puedes configurar la clasificación automática para Google Cloud NetApp Volumes usando Trident.

Descripción general

La jerarquización automática permite a Trident aprovisionar volúmenes que mueven automáticamente los datos inactivos de un nivel de rendimiento a un nivel de capacidad. Esto reduce el coste de almacenamiento mientras se preserva el rendimiento para los datos a los que se accede con frecuencia.

Trident aplica la configuración de auto-tiering solo en el momento de la creación del volumen. Los cambios posteriores al aprovisionamiento no son compatibles con Trident 26.06.

Conceptos

Organización automática en niveles

La jerarquización automática mueve los datos a los que se accede con poca frecuencia de un nivel de rendimiento a un nivel de capacidad según los patrones de acceso. El movimiento de datos ocurre de forma asíncrona y no es inmediato.

Política de tiering

La política de jerarquización determina si la jerarquización automática está habilitada para un volumen.

Se admiten las siguientes políticas: * `auto`: permite la jerarquización automática basada en patrones de acceso * `none`: desactiva la jerarquización automática

Días de refrigeración

Los días de enfriamiento especifican el número mínimo de días que un bloque de datos debe permanecer inactivo antes de que sea elegible para la clasificación por niveles. Los días de enfriamiento se aplican solo cuando la política de clasificación por niveles se establece en `auto`.

Modelo de configuración

Ámbitos de configuración

La jerarquización automática puede configurarse en varios ámbitos:

- **Ámbito del storage pool** se aplica a todos los volúmenes aprovisionados desde el pool.
- **Ámbito del volumen** Aplica a un solo volumen a través de las anotaciones de `PersistentVolumeClaim`.

Trident determina la configuración efectiva según dónde se defina cada ajuste.

Precedencia de la configuración

Cuando se define la misma configuración en varios ámbitos, Trident aplica el siguiente orden de precedencia:

1. Anotaciones de `PersistentVolumeClaim`
2. Configuración del backend Trident
3. Valores predeterminados del pool de almacenamiento

Los ajustes definidos con mayor precedencia reemplazan los valores de nivel inferior.

Funcionalidad compatible en Trident 26.06

Trident 26.06 es compatible con las siguientes funciones de auto-tiering para Google Cloud NetApp Volumes:

- Habilitar o deshabilitar la clasificación automática durante el aprovisionamiento de volúmenes
- Definir una política de niveles en la configuración del backend de Trident
- Anular la política de niveles y los días de enfriamiento por volumen usando anotaciones de PVC
- Configurar los días de enfriamiento para los volúmenes con la jerarquización automática activada

Funcionalidad no soportada en Trident 26.06

Las siguientes operaciones no son compatibles:

- Modificar la configuración de auto-tiering después de crear el volumen
- Cambio de las políticas de niveles en volúmenes existentes usando actualizaciones de Kubernetes
- Aplicar la configuración de jerarquización automática fuera de los flujos de trabajo de aprovisionamiento gestionados por Trident

Parámetros de configuración del backend

Los siguientes parámetros controlan el comportamiento del auto-tiering cuando se definen en la configuración del backend de Trident:

Parámetro	Requerido	Descripción
tieringPolicy	No	Política de tiering para volúmenes (auto o none)
tieringMinimumCoolingDays	No	Número de días inactivos antes de que los datos se transfieran de nivel (intervalo: 2–183, predeterminado: 31)

Anulaciones a nivel de volumen usando anotaciones de PersistentVolumeClaim

Anotaciones compatibles

Las anotaciones de PersistentVolumeClaim permiten anular por volumen la configuración de auto-tiering.

Anotación	Descripción
trident.netapp.io/tieringPolicy	Anula la política de tiering del volumen
trident.netapp.io/tieringMinimumCoolingDays	Anula el valor de los días de cooling para el volumen

Ejemplo: PersistentVolumeClaim con anulaciones de auto-tiering

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

storage: 500Gi

Comportamiento y limitaciones

Comportamiento del aprovisionamiento

- Los ajustes de clasificación automática se evalúan y aplican solo en el momento de la creación del volumen.
- Trident no reconcilia la configuración de tiering después del aprovisionamiento.
- Los días de enfriamiento se ignoran cuando la política de niveles se establece en `none`.

Limitaciones de la plataforma

- La jerarquización automática solo es compatible con volúmenes NAS (NFS y SMB).
- Los volúmenes en bloque (iSCSI) no admiten auto-tiering.
- El grupo de almacenamiento de Google Cloud NetApp Volumes debe tener la auto-tiering activada en Google Cloud.

Valores admitidos

- Rango válido para `tieringMinimumCoolingDays`: 2 a 183
- Valor predeterminado: 31

Configura los grupos de almacenamiento en modo ONTAP de Google Cloud NetApp Volumes

A partir de Trident 26.06, puedes configurar los backends existentes `ontap-san` y `ontap-nas` para aprovisionar almacenamiento en los grupos de almacenamiento en modo ONTAP de Google Cloud NetApp Volumes (GCNV). Esta función es una Tech Preview.

NOTA

Esta función es una Tech Preview en Trident 26.06. Las funciones en fase de Tech Preview no son compatibles para uso en producción. La funcionalidad, los campos de configuración y la matriz compatible pueden cambiar antes de la disponibilidad general (GA).

Cómo funciona

Trident reutiliza la lógica existente de los controladores `ontap-san` y `ontap-nas` y redirige las llamadas REST de ONTAP a través de un endpoint proxy de GCNV. Este enfoque te permite aprovisionar y gestionar el almacenamiento en clústeres ONTAP alojados en GCNV mientras mantienes los mismos flujos de trabajo operativos que usas para un backend ONTAP directo. ONTAP-mode no introduce un nuevo controlador de almacenamiento. Lo habilitas por backend añadiendo un bloque de configuración `gcnv` a un backend `ontap-san` o `ontap-nas`.

La ruta de aprovisionamiento es la siguiente:

PersistentVolumeClaim → Trident (`ontap-san` o `ontap-nas`) → cliente REST de ONTAP → proxy GCNV → clúster de ONTAP en el pool GCNV

Ámbito compatible y no compatible

Esta versión preliminar (Tech Preview) admite lo siguiente:

- Controladores: `ontap-san` (iSCSI) y `ontap-nas` (NFS o SMB).
- Operaciones del ciclo de vida a través del proxy: inicialización del backend, creación y eliminación de volúmenes y flujos REST de ONTAP relacionados.
- Modelos de autenticación: Workload Identity Pool (WIP), clave de cuenta de servicio y Application Default Credentials (ADC) como recurso de reserva.

Lo siguiente queda fuera del alcance de esta versión preliminar técnica:

- Los `ontap-san-economy`, `ontap-nas-economy` y `ontap-nas-flexgroup` controladores.
- La trayectoria de personalidad ASA r2.
- Solución alternativa de ZAPI. El modo ONTAP usa solo ONTAP REST.

Prerrequisitos

Antes de configurar un backend en modo ONTAP, asegúrate de que tienes lo siguiente:

- Trident 26.06 o posterior.
- Un grupo de almacenamiento GCNV en modo ONTAP en tu proyecto y ubicación de destino.
- Permisos de GCP IAM para operaciones de proxy, adaptados adecuadamente a tu entorno.
- Una configuración de backend que incluye `proxyURL`, `projectNumber`, `location` y `poolID`.
- Para los flujos de trabajo de SAN iSCSI, los requisitos previos de iSCSI y multivía del lado del nodo para tu plataforma. Consulta ["Prepara el nodo trabajador"](#).

Configura el backend

Un `TridentBackendConfig` requiere `credentials`. Para el modo ONTAP, ese secreto contiene las credenciales del proxy de GCP, no las de ONTAP `managementLIF / username / password`. `svm` es opcional: cada pool de GCNV en modo ONTAP actualmente tiene un SVM, y Trident lo obtiene del pool cuando se omite.

Utiliza el mismo patrón de cuenta de servicio que el GCNV nativo: los campos no confidenciales en `gcnv.apiKey`, `private_key` y `private_key_id` en el secreto. Consulta ["Ejemplos de configuración de Google Cloud NetApp Volumes"](#).

backend de ontap-san

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: gcnv-ontap-san
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-san
  backendName: gcnv-ontap-san
```

```

credentials:
  name: gcnv-sa-secret
  type: secret
gcnv:
  proxyURL: "https://netapp.googleapis.com"
  projectNumber: "<project-number>"
  location: "<region-or-zone>"
  poolID: "<pool-id>"
  svm: "<svm-name>"

```

backend de ONTAP-NAS

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: gcnv-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: gcnv-ontap-nas
  credentials:
    name: gcnv-sa-secret
    type: secret
  gcnv:
    proxyURL: "https://netapp.googleapis.com"
    projectNumber: "<project-number>"
    location: "<region-or-zone>"
    poolID: "<pool-id>"
    apiKey:
      type: service_account
      project_id: "<project-id>"
      client_email: "<service-account-email>"
      client_id: "<client-id>"
      auth_uri: "https://accounts.google.com/o/oauth2/auth"
      token_uri: "https://oauth2.googleapis.com/token"
      auth_provider_x509_cert_url:
        "https://www.googleapis.com/oauth2/v1/certs"
      client_x509_cert_url: "<client-x509-cert-url>"

```

Secreto

```

apiVersion: v1
kind: Secret
metadata:

```

```

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

```

NOTA

No incluyas `private_key` ni `private_key_id` en la `TridentBackendConfig spec`; el CRD los rechaza. Utiliza `ontap-san` con el mismo `gcnv` y patrón de credenciales para el almacenamiento en bloque.

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

== Authentication

Trident resolves credentials for proxy access in the following order:

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

For this Tech Preview, use the following practices:

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

== Validation and initialization behavior

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

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

== Known limitations

- * This feature is a Tech Preview. Behavior and the supported matrix can change before GA.
- * ZAPI fallback is not used in ONTAP-mode.

```
* Protocol and node-readiness requirements still apply. For example, iSCSI workflows require the node-side prerequisites described in xref:{relative_path}../trident-use/worker-node-prep.html[Prepare the worker node].
* Existing ONTAP and GCNV environment constraints still apply.
```

== Upgrade and compatibility

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

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

== What's next?

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

Configura un backend de NetApp HCI o SolidFire

Aprende cómo crear y usar un backend de Element con tu instalación de Trident.

Detalles del controlador Element

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

El `solidfire-san` 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 el `StorageClass`.

Controlador	Protocolo	VolumeMode	Modos de acceso admitidos	Sistemas de archivos compatibles
solidfire-san	iSCSI	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos. Dispositivo de bloque sin formato.
solidfire-san	iSCSI	Sistema de archivos	RWO, RWOP	xfs, ext3, ext4

Antes de empezar

Necesitarás lo siguiente antes de crear un backend de Element.

- Un sistema de almacenamiento compatible que ejecuta Element software.
- Credenciales para un administrador o usuario inquilino de un clúster NetApp HCI/SolidFire que pueda administrar volúmenes.
- Todos tus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas. Consulta ["Información de preparación del nodo worker"](#).

Opciones de configuración del backend

Consulta la siguiente tabla para ver las opciones de configuración del backend:

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	Siempre "solidfire-san"
backendName	Nombre personalizado o el backend de almacenamiento	"solidfire_" + dirección IP de almacenamiento (iSCSI)
Endpoint	MVIP para el clúster SolidFire con credenciales de inquilino	
SVIP	Dirección IP y puerto de almacenamiento (iSCSI)	
labels	Conjunto de etiquetas arbitrarias con formato JSON para aplicar en volúmenes.	""
TenantName	Nombre del tenant a usar (se crea si no se encuentra)	
InitiatorIFace	Restringe el tráfico iSCSI a una interfaz del host específica	"default"
UseCHAP	Usa CHAP para autenticar iSCSI. Trident usa CHAP.	verdadero
AccessGroups	Lista de ID de grupos de acceso para usar	Encuentra el ID de un grupo de acceso llamado "trident"
Types	Especificaciones de QoS	
limitVolumeSize	Falla el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor	"" (no aplicado por defecto)
debugTraceFlags	Indicadores de depuración para utilizar cuando estés solucionando problemas. Por ejemplo, {"api":false, "method":true}	null

ADVERTENCIA

No uses `debugTraceFlags` a menos que estés solucionando problemas y

necesites un volcado de registro detallado.

Ejemplo 1: configuración de backend para `solidfire-san` driver con tres tipos de volumen

Este ejemplo muestra un archivo backend que utiliza autenticación CHAP y modela tres tipos de volúmenes con garantías de QoS específicas. Lo más probable es que luego definas clases de almacenamiento para consumir cada uno de estos usando 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 backend y clase de almacenamiento para `solidfire-san` driver con grupos virtuales

Este ejemplo muestra el archivo de definición de backend configurado con grupos virtuales junto con `StorageClasses` que hacen referencia a ellos.

Trident copia las etiquetas presentes en un pool de almacenamiento al LUN de almacenamiento backend durante el 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 grupos virtuales se definen en la sección `storage`. En este ejemplo, algunos grupos de almacenamiento establecen su propio tipo y otros anulan los valores predeterminados establecidos arriba.

```
---
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 grupos virtuales mencionados arriba. Usando el campo `parameters.selector`, cada StorageClass indica qué grupo(s) virtual(es) se pueden usar para alojar un volumen. El volumen tendrá los aspectos definidos en el grupo virtual elegido.

El primer StorageClass (`solidfire-gold-four`) se asignará al primer pool virtual. Este es el único pool que ofrece rendimiento gold con un Volume Type QoS de Gold. El último StorageClass (`solidfire-silver`) identifica cualquier pool de almacenamiento que ofrezca un rendimiento silver. Trident decidirá qué grupo virtual se selecciona y se asegurará de 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

```

Encuentra más información

- ["Grupos de acceso a volúmenes"](#)

Controladores SAN de ONTAP

Descripción general del controlador SAN de ONTAP

Conoce cómo configurar un backend de ONTAP con los controladores SAN de ONTAP y Cloud Volumes ONTAP.

Detalles del controlador SAN de ONTAP

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

Controlador	Protocolo	volumeMod e	Modos de acceso admitidos	Sistemas de archivos compatibles
ontap-san	iSCSI SCSI sobre FC	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin formato
ontap-san	iSCSI SCSI sobre FC	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen de sistema de archivos.	xfs, ext3, ext4

Controlador	Protocolo	volumeMod e	Modos de acceso admitidos	Sistemas de archivos compatibles
ontap-san	NVMe/TCP Consulta Consideraciones adicionales para NVMe/TCP.	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin formato
ontap-san	NVMe/TCP Consulta Consideraciones adicionales para NVMe/TCP.	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen de sistema de archivos.	xfs, ext3, ext4
ontap-san-economy	iSCSI	Bloque	RWO, ROX, RWX, RWOP	Sin sistema de archivos; dispositivo de bloque sin formato
ontap-san-economy	iSCSI	Sistema de archivos	RWO, RWOP ROX y RWX no están disponibles en el modo de volumen de sistema de archivos.	xfs, ext3, ext4

ADVERTENCIA

- Usa `ontap-san-economy` solo si esperas que el recuento de uso de volúmenes persistentes sea mayor que "[límites de volúmenes compatibles de ONTAP](#)".
- Usa `ontap-nas-economy` solo si se espera que el recuento de uso de volúmenes persistentes sea mayor que "[límites de volúmenes compatibles de ONTAP](#)" y no se puede usar el controlador `ontap-san-economy`.
- No uses `ontap-nas-economy` si crees que vas a necesitar protección de datos, recuperación ante desastres o movilidad.
- NetApp no recomienda usar FlexVol autogrow en todos los controladores ONTAP, excepto `ontap-san`. Como solución alternativa, Trident admite el uso de snapshot reserve y escala los volúmenes FlexVol en consecuencia.

Permisos de usuario

Trident espera ejecutarse como administrador de ONTAP o SVM, normalmente usando el `admin`usuario` del clúster o un ``vsadmin`usuario` de SVM, o un usuario con un nombre diferente que tenga el mismo rol. Para las implementaciones de Amazon FSx for NetApp ONTAP, Trident espera ejecutarse como administrador de ONTAP o SVM, usando el usuario del clúster ``fsxadmin` o un ``vsadmin`usuario` de SVM, o un usuario con un nombre diferente que tenga el mismo rol. El ``fsxadmin`usuario` es un reemplazo limitado para el usuario administrador del clúster.

NOTA

Si usas el parámetro `limitAggregateUsage`, se requieren permisos de administrador de clúster. Cuando usas Amazon FSx for NetApp ONTAP con Trident, el parámetro `limitAggregateUsage` no funcionará con las cuentas de usuario `vsadmin` y `fsxadmin`. La operación de configuración fallará si especificas este parámetro.

Aunque es posible crear un rol más restrictivo dentro de ONTAP que un controlador Trident pueda usar, no lo recomendamos. La mayoría de las nuevas versiones de Trident llamarán a APIs adicionales que habría que tener en cuenta, lo que hace que las actualizaciones sean difíciles y propensas a errores.

Consideraciones adicionales para NVMe/TCP

Trident admite el protocolo non-volatile memory express (NVMe) usando el `ontap-san` driver, incluyendo:

- IPv6
- Instantáneas y clones de volúmenes NVMe
- Cambiar el tamaño de un volumen NVMe
- Importar un volumen NVMe que se creó fuera de Trident para que su ciclo de vida pueda ser gestionado por Trident
- Multipathing nativo de NVMe
- Apagado correcto o incorrecto de los nodos K8s (24.06)

Trident no admite:

- DH-HMAC-CHAP que es compatible de forma nativa con NVMe
- Mapeador de dispositivos (DM) multipathing
- Cifrado LUKS

NOTA

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

Prepárate para configurar el backend con controladores SAN de ONTAP

Entiende los requisitos y las opciones de autenticación para configurar un backend de ONTAP con controladores SAN de ONTAP.

Requisitos

Para todos los backends de ONTAP, Trident requiere que al menos un agregado esté asignado a la SVM.

NOTA

"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. Consulta el ["esto"](#) artículo de base de conocimientos sobre cómo asignar agregados a SVMs en sistemas ASA r2.

Recuerda que también puedes ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, podrías configurar una `san-dev` clase que use el `ontap-san` controlador y una `san-default` clase que use el `ontap-san-economy` otro.

Todos tus nodos de trabajo de Kubernetes deben tener instaladas las herramientas iSCSI adecuadas.

Consulta ["Prepara el nodo trabajador"](#) para obtener más detalles.

Autentica el backend de ONTAP

Trident ofrece dos modos de autenticación para un backend ONTAP.

- Basado en credenciales: el nombre de usuario y la contraseña de un usuario de ONTAP con los permisos necesarios. Se recomienda usar un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin` para garantizar la máxima compatibilidad con las versiones de ONTAP.
- Basado en certificado: Trident también puede comunicarse con un clúster de ONTAP usando un certificado instalado en el backend. Aquí, la definición del backend debe contener valores codificados en Base64 del certificado del cliente, la clave y el certificado de la CA de confianza si se usa (recomendado).

Puedes actualizar los backends existentes para pasar de métodos basados en credenciales a métodos basados en certificados y viceversa. Sin embargo, solo se admite un método de autenticación a la vez. Para cambiar a otro método de autenticación, debes eliminar el método existente de la configuración del backend.

ADVERTENCIA

Si intentas proporcionar **tanto credenciales como certificados**, la creación del backend fallará con un error que indica que se proporcionó más de un método de autenticación en el archivo de configuración.

Habilita la autenticación basada en credenciales

Trident requiere las credenciales de un administrador con ámbito de SVM o de clúster para comunicarse con el backend de ONTAP. Se recomienda usar roles estándar predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad futura con versiones de ONTAP que podrían exponer APIs de funciones para futuras versiones de Trident. Se puede crear y usar un rol personalizado de inicio de sesión de seguridad con Trident, pero no se recomienda.

Un ejemplo de definición de backend se verá así:

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"  
}
```

Ten en cuenta que la definición del backend es el único lugar donde se almacenan las credenciales en texto plano. Después de crear el backend, los nombres de usuario y contraseñas se codifican con Base64 y se guardan como secretos de Kubernetes. La creación o actualización de un backend es el único paso que requiere conocimiento de las credenciales. Así que es una operación solo para el administrador, que debe realizar el administrador de Kubernetes o de almacenamiento.

Habilita la autenticación basada en certificados

Los backends, tanto nuevos como existentes, pueden usar un certificado y comunicarse con el backend de ONTAP. Se requieren tres parámetros en la definición del 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 usas una CA de confianza, tienes que proporcionar este parámetro. Esto se puede ignorar si no usas una CA de confianza.

Un flujo de trabajo típico implica los siguientes pasos.

Pasos

1. Genera un certificado y una clave de cliente. Al generarlos, asigna el nombre común (CN) al usuario de ONTAP con el que te vas a autenticar.

```
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. Agrega un certificado de CA de confianza al clúster de ONTAP. Esto puede que ya lo haya gestionado el administrador de almacenamiento. Ignora esto si no se usa 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. Instala el certificado y la clave del cliente (del 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
```

NOTA

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

4. Confirma que el rol de inicio de sesión de seguridad de ONTAP admite `cert` el 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. Prueba la autenticación usando el certificado generado. Reemplaza <ONTAP Management LIF> y <vserver name> con la IP de la LIF de administración y el nombre de la 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. Codifica el certificado, la clave y el certificado de CA confiable con Base64.

```
base64 -w 0 k8serv.pem >> cert_base64
base64 -w 0 k8serv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Crea un backend usando los valores obtenidos en el 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 |
+-----+-----+-----+
+-----+-----+

```

Actualiza los métodos de autenticación o rota las credenciales

Puedes actualizar un backend existente para usar un método de autenticación diferente o para rotar sus credenciales. Esto funciona en ambos sentidos: los backends que usan nombre de usuario y contraseña pueden actualizarse para usar certificados; los backends que utilizan certificados pueden actualizarse para usar nombre de usuario y contraseña. Para hacer esto, debes eliminar el método de autenticación existente y agregar el nuevo método de autenticación. Luego usa el archivo `backend.json` actualizado que contiene los parámetros necesarios para ejecutar `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 |
+-----+-----+-----+
+-----+-----+

```

NOTA

Al rotar contraseñas, el administrador de almacenamiento debe primero actualizar la

contraseña del usuario en ONTAP. Luego, se realiza una actualización del backend. Al rotar certificados, se pueden agregar varios certificados al usuario. Después, el backend se actualiza para usar el nuevo certificado, y luego se puede eliminar el certificado antiguo del clúster de ONTAP.

Actualizar un backend no interrumpe el acceso a los volúmenes ya creados ni afecta las conexiones de volumen realizadas después. Una actualización correcta del backend indica que Trident puede comunicarse con el backend de ONTAP y gestionar futuras operaciones de volumen.

Crear rol ONTAP personalizado para Trident

Puedes crear un rol de clúster de ONTAP con privilegios mínimos para que no tengas que usar el rol de admin de ONTAP para realizar operaciones en Trident. Cuando incluyes el nombre de usuario en una configuración de backend de Trident, Trident usa el rol de clúster de ONTAP que creaste para realizar las operaciones.

Consulta "[Generador de roles personalizados de Trident](#)" para más información sobre cómo crear roles personalizados de Trident.

Usando ONTAP CLI

1. Crea un nuevo rol usando el siguiente comando:

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

2. Crea un nombre de usuario para el usuario 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. Asigna el rol al usuario:

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

Usando System Manager

Realiza los siguientes pasos en ONTAP System Manager:

1. **Crea un rol personalizado:**

- a. Para crear un rol personalizado a nivel de cluster, selecciona **Cluster > Settings**.

(O) Para crear un rol personalizado a nivel de SVM, selecciona **Storage > Storage VMs > required SVM > Settings > Users and Roles**.

- b. Selecciona el icono de flecha (→) junto a **Users and Roles**.
- c. Selecciona **+Add** en **Roles**.
- d. Define las reglas para el rol y haz clic en **Guardar**.

2. **Asigna el rol al usuario Trident:** + Realiza los siguientes pasos en la página **Usuarios y roles**:

- a. Selecciona el icono Add + en **Usuarios**.

- b. Selecciona el nombre de usuario requerido y elige un rol en el menú desplegable de **Role**.
- c. Haz clic en **Guardar**.

Consulta las siguientes páginas para obtener más información:

- ["Roles personalizados para la administración de ONTAP" o "Define roles personalizados"](#)
- ["Trabaja con roles y usuarios"](#)

Autentica conexiones con CHAP bidireccional

Trident puede autenticar sesiones iSCSI con CHAP bidireccional para los `ontap-san` y `ontap-san-economy` controladores. Esto requiere habilitar la opción `useCHAP` en la definición de tu 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 desde el archivo del backend. NetApp recomienda usar CHAP bidireccional para autenticar conexiones. Mira 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
```

ADVERTENCIA

El `useCHAP` parámetro es una opción booleana que solo se puede configurar una vez. Se establece en falso de forma predeterminada. Después de que lo configuras en verdadero, ya no puedes ponerlo en falso.

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

Cómo funciona

Al establecer `useCHAP` en `true`, el administrador de almacenamiento le indica a Trident que configure CHAP en el backend de almacenamiento. Esto incluye lo siguiente:

- Configurar CHAP en la SVM:
 - Si el tipo de seguridad del iniciador predeterminado de la SVM es ninguno (establecido de manera predeterminada) y no hay LUN preexistentes en el volumen, Trident establecerá el tipo de seguridad predeterminado en CHAP y procederá a configurar el nombre de usuario y los secretos del iniciador y

del destino CHAP.

- Si la SVM contiene LUNs, Trident no habilitará CHAP en la SVM. Esto garantiza que el acceso a los LUNs que ya están presentes en la SVM no esté restringido.
- Configurar el iniciador CHAP y el nombre de usuario y los secretos del destino; estas opciones deben especificarse en la configuración del backend (como se muestra arriba).

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

Rotar credenciales y actualizar backends

Puedes actualizar las credenciales CHAP actualizando los parámetros CHAP en el archivo `backend.json`. Esto requerirá actualizar los secretos CHAP y usar el comando `tridentctl update` para reflejar estos cambios.

ADVERTENCIA

Al actualizar los secretos CHAP de un backend, debes usar `tridentctl` para actualizar el backend. No actualices las credenciales en el clúster de almacenamiento usando la CLI de ONTAP o el System Manager de ONTAP, ya que Trident no podrá detectar 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 Trident actualiza las credenciales en la SVM. Las nuevas conexiones usan las credenciales actualizadas y las conexiones existentes siguen activas. Desconectar y volver a conectar los PV antiguos hará que usen las credenciales actualizadas.

Opciones de configuración y ejemplos de ONTAP SAN

Crea y usa los controladores SAN de ONTAP con tu instalación de Trident. Esta sección ofrece ejemplos de configuración de backend y detalles para mapear backends 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 el uso de ciertos parámetros, como se indica. ["Conoce más sobre las diferencias entre los sistemas ASA r2 y otros sistemas ONTAP"](#). En la configuración del backend de Trident, no necesitas especificar que tu sistema es ASA r2. Cuando seleccionas `ontap-san` como `storageDriverName`, Trident detecta automáticamente el sistema ASA r2 u otros sistemas ONTAP. Algunos parámetros de configuración del backend no aplican a los sistemas ASA r2, como se indica en la tabla a continuación.

NOTA

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

Opciones de configuración del backend

A partir de la versión 26.06, puedes activar la asignación equilibrada de ONTAP para que ONTAP seleccione el agregado para los nuevos volúmenes. Consulta ["Utiliza la distribución equilibrada con los backends de ONTAP"](#) para conocer los requisitos y ver ejemplos.

Consulta la siguiente tabla para ver las opciones de configuración del backend:

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento. No se puede modificar después de la creación. Para actualizar este parámetro, debes crear un nuevo backend.	<code>ontap-san</code> o <code>ontap-san-economy</code>
<code>backendName</code>	Nombre personalizado o el backend de almacenamiento	Nombre del driver + "_" + <code>dataLIF</code>

Parámetro	Descripción	Predeterminado
managementLIF	<p>Dirección IP de un LIF de gestión de clúster o SVM.</p> <p>Se puede especificar un nombre de dominio completo (FQDN).</p> <p>Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p> <p>Para una conmutación de sitios sin interrupciones de MetroCluster, consulta el Ejemplo de MetroCluster.</p> <div> <p>NOTA</p> <p>Si usas credenciales "vsadmin", managementLIF debe ser el de la SVM; si usas credenciales "admin", managementLIF debe ser el del clúster.</p> </div>	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	<p>Dirección IP del LIF de protocolo. Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. No especifiques para iSCSI. Trident usa "Mapa LUN selectivo de ONTAP" para descubrir los LIF de iSCSI necesarios para establecer una sesión multipath. Se genera una advertencia si dataLIF se define explícitamente. Omite para MetroCluster. Consulta el Ejemplo de MetroCluster.</p>	Derivado por la SVM
svm	Máquina virtual de almacenamiento a usar Omitir para MetroCluster. Consulta el Ejemplo de MetroCluster .	Se deriva si se especifica un SVM managementLIF
useCHAP	<p>Usa CHAP para autenticar iSCSI para los controladores ONTAP SAN [parámetro booleano]. Establécelo en true para que Trident configure y use CHAP bidireccional como la autenticación predeterminada para el SVM dado en el backend. Consulta "Prepárate para configurar el backend con controladores SAN de ONTAP" para obtener más detalles. No es compatible con FCP o NVMe/TCP.</p>	false
chapInitiatorSecret	Secreto del iniciador de CHAP. Requerido si useCHAP=true	""
labels	Conjunto de etiquetas arbitrarias con formato JSON para aplicar en volúmenes	""

Parámetro	Descripción	Predeterminado
chapTargetInitiatorSecret	Secreto del iniciador de destino CHAP. Requerido si useCHAP=true	""
chapUsername	Nombre de usuario de entrada. Requerido si useCHAP=true	""
chapTargetUsername	Nombre de usuario de destino. Requerido si useCHAP=true	""
clientCertificate	Valor codificado en Base64 del certificado del cliente. Usado para auth basada en certificados	""
clientPrivateKey	Valor codificado en Base64 de la clave privada del cliente. Usado para auth basada en certificados	""
trustedCACertificate	Valor codificado en Base64 del certificado de CA de confianza. Opcional. Se usa para la autenticación basada en certificados.	""
username	Nombre de usuario necesario para comunicarte con el clúster ONTAP. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, mira "Autentica Trident en un SVM backend usando credenciales de Active Directory" .	""
password	Contraseña necesaria para comunicarte con el clúster ONTAP. Se utiliza para la autenticación basada en credenciales. Para la autenticación de Active Directory, mira "Autentica Trident en un SVM backend usando credenciales de Active Directory" .	""
svm	Máquina virtual de almacenamiento que vas a usar	Se deriva si se especifica un SVM managementLIF
storagePrefix	Prefijo que se utiliza al aprovisionar nuevos volúmenes en el SVM. No se puede modificar posteriormente. Para actualizar este parámetro, necesitas crear un nuevo backend.	trident

Parámetro	Descripción	Predeterminado
aggregate	<p>Agregado para el aprovisionamiento (opcional; si se configura, debe asignarse al SVM). Para el <code>ontap-nas-flexgroup</code> driver, esta opción se ignora. Si no se asigna, se puede utilizar cualquiera de los agregados disponibles para aprovisionar un volumen FlexGroup.</p> <p>NOTA</p> <p>Cuando se actualiza el agregado en SVM, se actualiza automáticamente en Trident mediante la consulta a SVM sin necesidad de reiniciar el controlador de Trident. Cuando has configurado un agregado específico en Trident para aprovisionar volúmenes, si el agregado se renombra o se traslada fuera del SVM, el backend pasa al estado de fallo en Trident mientras consulta el agregado de SVM. Debes cambiar el agregado por uno que esté presente en el SVM o eliminarlo por completo para que el backend vuelva a estar en línea.</p> <p>No especificar para sistemas ASA r2.</p> <p>No especifiques cuándo <code>useBalancedPlacement</code> está configurado como <code>true</code>.</p>	""
useBalancedPlacement	<p>Delegar la selección de agregados para nuevos volúmenes a ONTAP [booleano]. Requiere ONTAP 9.19.1 o posterior y <code>useREST</code> configurado en <code>true</code>. No se puede combinar con <code>aggregate</code>.</p> <p>Consulta "Utiliza la distribución equilibrada con los backends de ONTAP" para conocer los requisitos y ver ejemplos.</p>	false
limitAggregateUsage	<p>Falla el aprovisionamiento si el uso es superior a este porcentaje. Si estás usando un backend de Amazon FSx para NetApp ONTAP, no especifiques <code>limitAggregateUsage</code>. Los <code>fsxadmin</code> y <code>vsadmin</code> no tienen los permisos necesarios para recuperar el uso agregado y limitarlo usando Trident. No especificar para sistemas ASA r2.</p>	"" (no aplicado por defecto)
limitVolumeSize	<p>Falla el aprovisionamiento si el tamaño del volumen solicitado supera este valor. También restringe el tamaño máximo de los volúmenes que gestiona para LUNs.</p>	"" (no aplicado por defecto)
lunsPerFlexvol	<p>Máximo de LUNs por FlexVol, debe estar en el rango [50, 200]</p>	100

Parámetro	Descripción	Predeterminado
debugTraceFlags	Indicadores de depuración para utilizar cuando estés solucionando problemas. Por ejemplo, {"api":false, "method":true} no lo uses a menos que estés solucionando problemas y necesites un volcado detallado del registro.	null
useREST	<p>Parámetro booleano para usar las ONTAP REST APIs.</p> <div> <pre>`useREST` Cuando se establece en `true`, Trident usa las ONTAP REST APIs para comunicarse con el backend; cuando se establece en `false`, Trident usa 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 la aplicación `ontapi`. Esto se cumple con los roles predefinidos `vsadmin` y `cluster-admin`. A partir de la versión Trident 24.06 y ONTAP 9.15.1 o posteriores, `useREST` está configurado en `true` de forma predeterminada; cambia `useREST` a `false` para usar llamadas ONTAPI (ZAPI).</pre> </div> <p>useREST está totalmente calificado para NVMe/TCP.</p> <div> <p>NOTA</p> <p>NVMe solo es compatible con las API REST de ONTAP y no es compatible con ONTAPI (ZAPI).</p> <p>Si se especifica, siempre configúralo en true para sistemas ASA r2.</p> </div>	true para ONTAP 9.15.1 o posterior, de lo contrario false.
sanType	Usa para seleccionar iscsi para iSCSI, nvme para NVMe/TCP o fcp para SCSI sobre Fibre Channel (FC).	iscsi si está en blanco

Parámetro	Descripción	Predeterminado
formatOptions	Utiliza formatOptions para especificar argumentos de línea de comandos para el comando mkfs, que se aplica cada vez que se formatea un volumen. Esto te permite formatear el volumen según tus preferencias. Asegúrate de especificar formatOptions de forma similar a las opciones del comando mkfs, excluyendo la ruta del dispositivo. Ejemplo: "-E nodiscard" Compatible con ontap-san y ontap-san-economy controladores con el protocolo iSCSI. Además, compatible con sistemas ASA r2 cuando usas los protocolos iSCSI y NVMe/TCP.	
limitVolumePoolSize	Tamaño máximo solicitable de FlexVol al utilizar LUNs en el backend de ontap-san-economy.	"" (no aplicado por defecto)
denyNewVolumePools	Restringe ontap-san-economy a los backends crear nuevos volúmenes FlexVol para contener sus LUN. Solo se utilizan los FlexVol ya existentes para el aprovisionamiento de nuevos PV.	

Recomendaciones para usar formatOptions

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

- **-E nodiscard (ext3, ext4):** No intentes descartar bloques al momento de ejecutar mkfs (descartar bloques inicialmente es útil en dispositivos de estado sólido y almacenamiento disperso o Thin-Provisioning). Esto reemplaza la opción obsoleta "-K" y es aplicable a los sistemas de archivos ext3 y ext4.
- **-K (xfs):** No intentes descartar bloques durante la ejecución de mkfs. Esta opción es aplicable al sistema de archivos xfs.

Autentica Trident en un SVM backend usando credenciales de Active Directory

Puedes configurar Trident para que se autentique en una SVM de backend usando credenciales de Active Directory (AD). Antes de que una cuenta de AD pueda acceder a la SVM, tienes que configurar el acceso del controlador de dominio de AD al clúster o a la SVM. Para la administración del clúster con una cuenta de AD, tienes que crear un domain tunnel. Consulta ["Configura el acceso al controlador de dominio de Active Directory en ONTAP"](#) para obtener más detalles.

pasos

1. Configura los ajustes de Domain Name System (DNS) para un SVM de backend:

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

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

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

3. Usa 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, establece los parámetros `username` y `password` en el nombre de usuario o grupo de AD y la contraseña, respectivamente.

Opciones de configuración de backend para aprovisionar volúmenes

Puedes controlar el aprovisionamiento predeterminado usando estas opciones en la `defaults` sección de la configuración. Por ejemplo, mira los ejemplos de configuración abajo.

Parámetro	Descripción	Predeterminado
<code>spaceAllocation</code>	Asignación de espacio para LUNs	"verdadero" Si se especifica, configúralo en <code>true</code> para sistemas ASA r2.
<code>spaceReserve</code>	Modo de reserva de espacio; "ninguno" (thin) o "volumen" (thick). Configúralo en <code>none</code> para sistemas ASA r2.	"none"
<code>snapshotPolicy</code>	Política de SnapVault que se va a usar. Establece en <code>none</code> para sistemas ASA r2.	"none"
<code>qosPolicy</code>	Grupo de políticas de QoS para asignar a los volúmenes creados. Elige uno de <code>qosPolicy</code> o <code>adaptiveQosPolicy</code> por pool de almacenamiento/backend. Usar grupos de políticas de QoS con Trident requiere ONTAP 9.8 o una versión posterior. Deberías usar un grupo de políticas de QoS no compartido y asegurarte de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de QoS compartido impone el límite máximo para el rendimiento total de todas las cargas de trabajo.	""
<code>adaptiveQosPolicy</code>	Grupo de políticas de QoS adaptativo para asignar a los volúmenes creados. Elige uno de <code>qosPolicy</code> o <code>adaptiveQosPolicy</code> por cada pool de almacenamiento/backend	""
<code>snapshotReserve</code>	Porcentaje de volumen reservado para instantáneas. No especificar para sistemas ASA r2.	"0" si <code>snapshotPolicy</code> es "none", de lo contrario ""
<code>splitOnClone</code>	Divide un clon de su padre al momento de su creación	"false"
<code>encryption</code>	Activa NetApp Volume Encryption (NVE) en el nuevo volumen; el valor predeterminado es <code>false</code> . NVE debe estar licenciado y habilitado en el clúster para usar esta opción. Si NAE está habilitado en el backend, cualquier volumen aprovisionado en Trident tendrá NAE habilitado. Para más información, consulta: "Cómo funciona Trident con NVE y NAE" .	"falso" Si se especifica, configúralo en <code>true</code> para sistemas ASA r2.

Parámetro	Descripción	Predeterminado
luksEncryption	Activa el cifrado LUKS. Consulta "Usa Linux Unified Key Setup (LUKS)" .	"" Establéclo en false para sistemas ASA r2.
tieringPolicy	Política de niveles para usar "none" No especificar para sistemas ASA r2.	
nameTemplate	Plantilla para crear nombres de volúmenes personalizados.	""

Ejemplos de aprovisionamiento de volumen

Aquí tienes un ejemplo con 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'
```

NOTA

Para todos los volúmenes creados usando el `ontap-san` driver, Trident añade un 10 % extra de capacidad a la FlexVol para acomodar los metadatos del LUN. El LUN se aprovisiona con el tamaño exacto que el usuario solicita en el PVC. Trident añade un 10 % a la FlexVol (se muestra como tamaño disponible en ONTAP). Ahora los usuarios obtienen la cantidad de capacidad utilizable que solicitaron. Este cambio también evita que los LUN se vuelvan de solo lectura a menos que se utilice por completo el espacio disponible. Esto no se aplica a `ontap-san-economy`.

Para los backends 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 % adicional que Trident añade a la FlexVol para alojar los metadatos del LUN. Para `snapshotReserve = 5 %`, y una solicitud de PVC de 5 GiB, el tamaño total del volumen es 5.79 GiB y el tamaño disponible es 5.5 GiB. El `volume show` 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.

Actualmente, cambiar el tamaño es la única manera de usar el nuevo cálculo para un volumen existente.

Ejemplos de configuración mínima

Los siguientes ejemplos muestran configuraciones básicas que dejan la mayoría de los parámetros en sus valores predeterminados. Esta es la forma más fácil de definir un backend.

NOTA

Si estás usando Amazon FSx en NetApp ONTAP con Trident, NetApp recomienda que especifiques nombres DNS para las LIFs en vez de direcciones IP.

▼ Ejemplo de ONTAP SAN

Esta es una configuración básica usando el `ontap-san` driver.

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

▼ Ejemplo de MetroCluster

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

Para una conmutación de sitios y reversión sin problemas, especifica el SVM usando `managementLIF` y omite los parámetros `svm`. Por ejemplo:

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

▼ Ejemplo de ONTAP SAN economy

```
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 usas una CA confiable) se completan en `backend.json` y toman los valores codificados en base64 del certificado del cliente, la clave privada y el certificado de CA confiable, 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` configurado en `true`.

Ejemplo de ONTAP SAN CHAP

```
---
version: 1
storageDriverName: ontap-san
```

```

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

```

Ejemplo de ONTAP SAN economy CHAP

```

---
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 distribución equilibrada

Este ejemplo habilita la distribución equilibrada de ONTAP para que ONTAP seleccione el agregado para los nuevos volúmenes. La distribución equilibrada requiere ONTAP 9.19.1 o una versión posterior. Consulta ["Utiliza la distribución equilibrada con los backends de ONTAP"](#) para obtener más detalles.

```

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

```

▼ Ejemplo de NVMe/TCP

Debes tener una SVM configurada con NVMe en tu backend de ONTAP. Esta es una configuración básica

de backend para NVMe/TCP.

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

▼ Ejemplo de SCSI sobre FC (FCP)

Debes tener una SVM configurada con FC en tu backend de ONTAP. Esta es una configuración básica de backend para FC.

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

▼ 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}}"
```

▼ formatOptions ejemplo 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 backends con pools virtuales

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

Trident establece las etiquetas de aprovisionamiento en el campo "Comentarios". Los comentarios se establecen en el volumen FlexVol. Trident copia todas las etiquetas presentes en un pool virtual al 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` valores, y algunos pools anulan los valores predeterminados.

▼ Ejemplo de ONTAP SAN

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

```

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

```

▼ Ejemplo de ONTAP SAN economy

```

---
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"

```

Asigna backends a StorageClasses

Las siguientes definiciones de StorageClass hacen referencia a [Ejemplos de backends con pools virtuales](#). Usando el campo `parameters.selector`, cada StorageClass indica qué grupos virtuales se pueden usar para alojar un volumen. El volumen ahora tiene los aspectos definidos en el grupo virtual elegido.

- El `protection-gold` StorageClass se asigna al primer grupo virtual en el `ontap-san` backend. Este es el único grupo 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"

```

- El `protection-not-gold` StorageClass se asigna al segundo y tercer grupo virtual en `ontap-san` backend. Estos son los únicos grupos que ofrecen un nivel de protección distinto a gold.

```

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

```

- El `app-mysqldb` StorageClass se asigna al tercer grupo virtual en `ontap-san-economy` backend. Este es el único grupo que ofrece configuración de grupo de almacenamiento para la app tipo `mysqldb`.

```

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

```

- El protection-silver-creditpoints-20k StorageClass se asigna al segundo grupo virtual en ontap-san backend. Este es el único grupo que ofrece protección de nivel silver y 20 000 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"

```

- El creditpoints-5k StorageClass se asigna al tercer grupo virtual en el backend ontap-san y al cuarto grupo virtual en el backend ontap-san-economy. Estas son las únicas ofertas de grupos 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"

```

- El my-test-app-sc StorageClass se asigna al grupo virtual testAPP en el controlador ontap-san con sanType: nvme. Este es el único grupo que ofrece 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 decide qué grupo virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

Controladores NAS de ONTAP

Descripción general del controlador NAS de ONTAP

Conoce cómo configurar un backend de ONTAP con los controladores NAS de ONTAP y Cloud Volumes ONTAP.

Detalles del controlador NAS de ONTAP

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

Controlador	Protocolo	volumeMode	Modos de acceso admitidos	Sistemas de archivos compatibles
ontap-nas	NFS SMB	Sistema de archivos	RWO, ROX, RWX, RWOP	"", nfs, smb
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

ADVERTENCIA

- Usa `ontap-san-economy` solo si esperas que el recuento de uso de volúmenes persistentes sea mayor que "[límites de volúmenes compatibles de ONTAP](#)".
- Usa `ontap-nas-economy` solo si se espera que el recuento de uso de volúmenes persistentes sea mayor que "[límites de volúmenes compatibles de ONTAP](#)" y no se puede usar el controlador `ontap-san-economy`.
- No uses `ontap-nas-economy` si crees que vas a necesitar protección de datos, recuperación ante desastres o movilidad.
- NetApp no recomienda usar FlexVol autogrow en todos los controladores ONTAP, excepto `ontap-san`. Como solución alternativa, Trident admite el uso de snapshot reserve y escala los volúmenes FlexVol en consecuencia.

Permisos de usuario

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

Para las implementaciones de Amazon FSx for NetApp ONTAP, Trident espera ejecutarse como administrador

de ONTAP o SVM, usando el usuario del clúster `fsxadmin` o un `vsadmin` usuario de SVM, o un usuario con un nombre diferente que tenga el mismo rol. El `fsxadmin` usuario es un reemplazo limitado para el usuario administrador del clúster.

NOTA

Si usas el parámetro `limitAggregateUsage`, se requieren permisos de administrador de clúster. Cuando usas Amazon FSx for NetApp ONTAP con Trident, el parámetro `limitAggregateUsage` no funcionará con las cuentas de usuario `vsadmin` y `fsxadmin`. La operación de configuración fallará si especificas este parámetro.

Aunque es posible crear un rol más restrictivo dentro de ONTAP que un controlador Trident pueda usar, no lo recomendamos. La mayoría de las nuevas versiones de Trident llamarán a APIs adicionales que habría que tener en cuenta, lo que hace que las actualizaciones sean difíciles y propensas a errores.

Prepárate para configurar un backend con controladores ONTAP NAS

Entiende los requisitos, las opciones de autenticación y las políticas de exportación para configurar un backend ONTAP con drivers ONTAP NAS. A partir de la versión 25.10, NetApp Trident es compatible con "[Sistema de almacenamiento NetApp AFX](#)". NetApp AFX storage systems difieren de otros sistemas ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento. En la configuración del backend de Trident, no necesitas especificar que tu sistema es AFX. Cuando seleccionas `ontap-nas` como `storageDriverName`, Trident detecta automáticamente los sistemas AFX.

NOTA

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

Requisitos

- Para todos los backends de ONTAP, Trident requiere que al menos un agregado esté asignado a la SVM.
- Puedes ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, podrías configurar una clase Gold que use el `ontap-nas` controlador y una clase Bronze que use el `ontap-nas-economy` otro.
- Todos tus nodos worker de Kubernetes deben tener instaladas las herramientas NFS adecuadas. Consulta ["aquí"](#) para obtener más detalles.
- Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows. Consulta [Prepárate para aprovisionar volúmenes SMB](#) para obtener más detalles.

Autentica el backend de ONTAP

Trident ofrece dos modos de autenticación para un backend ONTAP.

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

Puedes actualizar los backends existentes para pasar de métodos basados en credenciales a métodos

basados en certificados y viceversa. Sin embargo, solo se admite un método de autenticación a la vez. Para cambiar a otro método de autenticación, debes eliminar el método existente de la configuración del backend.

ADVERTENCIA

Si intentas proporcionar **tanto credenciales como certificados**, la creación del backend fallará con un error que indica que se proporcionó más de un método de autenticación en el archivo de configuración.

Habilita la autenticación basada en credenciales

Trident requiere las credenciales de un administrador con ámbito de SVM o de clúster para comunicarse con el backend de ONTAP. Se recomienda usar roles estándar predefinidos como `admin` o `vsadmin`. Esto garantiza la compatibilidad futura con versiones de ONTAP que podrían exponer APIs de funciones para futuras versiones de Trident. Se puede crear y usar un rol personalizado de inicio de sesión de seguridad con Trident, pero no se recomienda.

Un ejemplo de definición de backend se verá así:

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"
  }
}
```

Ten en cuenta que la definición del backend es el único lugar donde se almacenan las credenciales en texto plano. Después de crear el backend, los nombres de usuario y contraseñas se codifican con Base64 y se guardan como secretos de Kubernetes. La creación o actualización de un backend es el único paso que requiere conocimiento de las credenciales. Así que es una operación solo para el administrador, que debe

realizar el administrador de Kubernetes o de almacenamiento.

Habilita la autenticación basada en certificados

Los backends, tanto nuevos como existentes, pueden usar un certificado y comunicarse con el backend de ONTAP. Se requieren tres parámetros en la definición del 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 usas una CA de confianza, tienes que proporcionar este parámetro. Esto se puede ignorar si no usas una CA de confianza.

Un flujo de trabajo típico implica los siguientes pasos.

Pasos

1. Genera un certificado y una clave de cliente. Al generarlos, asigna el nombre común (CN) al usuario de ONTAP con el que te vas a autenticar.

```
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. Agrega un certificado de CA de confianza al clúster de ONTAP. Esto puede que ya lo haya gestionado el administrador de almacenamiento. Ignora esto si no se usa 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. Instala el certificado y la clave del cliente (del 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. Confirma que el rol de inicio de sesión de seguridad de ONTAP admite `cert` el 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. Prueba la autenticación usando el certificado generado. Reemplaza `<ONTAP Management LIF>` y `<vserver name>` con la IP de la LIF de administración y el nombre de la SVM. Debes asegurarte de que el

LIF tenga su política de servicio configurada 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. Codifica el certificado, la clave y el certificado de CA confiable con Base64.

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

7. Crea un backend usando los valores obtenidos en el 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           |  
STATE | VOLUMES |  
+-----+-----+-----+-----+  
+-----+-----+  
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |  
online |      9 |  
+-----+-----+-----+-----+  
+-----+-----+
```

Actualiza los métodos de autenticación o rota las credenciales

Puedes actualizar un backend existente para usar un método de autenticación diferente o para rotar sus credenciales. Esto funciona en ambos sentidos: los backends que usan nombre de usuario y contraseña pueden actualizarse para usar certificados; los backends que utilizan certificados pueden actualizarse para usar nombre de usuario y contraseña. Para hacer esto, debes eliminar el método de autenticación existente y agregar el nuevo método de autenticación. Luego usa el archivo backend.json actualizado que contiene los parámetros necesarios para ejecutar `tridentctl update backend`.

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

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

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

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

```

NOTA

Al rotar contraseñas, el administrador de almacenamiento debe primero actualizar la contraseña del usuario en ONTAP. Luego, se realiza una actualización del backend. Al rotar certificados, se pueden agregar varios certificados al usuario. Después, el backend se actualiza para usar el nuevo certificado, y luego se puede eliminar el certificado antiguo del clúster de ONTAP.

Actualizar un backend no interrumpe el acceso a los volúmenes ya creados ni afecta las conexiones de volumen realizadas después. Una actualización correcta del backend indica que Trident puede comunicarse

con el backend de ONTAP y gestionar futuras operaciones de volumen.

Crear rol ONTAP personalizado para Trident

Puedes crear un rol de clúster de ONTAP con privilegios mínimos para que no tengas que usar el rol de admin de ONTAP para realizar operaciones en Trident. Cuando incluyes el nombre de usuario en una configuración de backend de Trident, Trident usa el rol de clúster de ONTAP que creaste para realizar las operaciones.

Consulta ["Generador de roles personalizados de Trident"](#) para más información sobre cómo crear roles personalizados de Trident.

Usando ONTAP CLI

1. Crea un nuevo rol usando el siguiente comando:

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

2. Crea un nombre de usuario para el usuario 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. Asigna el rol al usuario:

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

Usando System Manager

Realiza los siguientes pasos en ONTAP System Manager:

1. **Crea un rol personalizado:**

- a. Para crear un rol personalizado a nivel de cluster, selecciona **Cluster > Settings**.

(O) Para crear un rol personalizado a nivel de SVM, selecciona **Storage > Storage VMs > required svm > Settings > Users and Roles**.

- b. Selecciona el icono de flecha (→) junto a **Users and Roles**.
- c. Selecciona **+Add** en **Roles**.
- d. Define las reglas para el rol y haz clic en **Guardar**.

2. **Asigna el rol al usuario Trident:** + Realiza los siguientes pasos en la página **Usuarios y roles**:

- a. Selecciona el icono Add + en **Usuarios**.
- b. Selecciona el nombre de usuario requerido y elige un rol en el menú desplegable de **Role**.
- c. Haz clic en **Guardar**.

Consulta las siguientes páginas para obtener más información:

- ["Roles personalizados para la administración de ONTAP"](#) o ["Define roles personalizados"](#)

- ["Trabaja con roles y usuarios"](#)

Gestiona las políticas de exportación de NFS

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

Trident ofrece dos opciones cuando trabajas con políticas de exportación:

- Trident puede gestionar dinámicamente la política de exportación por sí mismo; en este modo de funcionamiento, el administrador de almacenamiento especifica una lista de bloques CIDR que representan direcciones IP admisibles. Trident añade automáticamente a la política de exportación las direcciones IP de nodo aplicables que estén dentro de estos rangos en el momento de la publicación. Como alternativa, cuando no se especifican CIDR, se añadirán a la política de exportación todas las direcciones IP de unidifusión de ámbito global que se encuentren en el nodo al que se está publicando el volumen.
- Los administradores de almacenamiento pueden crear una política de exportación y agregar reglas manualmente. Trident utiliza la política de exportación predeterminada a menos que se especifique un nombre de política de exportación diferente en la configuración.

Gestiona dinámicamente las políticas de exportación

Trident ofrece la capacidad de gestionar dinámicamente las políticas de exportación para los backends de ONTAP. Esto le da al administrador de almacenamiento la posibilidad de especificar un espacio de direcciones permitido para las direcciones IP de los nodos de trabajo, en vez de definir reglas explícitas manualmente. Esto simplifica mucho la gestión de las políticas de exportación; las modificaciones en 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 trabajo que están montando volúmenes y tienen direcciones IP dentro del rango especificado, lo que permite una gestión automatizada y detallada.

NOTA

No uses Network Address Translation (NAT) cuando uses políticas de exportación dinámicas. Con NAT, el controlador de almacenamiento ve la dirección NAT del frontend y no la dirección IP real del host, así que se denegará el acceso cuando no se encuentre coincidencia en las reglas de exportación.

Ejemplo

Hay dos opciones de configuración que deben utilizarse. Aquí tienes 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
```

NOTA

Al usar esta función, debes asegurarte de que la unión raíz de tu SVM tenga una política de exportación previamente creada con una regla de exportación que permita el bloque CIDR del nodo (como la política de exportación predeterminada). Sigue siempre la práctica recomendada por NetApp de dedicar una SVM para Trident.

Aquí tienes una explicación de cómo funciona esta función usando el ejemplo de arriba:

- `autoExportPolicy` se establece en `true`. Esto indica que Trident crea una política de exportación para cada volumen provisionado con este backend para la `svm1` SVM y gestiona la adición y eliminación de reglas usando bloques de direcciones `autoExportCIDRs`. Hasta que un volumen se conecta a un nodo, el volumen utiliza una política de exportación vacía sin reglas para evitar el acceso no deseado a ese volumen. Cuando un volumen se publica en un nodo, Trident crea una política de exportación con el mismo nombre que el `qtree` subyacente que contiene la dirección IP del nodo dentro del bloque CIDR especificado. Estas direcciones IP también se añadirán a la política de exportación utilizada por el volumen principal FlexVol.
 - Por ejemplo:
 - UUID de backend `403b5326-8482-40db-96d0-d83fb3f4daec`
 - `autoExportPolicy` establecer en `true`
 - prefijo de almacenamiento `trident`
 - PVC UUID `a79bcf5f-7b6d-4a40-9876-e2551f159c1c`
 - El `qtree` llamado `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` crea una política de exportación para el FlexVol llamado `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 llamada `trident_empty` en la SVM. Las reglas para la política de exportación del FlexVol serán un superconjunto de cualquier regla contenida en las políticas de exportación del `qtree`. La política de exportación vacía se reutilizará para cualquier volumen que no esté adjunto.
- `autoExportCIDRs` contiene una lista de bloques de direcciones. Este campo es opcional y su valor predeterminado es `["0.0.0.0/0", "::/0"]`. Si no se define, Trident agrega todas las direcciones unicast de alcance global que se encuentran en los nodos de trabajo con publicaciones.

En este ejemplo, el espacio de direcciones `192.168.0.0/24` se proporciona. Esto indica que las direcciones IP de los nodos de Kubernetes que estén dentro de este rango de direcciones con publicaciones se añadirán 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 compara con los bloques de direcciones proporcionados en `autoExportCIDRs`. Al momento de publicar, después de filtrar las IP, Trident crea las reglas de la política de exportación para las direcciones IP de cliente del nodo al que está publicando.

Puedes actualizar `autoExportPolicy` y `autoExportCIDRs` para los backends después de crearlos. Puedes añadir nuevos CIDR para un backend que se gestiona automáticamente o eliminar los CIDR existentes. Ten cuidado al eliminar los CIDR para asegurarte de que no se interrumpan las conexiones existentes. También puedes elegir deshabilitar `autoExportPolicy` para un backend y volver a una política de exportación creada manualmente. Esto requerirá configurar el parámetro `exportPolicy` en la configuración del backend.

Después de que Trident crea o actualiza un backend, puedes verificar el backend usando `tridentctl` o el correspondiente `tridentbackend` CRD:

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

```

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

```

Al eliminar un nodo, Trident revisa todas las políticas de exportación para eliminar las reglas de acceso correspondientes al nodo. Al eliminar esta dirección IP de nodo de las políticas de exportación de los backends administrados, Trident evita montajes no autorizados, a menos que esta IP sea reutilizada por un nuevo nodo en el clúster.

Para los backends preexistentes, actualizar el backend con `tridentctl update backend` asegura que Trident gestione las políticas de exportación automáticamente. Esto crea dos nuevas políticas de exportación nombradas según el UUID y el nombre del qtree del backend cuando sean necesarias. Los volúmenes que están presentes en el backend usarán las nuevas políticas de exportación después de desmontarlos y volver a montarlos.

NOTA

Al eliminar un backend con políticas de exportación autogestionadas, se eliminará la política de exportación creada dinámicamente. Si el backend se vuelve a crear, se trata como un backend nuevo y resultará en la creación de una nueva política de exportación.

Si se actualiza la dirección IP de un nodo activo, debes reiniciar el pod de Trident en el nodo. Trident actualizará la política de exportación para los backends que administra para reflejar este cambio de IP.

Prepárate para aprovisionar volúmenes SMB

Con un poco de preparación adicional, puedes aprovisionar volúmenes SMB usando ``ontap-nas`drivers`.

ADVERTENCIA

Debes configurar tanto los protocolos NFS como SMB/CIFS en la SVM para crear un `ontap-nas-economy` volumen SMB para clústeres ONTAP locales. Si no configuras alguno de estos protocolos, la creación del volumen SMB fallará.

NOTA

`autoExportPolicy` no es compatible con volúmenes SMB.

Antes de empezar

Antes de que puedas aprovisionar volúmenes SMB, debes tener lo siguiente.

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

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

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

Pasos

1. Para ONTAP local, puedes crear opcionalmente un recurso compartido SMB o Trident puede crear uno para ti.

NOTA Se requieren recursos compartidos SMB para Amazon FSx for ONTAP.

Puedes crear los recursos compartidos de administrador de SMB de dos maneras: usando el complemento ["Microsoft Management Console"](#) Shared Folders o usando la CLI de ONTAP. Para crear los recursos compartidos de SMB usando la CLI de ONTAP:

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

El ``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. Crea un recurso compartido SMB asociado con la SVM especificada:

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

- c. Verifica que se creó el recurso compartido:

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

NOTA Consulta ["Crear un recurso compartido SMB"](#) para obtener detalles completos.

2. Al crear el backend, debes configurar lo siguiente para especificar los volúmenes SMB. Para todas las opciones de configuración del backend de FSx for ONTAP, consulta ["Opciones de configuración de FSx for ONTAP y ejemplos"](#).

Parámetro	Descripción	Ejemplo
smbShare	Puedes especificar uno de los siguientes: el nombre de un recurso compartido SMB creado usando Microsoft Management Console o la CLI de ONTAP, un nombre para permitir que Trident cree el recurso compartido SMB, o puedes dejar el parámetro en blanco para evitar el acceso compartido común a los volúmenes. Este parámetro es opcional para ONTAP local. Este parámetro es obligatorio para los backends de Amazon FSx for ONTAP y no puede estar en blanco.	smb-share
nasType	Debe establecerse en smb. Si es nulo, el valor predeterminado es <code>nfs</code> .	smb
securityStyle	Estilo de seguridad para nuevos volúmenes. Debe configurarse en ntfs o mixed para volúmenes SMB.	ntfs o mixed para volúmenes SMB
unixPermissions	Modo para nuevos volúmenes. Debe dejarse vacío para volúmenes SMB.	""

Habilita 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. Cuando SMB seguro está habilitado, puedes proporcionar acceso controlado a los recursos compartidos SMB para usuarios y grupos de usuarios de Active Directory (AD) usando listas de control de acceso (ACL).

Puntos para recordar

- No se admite la importación `ontap-nas-economy` de volúmenes.
- Solo se admiten clones de solo lectura para `ontap-nas-economy` volúmenes.
- Si Secure SMB está habilitado, Trident ignorará el recurso compartido SMB mencionado en el backend.
- Actualizar la anotación de PVC, la anotación de la storage class 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.
- Asegúrate de proporcionar usuarios de AD válidos al habilitar SMB seguro. Los usuarios no válidos no se añadirán a la ACL.
- Si proporcionas el mismo usuario de AD en el backend, la clase de almacenamiento y el PVC con diferentes permisos, la prioridad de permisos será: PVC, clase de almacenamiento y luego backend.
- SMB seguro es compatible para `ontap-nas` importaciones de volúmenes administrados y no aplica a importaciones de volúmenes no administrados.

Pasos

1. Especifica `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.

Agrega la `trident.netapp.io/smbShareAdUser` anotación a la clase de almacenamiento para habilitar SMB seguro sin fallar. 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. Puedes elegir una de las siguientes para `smbShareAdUserPermission`: `full_control`, `change` o `read`. El permiso predeterminado 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. Crea un 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 de configuración y ejemplos de ONTAP NAS

Crea y usa los controladores NAS de ONTAP con tu instalación de Trident. Esta sección ofrece ejemplos de configuración de backend y detalles para mapear backends a StorageClasses. A partir de la versión 25.10, NetApp Trident es compatible con ["NetApp sistemas de almacenamiento AFX"](#). NetApp AFX los sistemas de almacenamiento se diferencian de otros sistemas basados en ONTAP (ASA, AFF y FAS) en la implementación de su capa de almacenamiento.

NOTA

Sólo el `ontap-nas` controlador (con protocolo NFS) es compatible con NetApp AFX systems; el protocolo SMB no es compatible.

Opciones de configuración del backend

En la configuración del backend de Trident, no necesitas especificar que tu sistema es un sistema de almacenamiento AFX de NetApp. Cuando seleccionas `ontap-nas` como `storageDriverName`, Trident detecta automáticamente el sistema de almacenamiento AFX. Algunos parámetros de configuración del backend no aplican a los sistemas de almacenamiento AFX.

A partir de la versión 26.06, puedes activar la asignación equilibrada de ONTAP para que ONTAP seleccione el agregado para los nuevos volúmenes. La distribución equilibrada es obligatoria para los sistemas de almacenamiento AFX con ONTAP 9.19.1 o posterior. Consulta ["Utiliza la distribución equilibrada con los backends de ONTAP"](#) para conocer los requisitos y ver ejemplos.

La siguiente tabla muestra las opciones de configuración del backend:

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1

Parámetro	Descripción	Predeterminado
storageDriverName	<p>Nombre del controlador de almacenamiento.</p> <p>No se puede modificar después de la creación. Para actualizar este parámetro, debes crear un nuevo backend.</p> <div> <p>NOTA</p> <p>Para los sistemas AFX de NetApp, solo <code>ontap-nas</code> es compatible.</p> </div>	ontap-nas, ontap-nas-economy, o ontap-nas-flexgroup
backendName	Nombre personalizado o el backend de almacenamiento	Nombre del driver + "_" + dataLIF
managementLIF	<p>Dirección IP de un clúster o de una LIF de administración de SVM. Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>. Para una conmutación de sitios sin interrupciones de MetroCluster, consulta el Ejemplo de MetroCluster.</p>	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	<p>Dirección IP del LIF de protocolo. NetApp recomienda especificar <code>dataLIF</code>. Si no se proporciona, Trident obtiene los <code>dataLIF</code> del SVM. Puedes especificar un nombre de dominio completo (FQDN) para las operaciones de montaje NFS, lo que te permite crear un DNS de round-robin para balancear la carga entre varios <code>dataLIF</code>. Se puede cambiar después de la configuración inicial. Consulta . Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>. Omite para MetroCluster. Consulta el Ejemplo de MetroCluster.</p>	Dirección especificada o derivada de SVM, si no se especifica (no recomendado)
svm	Máquina virtual de almacenamiento a usar Omitir para MetroCluster. Consulta el Ejemplo de MetroCluster .	Se deriva si se especifica un SVM <code>managementLIF</code>
autoExportPolicy	Habilita la creación y actualización automática de políticas de exportación [Boolean]. Usando las opciones <code>autoExportPolicy</code> y <code>autoExportCIDRs</code> , Trident puede gestionar las políticas de exportación automáticamente.	false
autoExportCIDRs	Lista de CIDR para filtrar las direcciones IP de los nodos de Kubernetes cuando <code>autoExportPolicy</code> está habilitado. Usando las opciones <code>autoExportPolicy</code> y <code>autoExportCIDRs</code> , Trident puede gestionar las políticas de exportación automáticamente.	["0.0.0.0/0", ":::0"]

Parámetro	Descripción	Predeterminado
labels	Conjunto de etiquetas arbitrarias con formato JSON para aplicar en volúmenes	""
clientCertificate	Valor codificado en Base64 del certificado del cliente. Usado para auth basada en certificados	""
clientPrivateKey	Valor codificado en Base64 de la clave privada del cliente. Usado para auth basada en certificados	""
trustedCACertificate	Valor codificado en Base64 del certificado de CA de confianza. Opcional. Usado para auth basada en certificados	""
username	Nombre de usuario para conectarse al clúster/SVM. Se usa para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulta "Autentica Trident en un SVM backend usando credenciales de Active Directory" .	
password	Contraseña para conectarte al clúster/SVM. Se usa para la autenticación basada en credenciales. Para la autenticación de Active Directory, consulta "Autentica Trident en un SVM backend usando credenciales de Active Directory" .	
storagePrefix	<p>Prefijo que se utiliza al aprovisionar nuevos volúmenes en el SVM. No se puede actualizar después de configurarlo</p> <div> <p>NOTA</p> <p>Cuando usas ontap-nas-economy y un storagePrefix que tiene 24 caracteres o más, los qtrees no tienen el prefijo de almacenamiento incluido, aunque sí aparece en el nombre del volumen.</p> </div>	"Trident"

Parámetro	Descripción	Predeterminado
aggregate	<p>Agregado para el aprovisionamiento (opcional; si se configura, debe asignarse al SVM). Para el <code>ontap-nas-flexgroup</code> driver, esta opción se ignora. Si no se asigna, se puede utilizar cualquiera de los agregados disponibles para aprovisionar un volumen FlexGroup.</p> <div> <div>NOTA</div> <p>Cuando se actualiza el agregado en SVM, se actualiza automáticamente en Trident mediante la consulta a SVM sin necesidad de reiniciar el controlador de Trident. Cuando has configurado un agregado específico en Trident para aprovisionar volúmenes, si el agregado se renombra o se traslada fuera del SVM, el backend pasa al estado de fallo en Trident durante el sondeo del agregado de SVM. Debes cambiar el agregado por uno que esté presente en el SVM o eliminarlo por completo para que el backend vuelva a estar en línea.</p> <p>No especifiques para sistemas de almacenamiento AFX.</p> <p>No especifiques cuándo <code>useBalancedPlacement</code> está configurado como <code>true</code>.</p> </div>	""
useBalancedPlacement	<p>Delegar la selección de agregados para nuevos volúmenes a ONTAP [booleano]. Requiere ONTAP 9.19.1 o posterior y <code>useREST</code> configurado en <code>true</code>. No se puede combinar con <code>aggregate</code>.</p> <p>Consulta "Utiliza la distribución equilibrada con los backends de ONTAP" para conocer los requisitos y ver ejemplos.</p> <p>Si se especifica, configúralo siempre como <code>true</code> para los sistemas de almacenamiento AFX con ONTAP 9.19.1 o posterior.</p>	false; true para sistemas de almacenamiento AFX con ONTAP 9.19.1 o posterior
limitAggregateUsage	<p>Falla el aprovisionamiento si el uso es superior a este porcentaje. No aplica a Amazon FSx for ONTAP. No especifiques para sistemas de almacenamiento AFX.</p>	"" (no aplicado por defecto)

Parámetro	Descripción	Predeterminado
flexgroupAggregateList	<p>Lista de agregados para aprovisionamiento (opcional; si se configura, debe asignarse a la SVM). Todos los agregados asignados a la SVM se utilizan para aprovisionar un volumen FlexGroup. Compatible con el controlador de almacenamiento ontap-nas-flexgroup.</p> <p>NOTA Cuando se actualiza la lista de agregados en SVM, la lista se actualiza automáticamente en Trident mediante la consulta a SVM sin tener que reiniciar el controlador de Trident. Cuando has configurado una lista de agregados específica en Trident para aprovisionar volúmenes, si la lista de agregados se renombra o se mueve fuera de SVM, el backend pasa a estado de fallo en Trident mientras consulta el agregado de SVM. Debes cambiar la lista de agregados por una que esté presente en SVM o eliminarla por completo para que el backend vuelva a estar en línea.</p>	""
limitVolumeSize	Falla el aprovisionamiento si el tamaño del volumen solicitado supera este valor.	"" (no aplicado por defecto)
debugTraceFlags	Indicadores de depuración para utilizar cuando estés solucionando problemas. Por ejemplo, {"api":false, "method":true} no uses debugTraceFlags a menos que estés resolviendo problemas y necesites un volcado de registro detallado.	null
nasType	Configura la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o <code>null</code> . Si lo configuras en <code>null</code> , se usarán volúmenes NFS por defecto. Si se especifica, siempre se establece en <code>nfs</code> para sistemas de almacenamiento AFX.	<code>nfs</code>
nfsMountOptions	Lista separada por comas de opciones de montaje NFS. Las opciones de montaje para los volúmenes persistentes de Kubernetes normalmente se especifican en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident recurre a las opciones de montaje especificadas en el archivo de configuración del backend de almacenamiento. Si no se especifican opciones de montaje ni en la clase de almacenamiento ni en el archivo de configuración, Trident no establece ninguna opción de montaje en un volumen persistente asociado.	""

Parámetro	Descripción	Predeterminado
qtreesPerFlexvol	Máximo de Qtrees por FlexVol, debe estar en el rango [50, 300]	"200"
smbShare	Puedes especificar uno de los siguientes: el nombre de un recurso compartido SMB creado usando Microsoft Management Console o la CLI de ONTAP, un nombre para permitir que Trident cree el recurso compartido SMB, o puedes dejar el parámetro en blanco para evitar el acceso compartido común a los volúmenes. Este parámetro es opcional para ONTAP local. Este parámetro es obligatorio para los backends de Amazon FSx for ONTAP y no puede estar en blanco.	smb-share
useREST	Parámetro booleano para usar las ONTAP REST APIs. <code>useREST</code> Cuando se establece en <code>true</code> , Trident usa las ONTAP REST APIs para comunicarse con el backend; cuando se establece en <code>false</code> , Trident usa 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 la aplicación <code>ontapi</code> . Esto se cumple con los roles predefinidos <code>vsadmin</code> y <code>cluster-admin</code> . A partir de la versión Trident 24.06 y ONTAP 9.15.1 o posteriores, <code>useREST</code> está configurado en <code>true</code> de forma predeterminada; cambia <code>useREST</code> a <code>false</code> para usar llamadas ONTAPI (ZAPI). Si se especifica, siempre se establece 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 solicitable de FlexVol al utilizar Qtrees en el backend <code>ontap-nas-economy</code> .	"" (no aplicado por defecto)
denyNewVolumePools	Restringe <code>ontap-nas-economy</code> a los backends crear nuevos volúmenes FlexVol para contener sus Qtrees. Solo se utilizan los FlexVol ya existentes para el aprovisionamiento de nuevos PV.	
adAdminUser	Usuario o grupo de usuarios administradores de Active Directory con acceso total a los recursos compartidos SMB. Usa este parámetro para otorgar derechos de administrador al recurso compartido SMB con control total.	

Opciones de configuración de backend para aprovisionar volúmenes

Puedes controlar el aprovisionamiento predeterminado usando estas opciones en la `defaults` sección de la configuración. Por ejemplo, mira los ejemplos de configuración abajo.

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para Qtrees	"true"
spaceReserve	Modo de reserva de espacio; "ninguno" (fino) o "volumen" (grueso)	"none"
snapshotPolicy	Política de SnapVault a utilizar	"none"
qosPolicy	Grupo de políticas de QoS para asignar a los volúmenes creados. Elige uno de qosPolicy o adaptiveQosPolicy por cada pool de almacenamiento/backend	""
adaptiveQosPolicy	Grupo de políticas de QoS adaptativo para asignar a los volúmenes creados. Elige uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento/backend. No compatible con ontapas-economy.	""
snapshotReserve	Porcentaje de volumen reservado para instantáneas	"0" si snapshotPolicy es "none", de lo contrario ""
splitOnClone	Divide un clon de su padre al momento de su creación	"false"
encryption	Activa NetApp Volume Encryption (NVE) en el nuevo volumen; el valor predeterminado es false. NVE debe estar licenciado y habilitado en el clúster para usar esta opción. Si NAE está habilitado en el backend, cualquier volumen aprovisionado en Trident tendrá NAE habilitado. Para más información, consulta: "Cómo funciona Trident con NVE y NAE" .	"false"
tieringPolicy	Política de organización en niveles para usar "none"	
unixPermissions	Modo para nuevos volúmenes	"777" para volúmenes NFS; vacío (no aplicable) para volúmenes SMB
snapshotDir	Controla el acceso al .snapshot directorio	true, false (establecer explícitamente).
exportPolicy	Política de exportación a usar	"default"
securityStyle	Estilo de seguridad para nuevos volúmenes. NFS admite mixed y unix estilos de seguridad. SMB admite mixed y ntfs estilos de seguridad.	NFS predeterminado es unix. SMB predeterminado es ntfs.
nameTemplate	Plantilla para crear nombres de volúmenes personalizados.	""

NOTA

Usar grupos de políticas de QoS con Trident requiere ONTAP 9.8 o una versión posterior. Deberías usar un grupo de políticas de QoS no compartido y asegurarte de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de QoS compartido impone el límite máximo para el rendimiento total de todas las cargas de trabajo.

Ejemplos de aprovisionamiento de volumen

Aquí tienes un ejemplo con 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 usa un nuevo cálculo para asegurarse de 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 usando el nuevo cálculo. Este cálculo asegura que el usuario reciba el espacio escribible que pidió en el PVC, y no menos espacio del que solicitó. Antes de la v21.07, cuando el usuario solicitaba un PVC (por ejemplo, 5 GiB), con el `snapshotReserve` al 50 por ciento, solo obtenía 2.5 GiB de espacio escribible. Esto es porque lo que el usuario pedía era todo el volumen y `snapshotReserve` es un porcentaje de eso. Con Trident 21.07, lo que el usuario pide es el espacio escribible y Trident define el número de `snapshotReserve` como el porcentaje del volumen completo. Esto no aplica a `ontap-nas-economy`. Mira el siguiente ejemplo para ver cómo funciona esto:

El cálculo es el siguiente:

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

Para `snapshotReserve` = 50%, y una solicitud de PVC de 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 pidió en la solicitud de PVC. El `volume show` 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.

En el caso de los backends existentes de instalaciones anteriores, configura los volúmenes tal y como se explica más arriba al actualizar Trident. Para los volúmenes que creaste antes de la actualización, deberías ajustar su tamaño para que el cambio se vea reflejado. Por ejemplo, un PVC de 2 GiB con `snapshotReserve=50` antes daba como resultado un volumen que proporciona 1 GiB de espacio grabable. Al cambiar el tamaño del volumen a 3 GiB, por ejemplo, la aplicación obtiene 3 GiB de espacio grabable en un volumen de 6 GiB.

Ejemplos de configuración mínima

Los siguientes ejemplos muestran configuraciones básicas que dejan la mayoría de los parámetros en sus valores predeterminados. Esta es la forma más fácil de definir un backend.

NOTA

Si estás usando Amazon FSx en NetApp ONTAP con Trident, la recomendación es especificar nombres DNS para los LIF en vez de direcciones IP.

▼ Ejemplo de ONTAP NAS economy

```
---
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 ONTAP NAS FlexGroup

```
---
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

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

Para una conmutación de sitios sin interrupciones, especifica la SVM usando `managementLIF` y omite los parámetros `dataLIF` y `svm`. Por ejemplo:

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

▼ Ejemplo de volúmenes 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 mínima de backend. `clientCertificate`, `clientPrivateKey` y `trustedCACertificate` (opcional, si usas una CA de confianza) se rellenan en `backend.json` y toman los valores codificados en 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

Este ejemplo muestra cómo puedes indicarle a Trident que use políticas de exportación dinámicas para crear y gestionar la política de exportación automáticamente. Esto funciona igual para los controladores `ontap-nas-economy` 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 distribución equilibrada

Este ejemplo habilita la distribución equilibrada de ONTAP para que ONTAP seleccione el agregado para los nuevos volúmenes. La distribución equilibrada requiere ONTAP 9.19.1 o una versión posterior. Consulta ["Utiliza la distribución equilibrada con los backends de ONTAP"](#) para obtener más detalles.

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas-balanced-placement
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
username: vsadmin
password: password
useBalancedPlacement: true
```

▼ Ejemplo de direcciones IPv6

Este ejemplo muestra `managementLIF` usando 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 for ONTAP usando volúmenes SMB

El smbShare parámetro es necesario para FSx for ONTAP usando volúmenes SMB.

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

▼ 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 backends 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 grupos virtuales se definen en la sección de almacenamiento.

Trident establece las etiquetas de aprovisionamiento en el campo "Comentarios". Los comentarios se establecen en FlexVol para `ontap-nas` o en FlexGroup para `ontap-nas-flexgroup`. Trident copia todas las etiquetas presentes en un pool virtual al volumen de almacenamiento al aprovisionar. 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` valores, y algunos pools anulan los valores predeterminados.

▼ Ejemplo de ONTAP NAS

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: "false"
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
  - labels:
      app: msoffice
      cost: "100"
      zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
      adaptiveQosPolicy: adaptive-premium
  - labels:
      app: slack
      cost: "75"
      zone: us_east_1b
    defaults:
```

```

    spaceReserve: none
    encryption: "true"
    unixPermissions: "0755"
- labels:
    department: legal
    creditpoints: "5000"
    zone: us_east_1b
    defaults:
        spaceReserve: none
        encryption: "true"
        unixPermissions: "0755"
- labels:
    app: wordpress
    cost: "50"
    zone: us_east_1c
    defaults:
        spaceReserve: none
        encryption: "true"
        unixPermissions: "0775"
- labels:
    app: mysqldb
    cost: "25"
    zone: us_east_1d
    defaults:
        spaceReserve: volume
        encryption: "false"
        unixPermissions: "0775"

```

▼ Ejemplo de ONTAP NAS FlexGroup

```

---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
    spaceReserve: none
    encryption: "false"
labels:
    store: flexgroup_store
    k8scluster: prod-cluster-1
region: us_east_1
storage:
    - labels:

```

```

    protection: gold
    creditpoints: "50000"
    zone: us_east_1a
    defaults:
      spaceReserve: volume
      encryption: "true"
      unixPermissions: "0755"
- labels:
    protection: gold
    creditpoints: "30000"
    zone: us_east_1b
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0755"
- labels:
    protection: silver
    creditpoints: "20000"
    zone: us_east_1c
    defaults:
      spaceReserve: none
      encryption: "true"
      unixPermissions: "0775"
- labels:
    protection: bronze
    creditpoints: "10000"
    zone: us_east_1d
    defaults:
      spaceReserve: volume
      encryption: "false"
      unixPermissions: "0775"

```

▼ Ejemplo de ONTAP NAS economy

```

---
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"

```

Asigna backends a StorageClasses

Las siguientes definiciones de StorageClass hacen referencia a [Ejemplos de backends con pools virtuales](#). Usando el campo `parameters.selector`, cada StorageClass indica qué grupos virtuales se pueden usar para alojar un volumen. El volumen tiene los aspectos definidos en el grupo virtual elegido.

- El `protection-gold` StorageClass se asigna al primer y segundo grupo virtual en el backend `ontap-nas-flexgroup`. Estos son los únicos grupos 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"

```

- El protection-not-gold StorageClass se asigna al tercer y cuarto grupo virtual en el ontap-nas-flexgroup backend. Estos son los únicos grupos que ofrecen un nivel de protección distinto a gold.

```

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

```

- El app-mysqldb StorageClass se asigna al cuarto grupo virtual en el backend ontap-nas. Este es el único grupo que ofrece configuración de grupo de almacenamiento para apps tipo mysqldb.

```

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

```

- El protection-silver-creditpoints-20k StorageClass se asigna al tercer grupo virtual en el backend ontap-nas-flexgroup. Este es el único grupo que ofrece protección de nivel silver y 20 000 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"

```

- El `creditpoints-5k StorageClass` se corresponde con el tercer grupo virtual en el backend `ontap-nas` y con el segundo grupo virtual en el backend `ontap-nas-economy`. Estas son las únicas ofertas de grupos 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 decide qué grupo virtual se selecciona y garantiza que se cumpla el requisito de almacenamiento.

Actualiza dataLIF después de la configuración inicial

Puedes cambiar el dataLIF después de la configuración inicial ejecutando el siguiente comando para proporcionar el nuevo archivo JSON del backend con el dataLIF actualizado.

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

NOTA

Si los PVC están conectados a uno o varios pods, tienes que desactivar todos los pods correspondientes y luego volverlos a activar para que el nuevo dataLIF surta efecto.

Ejemplos seguros de SMB

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 storage pool

```
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 el 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
```

NOTA

Asegúrate de agregar annotations para habilitar SMB seguro. SMB seguro no funciona sin las anotaciones, independientemente de las configuraciones establecidas en el Backend o PVC.

Ejemplo de clase de almacenamiento con el 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 único usuario 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 varios usuarios 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:

```

Utiliza la distribución equilibrada con los backends de ONTAP

Puedes habilitar la distribución equilibrada de ONTAP en los backends de ONTAP. Con la distribución equilibrada, ONTAP selecciona el agregado óptimo para cada nuevo volumen, así que no necesitas gestionar la asignación de agregados en Trident.

Cómo funciona la asignación equilibrada

De forma predeterminada, Trident detecta los agregados asignados a una SVM, trata cada agregado como un grupo de almacenamiento y selecciona un agregado al aprovisionar un volumen.

Cuando activas la ubicación equilibrada:

- Trident muestra todo el SVM como un único grupo de almacenamiento en lugar de mostrar los agregados de forma individual.
- ONTAP selecciona el agregado para cada nuevo volumen y distribuye los volúmenes entre los agregados disponibles.
- Trident crea volúmenes mediante la API de REST de ONTAP `/application/containers`.

La distribución equilibrada está disponible para los sistemas ONTAP unificados (AFF, FAS y ASA) y los sistemas de almacenamiento AFX de NetApp.

Requisitos

- El backend debe utilizar ONTAP 9.19.1 o una versión posterior.
- Trident debe comunicarse con ONTAP mediante REST. La distribución equilibrada no está disponible con ZAPI.
- La configuración del backend no debe especificar agregados. No puedes combinar la distribución equilibrada con la selección explícita de agregados.

Valores por defecto

El valor por defecto de `useBalancedPlacement` depende del sistema de almacenamiento:

Sistema de almacenamiento	Predeterminado	Notas
ONTAP unificado (AFF, FAS, ASA)	<code>false</code>	Trident selecciona los agregados a menos que actives la colocación equilibrada.
NetApp AFX (ONTAP 9.19.1 o posterior)	<code>true</code>	Es necesario que la ubicación sea equilibrada. Establecer <code>useBalancedPlacement</code> en <code>false</code> hace que la validación del backend falle.
NetApp AFX (anterior a ONTAP 9.19.1)	<code>false</code>	La asignación equilibrada no está disponible.

Opción de configuración

Parámetro	Descripción	Predeterminado
<code>useBalancedPlacement</code>	Delegar la selección de agregados para nuevos volúmenes en ONTAP. Configura esta opción en la raíz de la configuración del backend o en grupos virtuales individuales.	<code>false</code> ; <code>true</code> para AFX en ONTAP 9.19.1 o versiones posteriores

Asignación equilibrada con grupos virtuales

La asignación equilibrada funciona tanto con como sin grupos virtuales:

- Sin grupos de almacenamiento virtuales, Trident informa el SVM como un único grupo de almacenamiento y crea todos los nuevos volúmenes utilizando una distribución equilibrada.
- Con los grupos virtuales, Trident informa los grupos virtuales y asigna los volúmenes a ellos como de costumbre. Si el grupo virtual coincidente tiene habilitada la distribución equilibrada, ONTAP selecciona el agregado para el volumen.

Establece `useBalancedPlacement` en la raíz de la configuración del backend para aplicarlo a todos los grupos virtuales, o configúralo en grupos virtuales concretos para habilitarlo de forma selectiva.

Ejemplos

El siguiente ejemplo permite un reparto equilibrado en un backend ONTAP unificado:

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

El siguiente ejemplo permite una distribución equilibrada utilizando `TridentBackendConfig`:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: nas-balanced-placement
  managementLIF: 10.0.0.1
```

```

svm: trident_svm
useBalancedPlacement: true
credentials:
  name: backend-tbc-ontap-nas-secret

```

El siguiente ejemplo habilita la distribución equilibrada únicamente en el `gold` grupo virtual. Trident sigue seleccionando agregados para los volúmenes que coinciden con el `bronze` grupo virtual:

```

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

```

Errores de validación del backend

La creación o actualización del backend falla en los siguientes casos:

Configuración	Resultado
<code>useBalancedPlacement: true</code> en ONTAP anterior a 9.19.1	La validación falló. Actualiza a ONTAP 9.19.1 o una versión posterior.
<code>useBalancedPlacement: true</code> en un backend que utiliza ZAPI	La validación falló. Configura el backend para que utilice REST.
<code>useBalancedPlacement: true</code> en combinación con agregados específicos	La validación falló. Elimina la configuración del agregado o desactiva la distribución equilibrada.
<code>useBalancedPlacement: false</code> en AFX con ONTAP 9.19.1 o posterior	La validación falló. Se requiere una distribución equilibrada para AFX en ONTAP 9.19.1 o posterior.

Amazon FSx for NetApp ONTAP

Usa Trident con Amazon FSx for NetApp ONTAP

"[Amazon FSx for NetApp ONTAP](#)" es un servicio de AWS totalmente administrado que ejecuta sistemas de archivos impulsados por el sistema operativo de almacenamiento

NetApp ONTAP. Proporciona características, rendimiento y administración de ONTAP con la escalabilidad y la simplicidad operativa de AWS. Un sistema de archivos es el recurso principal en Amazon FSx y es análogo a un clúster ONTAP local. Cada sistema de archivos contiene una o varias máquinas virtuales de almacenamiento (SVM), y cada SVM contiene uno o varios volúmenes que almacenan archivos y directorios. Esta integración permite a los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) aprovisionar volúmenes persistentes respaldados por ONTAP para cargas de trabajo de bloques y archivos.

Requisitos

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

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

NOTA

Asegúrate de seguir los pasos de preparación de nodo necesarios para Amazon Linux y Ubuntu ["Amazon Machine Images"](#) (AMIs) según tu tipo de AMI de EKS.

Consideraciones

- Volúmenes SMB:
 - Los volúmenes SMB son compatibles usando solo el `ontap-nas` driver.
 - Los volúmenes SMB no son compatibles con el complemento Trident EKS.
 - Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows. Consulta ["Prepárate para aprovisionar volúmenes SMB"](#) para obtener más detalles.
- Antes de Trident 24.02, los volúmenes creados en sistemas de archivos de Amazon FSx que tenían copias de seguridad automáticas habilitadas no podían ser eliminados por Trident. Para evitar este problema en Trident 24.02 o versiones posteriores, especifica el `fsxFilesystemID`, `AWS apiRegion`, `AWS apikey` y `AWS secretKey` en el archivo de configuración del backend para AWS FSx for ONTAP.

NOTA

Si estás especificando una función de IAM para Trident, entonces puedes omitir especificar los campos `apiRegion`, `apiKey` y `secretKey` explícitamente para Trident. Para obtener más información, consulta ["Opciones de configuración de FSx for ONTAP y ejemplos"](#).

Uso simultáneo de Trident SAN/iSCSI y el controlador EBS-CSI

Si planeas usar controladores `ontap-san` (por ejemplo, iSCSI) con AWS (EKS, ROSA, EC2 o cualquier otra instancia), la configuración de multivía requerida en los nodos podría entrar en conflicto con el controlador CSI de Amazon Elastic Block Store (EBS). Para asegurarte de que la multivía funcione sin interferir con los discos EBS en el mismo nodo, necesitas excluir EBS en tu configuración de multivía. Este ejemplo muestra un `multipath.conf` archivo que incluye la configuración requerida de Trident y excluye los discos EBS de la multivía:

```
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. Puedes usar el `fsxadmin` usuario para tu sistema de archivos o el `vsadmin` usuario configurado para tu SVM.

ADVERTENCIA

Trident espera ejecutarse como un `vsadmin` usuario de SVM o como un usuario con un nombre diferente que tenga el mismo rol. Amazon FSx for NetApp ONTAP tiene un `fsxadmin` usuario que es un reemplazo limitado del usuario de clúster de ONTAP `admin`. Te recomendamos mucho usar `vsadmin` con Trident.

- Basado en certificado: Trident se comunicará con la SVM en tu sistema de archivos FSx usando un certificado instalado en tu SVM.

Para obtener detalles sobre cómo habilitar la autenticación, consulta la autenticación para tu tipo de controlador:

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

Imágenes de máquina de Amazon (AMIs) probadas

El clúster EKS es compatible con varios sistemas operativos, pero AWS ha optimizado ciertas Amazon Machine Images (AMIs) para contenedores y EKS. Las siguientes AMIs se han probado con NetApp Trident 25.02.

AMI	NAS	NAS-economy	iSCSI	iSCSI-economy
AL2023_x86_64_STANDARD	Sí	Sí	Sí	Sí
AL2_x86_64	Sí	Sí	Sí*	Sí*
BOTTLEROCKET_x86_64	Sí**	Sí	N/A	N/A
AL2023_ARM_64_STANDARD	Sí	Sí	Sí	Sí

AL2_ARM_64	Sí	Sí	Sí*	Sí*
BOTTLEROCKET_ARM_64	Sí**	Sí	N/A	N/A

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

NOTA

Si la AMI que buscas 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 AWS add-On 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 (regular, qtree/lun – economy, NAS con backup de AWS)

Encuentra más información

- ["Documentación de Amazon FSx para NetApp ONTAP"](#)
- ["Entrada de blog sobre Amazon FSx para NetApp ONTAP"](#)

Crea un rol de IAM y un secreto de AWS

Puedes configurar pods de Kubernetes para acceder a recursos de AWS autenticándote como un rol de AWS IAM en lugar de proporcionar credenciales de AWS explícitas.

NOTA

Para autenticarse mediante una función de AWS IAM, debes tener un clúster de Kubernetes implementado usando EKS.

Crear secreto de AWS Secrets Manager

Como Trident va a emitir APIs contra un vserver de FSx para gestionar el almacenamiento por ti, necesitará credenciales para hacerlo. La forma segura de pasar esas credenciales es a través de un secreto de AWS Secrets Manager. Así que, si aún no tienes uno, tendrás que crear un secreto de AWS Secrets Manager que contenga las credenciales para la cuenta vsadmin.

Este ejemplo 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 funcionar correctamente. Por lo tanto, necesitas crear una política que le dé a Trident los permisos que necesita.

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

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

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"  
}
```

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

Puedes configurar una cuenta de servicio de Kubernetes para que asuma un rol de AWS Identity and Access Management (IAM) con EKS Pod Identity o IAM role for Service account association (IRSA). Cualquier pod que esté 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 Amazon EKS Pod Identity proporcionan la capacidad de administrar credenciales para tus aplicaciones, de forma similar a como los perfiles de instancias de Amazon EC2 proporcionan credenciales a las instancias de Amazon EC2.

Instala Pod Identity en tu clúster EKS:

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

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

Para más información consulta ["Configura el agente de identidad de Amazon EKS Pod"](#).

Crea trust-relationship.json:

Crea trust-relationship.json para permitir que EKS Service Principal asuma este rol para Pod Identity. Luego, crea 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"
      ]
    }
  ]
}
```

```
]
}
```

Adjunta la política de rol al rol IAM:

Adjunta la política de rol del paso anterior al rol IAM que creaste:

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

Crea una asociación de identidad de pod:

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

Función IAM para la asociación de cuenta 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"
    }
  }
}
]
```

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

- **<account_id>** - Tu ID de cuenta AWS
- **<oidc_provider>** - El OIDC de tu cluster EKS. Puedes obtener el `oidc_provider` ejecutando:

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

Adjunta el rol IAM con la política IAM:

Una vez que el rol ha sido creado, adjunta la política (que fue creada en el paso anterior) al rol usando este comando:

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

Verifica que el proveedor OICD está asociado:

Verifica que tu proveedor OIDC está asociado con tu cluster. Puedes verificarlo usando este comando:

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

Si la salida está vacía, usa el siguiente comando para asociar IAM OIDC a tu clúster:

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

Si usas **eksctl**, usa el siguiente ejemplo para crear una función IAM para la 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
```

Instala Trident

Trident agiliza la administración del almacenamiento de Amazon FSx para NetApp ONTAP en Kubernetes para que tus desarrolladores y administradores se enfoquen en la puesta en marcha de aplicaciones. Puedes instalar Trident usando uno de los siguientes métodos:

- Helm
- Complemento EKS

Si quieres hacer uso de la funcionalidad de instantáneas, instala el complemento controlador de instantáneas CSI. Consulta ["Habilita la funcionalidad de instantáneas para volúmenes CSI"](#) para obtener más información.

Instala Trident con helm

Identidad de pod

1. Agrega el repositorio Trident Helm:

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

2. Instala Trident usando el siguiente ejemplo:

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

Puedes usar el comando `helm list` para revisar detalles de la 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 cuenta de servicio (IRSA)

1. Agrega el repositorio Trident Helm:

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

```
chart
```

2. Establece los valores de **proveedor de nube** e **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
```

Puedes usar el comando `helm list` para revisar detalles de la 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 estás planeando usar iSCSI, asegúrate de que iSCSI esté habilitado en tu máquina cliente. Si estás usando AL2023 Worker node OS, puedes automatizar la instalación del cliente iSCSI añadiendo el parámetro `node prep` en la instalación de helm:

NOTA

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

Instala Trident mediante el add-on EKS

El complemento Trident EKS incluye los últimos parches de seguridad, correcciones de errores y está validado por AWS para funcionar con Amazon EKS. El complemento EKS te permite asegurarte de forma constante de que tus clústeres de Amazon EKS sean seguros y estables, y reducir la cantidad de trabajo que necesitas hacer para instalar, configurar y actualizar complementos.

Prerrequisitos

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

- Una cuenta de clúster de Amazon EKS con suscripción de complemento
- 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 existente de Amazon FSx para NetApp ONTAP

Habilita el complemento Trident para AWS

Consola de gestión

1. Abre la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, selecciona **Clusters**.
3. Selecciona el nombre del clúster para el que quieres configurar el complemento NetApp Trident CSI.
4. Selecciona **Add-ons** y luego **Get more add-ons**.
5. Sigue estos pasos para seleccionar el complemento:
 - a. Desplázate hasta la sección **AWS Marketplace add-ons** y escribe **"Trident"** en el cuadro de búsqueda.
 - b. Selecciona la casilla de comprobación en la esquina superior derecha del cuadro Trident by NetApp.
 - c. Selecciona **Siguiente**.
6. En la página de configuración **Configurar add-ons seleccionados**, haz lo siguiente:

NOTA Omite estos pasos si estás usando la asociación Pod Identity.

- a. Selecciona la **Version** que te gustaría usar.
- b. Si estás usando la autenticación IRSA, asegúrate de establecer los valores de configuración disponibles en la configuración opcional:
 - Selecciona la **Version** que te gustaría usar.
 - Sigue el **Add-on configuration schema** y establece el parámetro **configurationValues** en la sección **Configuration values** al role-arn que creaste en el paso anterior (el valor debe tener el siguiente formato):

```
{

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

}
```

+

Si seleccionas Override como método de resolución de conflictos, una o más de las configuraciones

del add-on existente pueden sobrescribirse con las configuraciones del Amazon EKS add-on. Si no habilitas esta opción y hay un conflicto con tus configuraciones existentes, la operación falla. Puedes usar el mensaje de error resultante para solucionar el conflicto. Antes de seleccionar esta opción, asegúrate de que el Amazon EKS add-on no gestione configuraciones que necesites administrar tú mismo.

7. Elige **Siguiente**.

8. En la página **Revisar y agregar**, elige **Crear**.

Después de que se complete la instalación del complemento, verás tu complemento instalado.

AWS CLI

1. Crea el `add-on.json` file:

Para la identidad del pod, usa el siguiente formato:

NOTA | Usa la

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

Para la autenticación de IRSA, usa 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"
  }
}
```

NOTA | Reemplaza `<role ARN>` con el ARN del rol que se creó en el paso anterior.

2. Instala 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
```

Actualiza el add-on Trident EKS

Consola de gestión

1. Abre la consola de Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, selecciona **Clusters**.
3. Selecciona el nombre del clúster para el que quieres actualizar el software complementario Trident CSI de NetApp.
4. Selecciona la pestaña **Add-ons**.
5. Selecciona **Trident by NetApp** y luego selecciona **Editar**.
6. En la página **Configura Trident por NetApp**, haz lo siguiente:
 - a. Selecciona la **Version** que te gustaría usar.
 - b. Expande las **Configuraciones de configuración opcionales** y modifícalas según sea necesario.
 - c. Selecciona **Guardar cambios**.

AWS CLI

El siguiente ejemplo actualiza el add-on EKS:

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

eksctl

- Comprueba la versión actual de tu FSxN Trident CSI add-on. Reemplaza my-cluster con el nombre de tu 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'\"}			

- Actualiza el software complementario a la versión que aparece bajo UPDATE AVAILABLE en la salida del paso anterior.

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

Si quitas la opción `--force` y alguna de las configuraciones del complemento de Amazon EKS entra en conflicto con tus configuraciones actuales, entonces la actualización del complemento de Amazon EKS falla; recibes un mensaje de error para ayudarte a resolver el conflicto. Antes de especificar esta opción, asegúrate de que el complemento de Amazon EKS no administre configuraciones que necesites administrar, porque esas configuraciones se sobrescriben con esta opción. Para más información sobre otras opciones para esta configuración, consulta "[Complementos](#)". Para más información sobre la administración de campos de Kubernetes de Amazon EKS, consulta "[Gestión de campos de Kubernetes](#)".

Desinstala/elimina el complemento Trident EKS

Tienes dos opciones para eliminar un complemento de Amazon EKS:

- **Conservar el software complementario en tu clúster** – Esta opción elimina la administración de cualquier configuración por parte de Amazon EKS. También elimina la capacidad de Amazon EKS para notificarte sobre actualizaciones y actualizar automáticamente el Amazon EKS add-on después de que inicies una actualización. Sin embargo, conserva el software complementario en tu clúster. Esta opción hace que el add-on sea una instalación autogestionada, en lugar de un Amazon EKS add-on. Con esta opción, no hay tiempo de inactividad para el add-on. Retén la `--preserve` opción en el comando para conservar el add-on.
- **Elimina el software complementario por completo de tu clúster** – NetApp recomienda que elimines el complemento de Amazon EKS de tu clúster solo si no hay recursos en tu clúster que dependan de él. Elimina la opción `--preserve` del comando `delete` para eliminar el complemento.

NOTA Si el software complementario tiene una cuenta IAM asociada, la cuenta IAM no se elimina.

Consola de gestión

1. Abre la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters>.
2. En el panel de navegación izquierdo, selecciona **Clusters**.
3. Selecciona el nombre del clúster del que quieres quitar el NetApp Trident CSI add-on.
4. Selecciona la pestaña **Complementos** y luego selecciona **Trident by NetApp**.*
5. Selecciona **Eliminar**.
6. En el cuadro de diálogo **Remove netapp_trident-operator confirmation**, haz lo siguiente:
 - a. Si quieres que Amazon EKS deje de administrar la configuración del software complementario, selecciona **Conservar en el clúster**. Haz esto si quieres conservar el software complementario en tu clúster para que puedas administrar tú mismo todas las configuraciones del complemento.
 - b. Ingresa **netapp_trident-operator**.
 - c. Selecciona **Eliminar**.

AWS CLI

Reemplaza `my-cluster` con el nombre de tu clúster y luego ejecuta 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
```

Configurar una clase de almacenamiento

El "[Objeto de Kubernetes StorageClass](#)" identifica a un proveedor y le indica cómo aprovisionar volúmenes. Esta sección te muestra cómo configurar un objeto de Kubernetes StorageClass que especifica a Trident como el proveedor.

Crear un objeto StorageClass

Cuando creas un StorageClass para FSx for ONTAP, Trident creará automáticamente la configuración del backend.

NOTA

Si quieres configurar manualmente el backend de almacenamiento, consulta la sección [Crear un Kubernetes StorageClass sin configuración automática del backend](#) para saber cómo crear el backend Trident y la clase de almacenamiento por separado.

Especifica los parámetros requeridos StorageClass

Los siguientes tres parámetros deben definirse al crear un StorageClass:

Parámetro	Requerido	Tipo	Descripción
<code>fsxFilesystemID</code>	Sí	cadena	FSx para NetApp ONTAP filesystem ID
<code>storageDriverName</code>	Sí	cadena	Controlador de almacenamiento Trident (por ejemplo, <code>ontap-nas</code> o <code>ontap-san</code>)
<code>credentialsName</code>	Sí	cadena	Nombre del secreto de Kubernetes que contiene FSx for ONTAP credenciales

Especifica parámetros opcionales

Puedes pasar parámetros opcionales de backend a través de StorageClass. Define todos los valores opcionales como cadenas en la sección StorageClass `parameters`. Para obtener una lista completa de los parámetros de backend, consulta: "[Configuración del backend de FSx para NetApp ONTAP](#)".

Ejemplo de archivos de configuración de StorageClass.

El siguiente ejemplo muestra un StorageClass que activa la configuración automática del backend.

YAML

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

JSON

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

Crear el StorageClass

Una vez que hayas creado tu archivo de configuración, ejecuta el siguiente comando para crear la clase de almacenamiento.

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

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

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

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

Después de aplicar StorageClass, Trident crea el backend automáticamente. Luego, puedes crear PersistentVolumeClaims que hacen referencia a este StorageClass.

Verifica el estado de la configuración del backend

Trident registra el resultado de la creación del backend en las anotaciones de StorageClass.

Anotación	Descripción
trident.netapp.io/configuratorStatus	Resultado de la configuración (Success o Failure)
trident.netapp.io/configuratorMessage	Estado detallado o mensaje de error
trident.netapp.io/configuratorName	Nombre del recurso interno del configurador
trident.netapp.io/managed	Indica que el StorageClass está gestionado por Trident
trident.netapp.io/additionalStoragePools	Grupos de almacenamiento creados para este backend

Para verificar el estado, ejecuta:

```
kubectl get storageclass ontap-fsx-demo -o yaml
```

Confirma que `trident.netapp.io/configuratorStatus` está configurado en `Success`. Si el valor es `Failure`, revisa `trident.netapp.io/configuratorMessage` para ver el error.

Añade sistemas de archivos FSxN adicionales

Si necesitas capacidad de almacenamiento adicional mientras sigues usando el mismo StorageClass, añade ID de sistemas de archivos FSxN adicionales.

Edita el StorageClass y añade la siguiente anotación:

```
metadata:
  annotations:
    trident.netapp.io/additionalFsxnFileSystemID: '["fs-
xxxxxxxxxxxxxxxxxxxxxx"]'
```

Después de aplicar el cambio, Trident actualiza la configuración del backend y actualiza las anotaciones de StorageClass.

Consideraciones operativas y limitaciones

- Eliminar un StorageClass que tiene la configuración automática de backend normalmente elimina el backend Trident asociado. Esto puede interrumpir la conectividad de almacenamiento y afectar las cargas de trabajo en ejecución. Valida el impacto antes de eliminar un StorageClass administrado.
- La configuración automática del backend solo es compatible con AWS FSx for NetApp ONTAP.

Crear un Kubernetes StorageClass sin configuración automática del backend

Si quieres crear el backend de Trident y StorageClass por separado, entonces sigue estos pasos.

Entiende cómo funciona la configuración automática del backend

Trident obtiene la configuración del backend a partir de la definición de StorageClass. Cuando aplicas la StorageClass, Trident valida los parámetros necesarios, crea el backend y anota la StorageClass con el estado.

Trident crea el VolumeSnapshotClass solo una vez. Trident reutiliza el mismo VolumeSnapshotClass para los siguientes StorageClasses.

Crear el backend Trident

Para crear un backend Trident, necesitas crear un archivo de configuración en formato JSON o YAML. El archivo debe especificar el tipo de almacenamiento que quieres (NAS o SAN), el sistema de archivos, la SVM de la que lo vas a obtener y cómo autenticarte con ella. El siguiente ejemplo muestra cómo definir almacenamiento basado en NAS y usar un secreto de AWS para guardar las credenciales de la SVM que quieres usar:

YAML

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
```

```

    fsxFileSystemID: fs-xxxxxxxxxx
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name"
    type: awsarn

```

JSON

```

{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas"
    "namespace": "trident"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
      "fsxFileSystemID": "fs-xxxxxxxxxx"
    },
    "managementLIF": null,
    "credentials": {
      "name": "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name",
      "type": "awsarn"
    }
  }
}

```

Detalles del controlador de FSx for ONTAP

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

Nombre del controlador	Descripción
ontap-san	Cada PV aprovisionado es un LUN dentro de su propio volumen de Amazon FSx for NetApp ONTAP. Recomendado para almacenamiento en bloque.
ontap-nas	Cada PV aprovisionado es un volumen completo de Amazon FSx for NetApp ONTAP. Recomendado para NFS y SMB.
ontap-san-economy	Cada PV aprovisionado es un LUN con un número configurable de LUNs por volumen de Amazon FSx para NetApp ONTAP.

Nombre del controlador	Descripción
ontap-nas-economy	Cada PV aprovisionado es un qtree, con un número configurable de qtrees por volumen de Amazon FSx para NetApp ONTAP.
ontap-nas-flexgroup	Cada PV aprovisionado es un volumen completo de Amazon FSx for NetApp ONTAP FlexGroup.

Para obtener detalles del controlador, consulta ["Controladores NAS"](#) y ["Controladores SAN"](#).

Crea el backend

Después de crear el archivo de configuración, ejecuta los siguientes comandos para crear y validar la configuración del backend de Trident (TBC):

- Crea la configuración del backend de Trident (TBC) desde el archivo yaml y ejecuta el siguiente comando:

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

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

- Valida que la configuración de backend de Trident (TBC) se creó 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	

Para más información sobre otras opciones de configuración, consulta la sección [Configuración avanzada del backend y ejemplos](#) a continuación.

Configura una clase de almacenamiento sin configuración automática del backend

A continuación se muestran ejemplos de configuraciones de Storage Class para su uso con Trident y FSx for ONTAP.

Clase de almacenamiento para NFS

Puedes usar este ejemplo para configurar StorageClass para volúmenes que usan NFS (consulta la sección de atributos de Trident a continuación para 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"
```

Clase de almacenamiento para iSCSI

Usa este ejemplo para configurar StorageClass para volúmenes que usan 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"
```

Clase de almacenamiento con NFSv3 y AWS Bottlerocket

Para aprovisionar volúmenes NFSv3 en AWS Bottlerocket, agrega lo requerido `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
```

Atributos de Trident StorageClass

Estos parámetros determinan qué grupos de almacenamiento administrados por Trident se deben utilizar para aprovisionar volúmenes de un tipo dado.

Atributo	Tipo	Valores	Oferta	Solicitud	Con el apoyo de
medios ¹	cadena	hdd, híbrido, ssd	El pool contiene medios de este tipo; híbrido significa ambos	Tipo de medio especificado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
provisioningType	cadena	delgado, grueso	Pool admite este método de aprovisionamiento	Método de aprovisionamiento o especificado	grueso: todo ontap; fino: todo ontap & solidfire-san
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 drivers
instantáneas	bool	verdadero, falso	El pool admite volúmenes con instantáneas	Volumen con instantáneas habilitadas	ontap-nas, ontap-san, solidfire-san
clones	bool	verdadero, falso	El pool admite la clonación de volúmenes	Volumen con clones habilitados	ontap-nas, ontap-san, solidfire-san
cifrado	bool	verdadero, falso	El pool admite volúmenes cifrados	Volumen con cifrado habilitado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	entero	entero positivo	El pool es capaz de garantizar IOPS en este rango	Volumen garantizó estas IOPS	solidfire-san

¹: No soportado por ONTAP Select o FSx for ONTAP systems

Consulta "[Objetos de Kubernetes y Trident](#)" para ver detalles sobre cómo las clases de almacenamiento interactúan con el `PersistentVolumeClaim` y los parámetros para controlar cómo Trident aprovisiona volúmenes.

Crear la clase de almacenamiento

Una vez que hayas configurado StorageClass, puedes crearlo en Kubernetes.

Pasos

1. Este es un objeto de Kubernetes, así que usa `kubectl` para crearlo en Kubernetes.

```
kubectl create -f storage-class-ontapas.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 backend.

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

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

Aprovisionar volúmenes SMB

Puedes aprovisionar volúmenes SMB usando el controlador `ontap-nas`. Sin embargo, para hacerlo debes completar estos pasos: ["Prepárate para aprovisionar volúmenes SMB"](#).

Configuración avanzada del backend y ejemplos

Consulta la siguiente tabla para ver las opciones de configuración del backend:

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 backend de almacenamiento	Nombre del driver + "_" + dataLIF

Parámetro	Descripción	Ejemplo
managementLIF	Dirección IP de un clúster o de una LIF de administración de SVM. Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si proporcionas el fsxFilesystemID bajo el campo aws, no necesitas proporcionar el managementLIF porque Trident obtiene la información de SVM managementLIF desde AWS. Así que debes proporcionar credenciales para un usuario bajo la SVM (por ejemplo: vsadmin) y el usuario debe tener el rol vsadmin.	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	Dirección IP del LIF de protocolo. Controladores NAS de ONTAP: NetApp recomienda especificar dataLIF. Si no se proporciona, Trident obtiene los dataLIF del SVM. Puedes especificar un nombre de dominio completo (FQDN) para las operaciones de montaje NFS, lo que te permite crear un DNS de round-robin para balancear la carga entre varios dataLIF. Se puede cambiar después de la configuración inicial. Controladores SAN de ONTAP: No lo especifiques para iSCSI. Trident usa ONTAP Selective LUN Map para descubrir los LIF de iSCSI necesarios para establecer una sesión multipath. Se genera una advertencia si dataLIF se define explícitamente. Se puede configurar para usar direcciones IPv6 si Trident se instaló usando el flag de IPv6. Las direcciones IPv6 deben definirse entre corchetes, como [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	

Parámetro	Descripción	Ejemplo
<code>autoExportPolicy</code>	Habilita la creación y actualización automática de políticas de exportación [Boolean]. Usando las opciones <code>autoExportPolicy</code> y <code>autoExportCIDRs</code> , Trident puede gestionar las políticas de exportación automáticamente.	<code>false</code>
<code>autoExportCIDRs</code>	Lista de CIDR para filtrar las direcciones IP de los nodos de Kubernetes cuando <code>autoExportPolicy</code> está habilitado. Usando las opciones <code>autoExportPolicy</code> y <code>autoExportCIDRs</code> , Trident puede gestionar las políticas de exportación automáticamente.	<code>["0.0.0.0/0", "::/0"]</code>
<code>labels</code>	Conjunto de etiquetas arbitrarias con formato JSON para aplicar en volúmenes	<code>""</code>
<code>clientCertificate</code>	Valor codificado en Base64 del certificado del cliente. Usado para auth basada en certificados	<code>""</code>
<code>clientPrivateKey</code>	Valor codificado en Base64 de la clave privada del cliente. Usado para auth basada en certificados	<code>""</code>
<code>trustedCACertificate</code>	Valor codificado en Base64 del certificado de CA de confianza. Opcional. Se usa para la autenticación basada en certificados.	<code>""</code>
<code>username</code>	Nombre de usuario para conectarte al clúster o SVM. Se utiliza para la autenticación basada en credenciales. Por ejemplo, <code>vsadmin</code> .	
<code>password</code>	Contraseña para conectarse al clúster o SVM. Se utiliza para la autenticación basada en credenciales.	
<code>svm</code>	Máquina virtual de almacenamiento que vas a usar	Derivado si se especifica un LIF de gestión de SVM.
<code>storagePrefix</code>	Prefijo que se utiliza al aprovisionar nuevos volúmenes en el SVM. No se puede modificar después de la creación. Para actualizar este parámetro, tendrás que crear un nuevo backend.	<code>trident</code>

Parámetro	Descripción	Ejemplo
limitAggregateUsage	No especifiques para Amazon FSx for NetApp ONTAP. Los <code>fsxadmin</code> y <code>vsadmin</code> no tienen los permisos necesarios para recuperar el uso agregado y limitarlo usando Trident.	No uses.
limitVolumeSize	Falla el aprovisionamiento si el tamaño del volumen solicitado supera este valor. También restringe el tamaño máximo de los volúmenes que administra para <code>qtrees</code> y LUNs, y la <code>qtreesPerFlexvol</code> opción permite personalizar el número máximo de <code>qtrees</code> por FlexVol volume	"" (no aplicado por defecto)
lunsPerFlexvol	LUNs máximos por FlexVol volume, deben estar en el rango [50, 200]. Solo para SAN.	"100"
debugTraceFlags	Indicadores de depuración para utilizar cuando estés solucionando problemas. Por ejemplo, <code>{"api":false, "method":true}</code> no uses <code>debugTraceFlags</code> a menos que estés resolviendo problemas y necesites un volcado de registro detallado.	null
nfsMountOptions	Lista separada por comas de opciones de montaje NFS. Las opciones de montaje para volúmenes persistentes de Kubernetes normalmente se especifican en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident usará las opciones de montaje especificadas en el archivo de configuración del backend de almacenamiento. Si no se especifican opciones de montaje en la clase de almacenamiento ni en el archivo de configuración, Trident no establecerá ninguna opción de montaje en un volumen persistente asociado.	""

Parámetro	Descripción	Ejemplo
<code>nasType</code>	Configura la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o <code>null</code> . Debes establecerlo en <code>smb</code> para volúmenes SMB. Si lo configuras en <code>null</code> , se usarán volúmenes NFS por defecto.	<code>nfs</code>
<code>qtreesPerFlexvol</code>	Máximo de <code>qtrees</code> por FlexVol volume, debe estar en el rango [50, 300]	<code>"200"</code>
<code>smbShare</code>	Puedes especificar uno de los siguientes: el nombre de un recurso compartido SMB creado usando Microsoft Management Console o ONTAP CLI, o un nombre para permitir que Trident cree el recurso compartido SMB. Este parámetro es obligatorio para los backends de Amazon FSx for ONTAP.	<code>smb-share</code>
<code>useREST</code>	Parámetro booleano para usar las ONTAP REST APIs. Cuando se establece en <code>true</code> , Trident usará las ONTAP REST APIs 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 la aplicación <code>ontap</code> . Esto se cumple con los roles predefinidos <code>vsadmin</code> y <code>cluster-admin</code> .	<code>false</code>
<code>aws</code>	Puedes especificar lo siguiente en el archivo de configuración para AWS FSx for ONTAP: - <code>fsxFilesystemID</code> : especifica el ID del sistema de archivos de AWS FSx. - <code>apiRegion</code> : nombre de la región de la API de AWS. - <code>apiKey</code> : clave de API de AWS. - <code>secretKey</code> : clave secreta de AWS.	<code>""</code> <code>""</code> <code>""</code>

Parámetro	Descripción	Ejemplo
credentials	Especifica las credenciales de FSx SVM que se van a guardar en AWS Secrets Manager. - name: Amazon Resource Name (ARN) del secreto, que contiene las credenciales de SVM. - type: Establéclo en awsarn. Consulta "Crea un secreto de AWS Secrets Manager" para obtener más información.	

Opciones de configuración de backend para aprovisionar volúmenes

Puedes controlar el aprovisionamiento predeterminado usando estas opciones en la `defaults` sección de la configuración. Por ejemplo, mira los ejemplos de configuración abajo.

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para LUNs	true
spaceReserve	Modo de reserva de espacio; "ninguno" (fino) o "volumen" (grueso)	none
snapshotPolicy	Política de SnapVault a utilizar	none
qosPolicy	Grupo de políticas de QoS para asignar a los volúmenes creados. Elige una de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o backend. Usar grupos de políticas de QoS con Trident requiere ONTAP 9.8 o una versión posterior. Deberías usar un grupo de políticas de QoS no compartido y asegurarte de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de QoS compartido impone el límite máximo para el rendimiento total de todas las cargas de trabajo.	""
adaptiveQosPolicy	Grupo de políticas de QoS adaptativo para asignar a los volúmenes creados. Elige una de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o backend. No compatible con ontap-nas-economy.	""
snapshotReserve	Porcentaje de volumen reservado para snapshots "0"	Si snapshotPolicy es none, else "

Parámetro	Descripción	Predeterminado
<code>splitOnClone</code>	Divide un clon de su padre al momento de su creación	<code>false</code>
<code>encryption</code>	Activa NetApp Volume Encryption (NVE) en el nuevo volumen; el valor predeterminado es <code>false</code> . NVE debe estar licenciado y habilitado en el clúster para usar esta opción. Si NAE está habilitado en el backend, cualquier volumen provisionado en Trident tendrá NAE habilitado. Para más información, consulta: " Cómo funciona Trident con NVE y NAE ".	<code>false</code>
<code>luksEncryption</code>	Activa el cifrado LUKS. Consulta " Usa Linux Unified Key Setup (LUKS) ". Solo para SAN.	""
<code>tieringPolicy</code>	Política de tiering a usar <code>none</code>	
<code>unixPermissions</code>	Modo para nuevos volúmenes. Dejar vacío para volúmenes SMB.	""
<code>securityStyle</code>	Estilo de seguridad para nuevos volúmenes. NFS admite <code>mixed</code> y <code>unix</code> estilos de seguridad. SMB admite <code>mixed</code> y <code>ntfs</code> estilos de seguridad.	NFS predeterminado es <code>unix</code> . SMB predeterminado es <code>ntfs</code> .

Configura un PVC

Esta sección incluye instrucciones sobre cómo crear un `PersistentVolumeClaim` (PVC) que utiliza la `StorageClass` de Kubernetes configurada para solicitar un PV. Si tiene éxito, luego puedes montar el PV en un pod.

Crea el PVC

Una "[PersistentVolumeClaim](#)" (PVC) es una solicitud de acceso al `PersistentVolume` en el clúster. El PVC se puede configurar para solicitar almacenamiento de un tamaño o modo de acceso determinados. Usando el `StorageClass` asociado, el administrador del clúster puede controlar más que solo el tamaño y el modo de acceso de `PersistentVolume`, como el rendimiento o el nivel de servicio.

Después de crear el backend Trident y `StorageClass` puedes crear un PVC. Después de crear el PVC, puedes montar el volumen en un pod.

Manifiestos de muestra

Los siguientes ejemplos muestran las opciones básicas de configuración del PVC.

PVC con acceso RWX

Este ejemplo muestra un PVC básico con acceso RWX que está asociado con una `StorageClass` 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 un StorageClass llamado protection-gold.

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

Crear PVC

Pasos

1. Crea la PVC.

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

2. Verifica el estado del PVC.

```
kubectl get pvc
```

NAME	STATUS	VOLUME	CAPACITY	ACCESS	MODES	STORAGECLASS	AGE
------	--------	--------	----------	--------	-------	--------------	-----

pvc-storage	Bound	pv-name	2Gi	RWO	5m
-------------	-------	---------	-----	-----	----

Consulta ["Objetos de Kubernetes y Trident"](#) para ver detalles sobre cómo las clases de almacenamiento interactúan con el PersistentVolumeClaim y los parámetros para controlar cómo Trident aprovisiona volúmenes.

Implementa una aplicación

Una vez creada la clase de almacenamiento y el PVC, puedes montar el PV en un pod. Esta sección muestra el comando de ejemplo y la configuración para conectar el PV a un pod.

Implementa una aplicación de ejemplo

Pasos

1. Monta 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
```

NOTA

Puedes monitorear el progreso usando `kubectl get pod --watch`.

2. Verifica que el volumen esté 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 puedes eliminar el Pod. La aplicación del Pod ya no existirá, pero el volumen permanecerá.

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

Configura el complemento Trident EKS en un clúster EKS

NetApp Trident optimiza la gestión del almacenamiento de Amazon FSx for NetApp ONTAP en Kubernetes para que tus desarrolladores y administradores puedan centrarse en la puesta en marcha de aplicaciones. El complemento NetApp Trident EKS incluye los últimos parches de seguridad, correcciones de errores y está validado por AWS para funcionar con Amazon EKS. El complemento EKS te permite asegurarte de forma constante de que tus clústeres de Amazon EKS sean seguros y estables, y reducir la cantidad de trabajo que necesitas hacer para instalar, configurar y actualizar complementos.

Prerrequisitos

Asegúrate 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. Consulta ["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 existente de Amazon FSx para NetApp ONTAP

Pasos

1. Asegúrate de crear un rol de IAM y un secreto de AWS para que los pods de EKS puedan acceder a los recursos de AWS. Para ver las instrucciones, consulta ["Crea un rol de IAM y un secreto de AWS"](#).
2. En tu clúster EKS Kubernetes, ve a la pestaña **Add-ons**.



① 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

Kubernetes version [Info](#)

1.30

Support period① [Standard support until July 28, 2025](#)**Provider**

EKS

Cluster health issues

✓ 0

Upgrade insights

✓ 0

Overview

Resources

Compute

Networking

Add-ons 1

Access

Observability

Update history

Tags

① 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. Ve a **AWS Marketplace add-ons** y elige la categoría *storage*.

AWS Marketplace add-ons (1)

Discover, subscribe to and configure EKS add-ons to enhance your EKS clusters.

Filtering options

Any category

NetApp, Inc.

Any pricing model

[Clear filters](#)

NetApp, Inc. ✕

< 1 >

**NetApp Trident**

NetApp Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. [Product details](#)

Standard Contract**Category**
storage**Listed by**
[NetApp, Inc.](#)**Supported versions**
1.31, 1.30, 1.29, 1.28,
1.27, 1.26, 1.25, 1.24,
1.23**Pricing starting at**
[View pricing details](#)[Cancel](#)[Next](#)

4. Localiza **NetApp Trident** y selecciona la casilla para el complemento Trident, y haz clic en **Siguiente**.

5. Elige 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. Configura 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 >

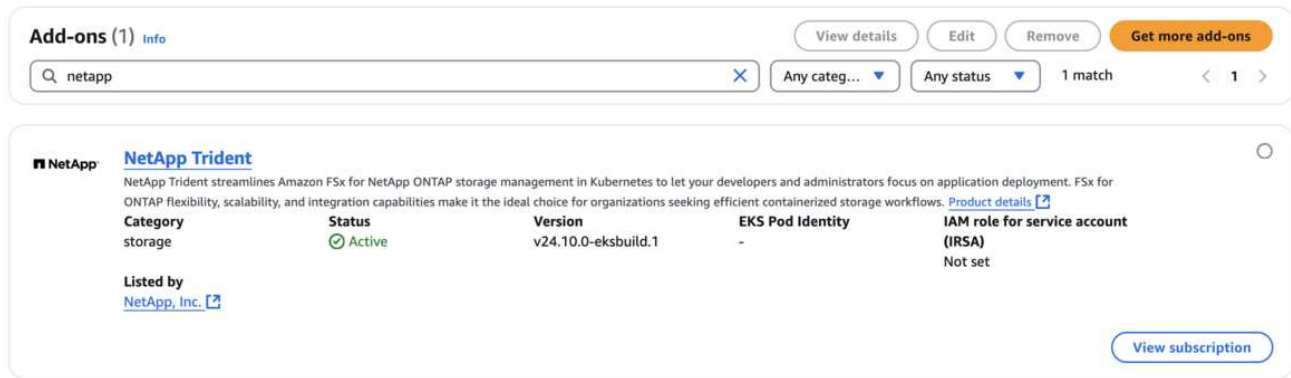
Add-on name	IAM role	Service account
No Pod Identity associations		
None of the selected add-on(s) have Pod Identity associations.		

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

7. Si estás usando IRSA (IAM roles para service account), consulta los pasos de configuración adicionales "aquí".

8. Selecciona **Crear**.

9. Verifica que el estado del complemento sea *Activo*.



10. Ejecuta el siguiente comando para verificar que Trident está instalado correctamente en el clúster:

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

11. Continúa con la configuración y configura el backend de almacenamiento. Para más información, consulta "[Configura el backend de almacenamiento](#)".

Instala o desinstala el complemento Trident EKS usando la CLI

Instala el complemento Trident EKS de NetApp usando la CLI:

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)
```

Desinstala el complemento Trident EKS de NetApp usando la CLI:

El siguiente comando desinstala el complemento Trident EKS:

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

Crea backends con kubectl

Un backend define la relación entre Trident y un sistema de almacenamiento. Le dice a Trident cómo comunicarse con ese sistema de almacenamiento y cómo Trident debe aprovisionar volúmenes desde él. Después de instalar Trident, el siguiente paso es crear un backend. La `TridentBackendConfig` Custom Resource Definition (CRD) te permite crear y administrar backends de Trident directamente a través de la interfaz de

Kubernetes. Puedes hacer esto usando `kubectl` o la herramienta CLI equivalente para tu distribución de Kubernetes.

TridentBackendConfig

`TridentBackendConfig` (`tbc`, `tbconfig`, `tbackendconfig`) es un CRD frontend con espacio de nombres que te permite administrar backends de Trident usando `kubectl`. Los administradores de Kubernetes y almacenamiento ahora pueden crear y administrar backends directamente a través de la CLI de Kubernetes sin necesitar una utilidad de línea de comandos dedicada (`tridentctl`).

Al crear un `TridentBackendConfig` objeto, sucede lo siguiente:

- Trident crea automáticamente un backend según la configuración que proporciones. Esto se representa internamente como un `TridentBackend` (`tbe`, `tridentbackend`) CR.
- El `TridentBackendConfig` está vinculado de forma única a un `TridentBackend` que fue creado por Trident.

Cada `TridentBackendConfig` mantiene una correspondencia uno a uno con un `TridentBackend`. El primero es la interfaz que se proporciona al usuario para diseñar y configurar backends; el segundo es la forma en que Trident representa el objeto backend real.

ADVERTENCIA

`TridentBackend`` Las CR se crean automáticamente por Trident. No deberías modificarlas. Si quieres actualizar los backends, hazlo modificando el objeto ``TridentBackendConfig`.

Mira el siguiente ejemplo para 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 puedes echar un vistazo a los ejemplos en el directorio ["trident-installer"](#) para ver configuraciones de muestra para la plataforma o servicio de almacenamiento que quieras.

El `spec` toma parámetros de configuración específicos del backend. En este ejemplo, el backend usa el `ontap-san` storage driver y usa los parámetros de configuración que se muestran aquí. Para la lista de opciones de configuración para tu storage driver deseado, consulta el ["Información de configuración del backend para tu controlador de almacenamiento"](#).

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

- `credentials`: Este parámetro es obligatorio y contiene las credenciales utilizadas para autenticarse con el sistema/servicio de almacenamiento. Esto se establece como un secreto de Kubernetes creado por el usuario. Las credenciales no se pueden pasar en texto sin formato y generarán un error.
- `deletionPolicy`: Este campo define qué debe suceder cuando se elimina el `TridentBackendConfig`. Puede tomar uno de dos valores posibles:
 - `delete`: Esto elimina tanto `TridentBackendConfig` CR como el backend asociado. Este es el valor predeterminado.
 - `retain`: Cuando se elimina una `TridentBackendConfig` CR, la definición del backend seguirá presente y se puede administrar con `tridentctl`. Configurar la política de eliminación en `retain` permite a los usuarios volver a una versión anterior (pre-21.04) y conservar los backends creados. El valor de este campo se puede actualizar después de que se cree una `TridentBackendConfig`.

NOTA

El nombre de un backend se establece usando `spec.backendName`. Si no se especifica, el nombre del backend se establece como el nombre del objeto `TridentBackendConfig` (`metadata.name`). Se recomienda establecer explícitamente los nombres de los backends usando `spec.backendName`.

CONSEJO

Los backends que fueron creados con `tridentctl` no tienen un objeto `TridentBackendConfig` asociado. Puedes elegir administrar esos backends con `kubectl` creando un CR `TridentBackendConfig`. Debes tener cuidado de especificar parámetros de configuración idénticos (como `spec.backendName`, `spec.storagePrefix`, `spec.storageDriverName` y así sucesivamente). Trident vinculará automáticamente el `TridentBackendConfig` recién creado con el backend preexistente.

Resumen de pasos

Para crear un nuevo backend usando `kubectl`, debes hacer lo siguiente:

1. Crea un "[Kubernetes Secret](#)". El secreto contiene las credenciales que Trident necesita para comunicarse con el clúster/servicio de almacenamiento.
2. Crea un `TridentBackendConfig` objeto. Esto contiene detalles sobre el clúster o servicio de almacenamiento y hace referencia al secreto creado en el paso anterior.

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

Paso 1: crea un secreto de Kubernetes

Crea un secreto que contenga las credenciales de acceso para el backend. Esto es único para cada servicio o plataforma de almacenamiento. Aquí tienes 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 los campos secretos de la plataforma de almacenamiento	Secreto	Descripción de los campos
Azure NetApp Files	clientID	El ID del cliente de un registro de app
Element (NetApp HCI/SolidFire)	Punto final	MVIP para el clúster SolidFire con credenciales de inquilino
ONTAP	nombre de usuario	Nombre de usuario para conectarse al clúster/SVM. Usada para la autenticación basada en credenciales
ONTAP	contraseña	Contraseña para conectarte al clúster/SVM. Usada para la autenticación basada en credenciales
ONTAP	clientPrivateKey	Valor codificado en Base64 de la clave privada del cliente. Usado para la autenticación basada en certificados
ONTAP	chapUsername	Nombre de usuario de entrada. Obligatorio si useCHAP=true. Para ontap-san y ontap-san-economy
ONTAP	chapInitiatorSecret	Secreto del iniciador de CHAP. Obligatorio si useCHAP=true. Para ontap-san y ontap-san-economy
ONTAP	chapTargetUsername	Nombre de usuario de destino. Obligatorio si useCHAP=true. Para ontap-san y ontap-san-economy
ONTAP	chapTargetInitiatorSecret	Secreto del iniciador de destino CHAP. Obligatorio si useCHAP=true. Para ontap-san y ontap-san-economy

El secreto creado en este paso se va a referenciar en el campo `spec.credentials` del objeto `TridentBackendConfig` que se crea en el siguiente paso.

Paso 2: crea el `TridentBackendConfig` CR

Ya estás listo para crear tu `TridentBackendConfig` CR. En este ejemplo, se crea un backend que usa el `ontap-san` driver mediante el objeto `TridentBackendConfig` que se muestra 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: verifica el estado de la `TridentBackendConfig` CR

Ahora que creaste la `TridentBackendConfig`CR`, puedes verificar el estado. Mira 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 creó exitosamente un backend y se vinculó al `TridentBackendConfig` CR.

La fase puede tomar uno de los siguientes valores:

- **Bound:** El `TridentBackendConfig` CR está asociado con un backend, y ese backend contiene `configRef` configurado con el `TridentBackendConfig` uid del CR.
- **Unbound:** Representado mediante `""`. El `TridentBackendConfig` objeto no está vinculado a un backend. Todos los nuevos `TridentBackendConfig` CR están en esta fase por defecto. Después de que la fase cambie, no puede volver a estar sin vincular.
- **Deleting:** El `TridentBackendConfig` CR `deletionPolicy` se configuró para eliminarse. Cuando el

TridentBackendConfig CR se elimina, pasa al estado de eliminación.

- Si no existen reclamos de volumen persistentes (PVC) en el backend, eliminar el TridentBackendConfig hará que Trident elimine el backend así como el TridentBackendConfig CR.
- Si hay una o más PVC en el backend, este pasa a un estado de eliminación. El TridentBackendConfig CR posteriormente también entra en fase de eliminación. El backend y TridentBackendConfig se eliminan solo después de que se eliminen todas las PVC.
- Lost: El backend asociado con el TridentBackendConfig CR se eliminó accidental o deliberadamente y el TridentBackendConfig CR todavía tiene una referencia al backend eliminado. El TridentBackendConfig CR todavía puede eliminarse independientemente del deletionPolicy valor.
- Unknown: Trident no puede determinar el estado ni la existencia del backend asociado con el TridentBackendConfig CR. Por ejemplo, si el servidor API no responde o si el tridentbackends.trident.netapp.io CRD falta. Esto podría requerir intervención.

En esta etapa, ¡el backend se ha creado correctamente! Hay varias operaciones que también se pueden gestionar, como ["actualizaciones y eliminaciones del backend"](#).

(Opcional) Paso 4: obtén más detalles

Puedes ejecutar el siguiente comando para obtener más información sobre tu backend:

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

NAME	BACKEND NAME	BACKEND UUID	
PHASE	STATUS	STORAGE DRIVER	DELETION POLICY
backend-tbc-ontap-san	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8	Bound Success ontap-san delete

Además, también puedes obtener un volcado YAML/JSON de TridentBackendConfig.

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

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  creationTimestamp: 2021-04-21T20:45:11Z
  finalizers:
    - trident.netapp.io
  generation: 1
  name: backend-tbc-ontap-san
  namespace: trident
  resourceVersion: "947143"
```

```

uid: 35b9d777-109f-43d5-8077-c74a4559d09c
spec:
  backendName: ontap-san-backend
  credentials:
    name: backend-tbc-ontap-san-secret
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  storageDriverName: ontap-san
  svm: trident_svm
  version: 1
status:
  backendInfo:
    backendName: ontap-san-backend
    backendUUID: 8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
  deletionPolicy: delete
  lastOperationStatus: Success
  message: Backend 'ontap-san-backend' created
  phase: Bound

```

backendInfo contiene el backendName y el backendUUID del backend que se creó en respuesta al TridentBackendConfig CR. El lastOperationStatus campo representa el estado de la última operación del TridentBackendConfig CR, que puede ser activada por el usuario (por ejemplo, si el usuario cambió algo en spec) o activada por Trident (por ejemplo, durante reinicios de Trident). Puede ser Success o Failed. phase representa el estado de la relación entre el TridentBackendConfig CR y el backend. En el ejemplo anterior, phase tiene el valor Bound, lo que significa que el TridentBackendConfig CR está asociado con el backend.

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

ADVERTENCIA

No puedes actualizar ni eliminar un backend que contenga un objeto asociado TridentBackendConfig usando `tridentctl`. Para entender los pasos para cambiar entre `tridentctl` y `TridentBackendConfig`, ["ver aquí"](#).

Gestiona backends

Gestiona los backends de Trident con kubectl

Conoce cómo realizar operaciones de gestión de backend usando `kubectl`.

Eliminar un backend

Al eliminar un `TridentBackendConfig`, le indicas a Trident que elimine o conserve los backends (según `deletionPolicy`). Para eliminar un backend, asegúrate de que `deletionPolicy` esté configurado para eliminar. Para eliminar solo el `TridentBackendConfig`, asegúrate de que `deletionPolicy` esté configurado para conservar. Esto asegura que el backend siga presente y se pueda administrar usando `tridentctl`.

Ejecuta 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. Debes tener cuidado al eliminar secretos. Solo deberías eliminar secretos si no están en uso por los backends.

Ver los backends existentes

Ejecuta el siguiente comando:

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

También puedes ejecutar `tridentctl get backend -n trident` o `tridentctl get backend -o yaml -n trident` para obtener una lista de todos los backends que existen. Esta lista también incluirá los backends que fueron creados con `tridentctl`.

Actualizar un backend

Puede haber varias razones para actualizar un backend:

- Las credenciales del sistema de almacenamiento han cambiado. Para actualizar las credenciales, se debe actualizar el secreto de Kubernetes que se usa en el objeto `TridentBackendConfig`. Trident actualizará automáticamente el backend con las credenciales más recientes proporcionadas. Ejecuta el siguiente comando para actualizar el secreto de Kubernetes:

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

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

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

- Alternativamente, puedes hacer cambios en el `TridentBackendConfig` CR existente usando el siguiente comando:

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

NOTA

- Si falla una actualización del backend, este sigue en su última configuración conocida. Puedes 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, puedes volver a ejecutar el comando de actualización.

Gestiona los backends de Trident con tridentctl

Conoce cómo realizar operaciones de gestión de backend usando `tridentctl`.

Crear un backend

Después de crear un "archivo de configuración backend", ejecuta el siguiente comando:

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

Si falla la creación del backend, algo estaba mal con la configuración del backend. Puedes 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 puedes ejecutar el comando `create` otra vez.

Eliminar un backend

Para eliminar un backend de Trident, haz lo siguiente:

1. Recupera el nombre del backend:

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

2. Elimina el backend:

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

NOTA

Si Trident ha aprovisionado volúmenes e instantáneas de este backend que aún existen, eliminar el backend impide que se aprovisionen nuevos volúmenes desde él. El backend seguirá existiendo en estado "Eliminando".

Ver los backends existentes

Para ver los backends que Trident conoce, haz lo siguiente:

- Para obtener un resumen, ejecuta el siguiente comando:

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

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

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

Actualizar un backend

Después de crear un nuevo archivo de configuración de backend, ejecuta el siguiente comando:

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

Si la actualización del backend falla, algo salió mal con la configuración del backend o intentaste una actualización no válida. Puedes 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 puedes ejecutar el comando `update` otra vez.

Identifica las clases de almacenamiento que usan un backend

Este es un ejemplo del tipo de preguntas que puedes responder con el JSON que `tridentctl` genera para los objetos backend. Esto usa la utilidad `jq`, que necesitas instalar.

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

Esto también se aplica a los backends que se crearon usando `TridentBackendConfig`.

Elige un método de gestión del backend de Trident

Conoce las diferentes formas de administrar backends en Trident.

Opciones para gestionar backends

Con la introducción de `TridentBackendConfig`, los administradores ahora tienen dos formas únicas de gestionar los backends. Esto plantea las siguientes preguntas:

- ¿Se pueden gestionar los backends creados usando `tridentctl` con `TridentBackendConfig`?
- ¿Se pueden gestionar los backends creados usando `TridentBackendConfig` mediante `tridentctl`?

Administra `tridentctl` backends usando `TridentBackendConfig`

Esta sección cubre los pasos necesarios para administrar backends que se crearon usando `tridentctl` directamente a través de la interfaz de Kubernetes creando `TridentBackendConfig` objetos.

Esto se aplicará a los siguientes escenarios:

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

En ambos escenarios, los backends seguirán presentes, con Trident programando los volúmenes y operando sobre ellos. Aquí los administradores tienen dos opciones:

- Sigue usando `tridentctl` para administrar los backends que se crearon con él.
- Vincula los backends creados usando `tridentctl` un nuevo `TridentBackendConfig` objeto. Hacer esto significa que los backends se gestionarán usando `kubectrl` y no `tridentctl`.

Para administrar un backend preexistente usando `kubectrl`, necesitarás crear un `TridentBackendConfig` que se vincule al backend existente. Aquí tienes un resumen de cómo funciona:

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

Paso 0: identifica el backend

Para crear un `TridentBackendConfig` que se vincule a un backend existente, necesitas obtener la configuración del backend. En este ejemplo, supongamos que se creó un backend usando 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: crea un secreto de Kubernetes

Crea un secreto que contenga las credenciales para el backend, 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: crea un `TridentBackendConfig` CR

El siguiente paso es crear una `TridentBackendConfig` CR que se vincule automáticamente con la preexistente `ontap-nas-backend` (como en este ejemplo). Asegúrate de que se cumplan los siguientes requisitos:

- El mismo nombre de backend 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 backend original.
- Las credenciales se proporcionan a través de un Kubernetes Secret y no en texto sin formato.

En este caso, el `TridentBackendConfig` se verá así:

```
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: mysqldb
  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: verifica el estado de la `TridentBackendConfig` CR

Después de que el TridentBackendConfig haya sido creado, su fase debe ser Bound. También debe reflejar el mismo nombre de backend y UUID que el backend existente.

```

kubectl get tbc tbc-ontap-nas-backend -n trident

```

NAME	BACKEND NAME	BACKEND UUID
PHASE STATUS		
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          |
| STATE  | VOLUMES |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-nas-backend      | ontap-nas      | 52f2eb10-e4c6-4160-99fc-
96b3be5ab5d7 | online |          25 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

Ahora el backend se va a administrar completamente usando el `tbc-ontap-nas-backend TridentBackendConfig` objeto.

Administra `TridentBackendConfig` backends usando `tridentctl`

`tridentctl` se puede usar para listar los backends que fueron creados usando `TridentBackendConfig`. Además, los administradores también pueden elegir administrar completamente dichos backends a través de `tridentctl` eliminando `TridentBackendConfig` y asegurándose de que `spec.deletionPolicy` esté configurado como `retain`.

Paso 0: identifica el backend

Por ejemplo, supongamos que el siguiente backend se creó usando `TridentBackendConfig`:

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME          BACKEND UUID
PHASE  STATUS  STORAGE DRIVER  DELETION POLICY
backend-tbc-ontap-san  ontap-san-backend    81abcb27-ea63-49bb-b606-
0a5315ac5f82  Bound  Success  ontap-san          delete

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE  | VOLUMES |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend      | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |          33 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

Desde la salida, se puede ver que `TridentBackendConfig` fue creado exitosamente y está vinculado a un backend [observa el UUID del backend].

Paso 1: confirma que `deletionPolicy` esté configurado en `retain`

Echemos un vistazo al valor de `deletionPolicy`. Esto debe configurarse en `retain`. Esto asegura que cuando se elimina una CR de `TridentBackendConfig`, la definición del backend seguirá presente y podrás gestionarla con `tridentctl`.

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME          BACKEND UUID
PHASE    STATUS    STORAGE DRIVER    DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-0a5315ac5f82    Bound    Success    ontap-san    delete

# Patch value of deletionPolicy to retain
kubectl patch tbc backend-tbc-ontap-san --type=merge -p
'{"spec":{"deletionPolicy":"retain"}}' -n trident
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-san patched

#Confirm the value of deletionPolicy
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME          BACKEND UUID
PHASE    STATUS    STORAGE DRIVER    DELETION POLICY
backend-tbc-ontap-san    ontap-san-backend    81abcb27-ea63-49bb-b606-0a5315ac5f82    Bound    Success    ontap-san    retain
```

NOTA

No sigas con el siguiente paso a menos que `deletionPolicy` esté configurado en `retain`.

Paso 2: elimina el `TridentBackendConfig` CR

El último paso es eliminar el `TridentBackendConfig` CR. Después de confirmar que el `deletionPolicy` está configurado como `retain`, puedes continuar con la eliminación:

```
kubectl delete tbc backend-tbc-ontap-san -n trident
tridentbackendconfig.trident.netapp.io "backend-tbc-ontap-san" deleted

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|      NAME      | STORAGE DRIVER |                               UUID                               |
| STATE  | VOLUMES |                               |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-0a5315ac5f82 |
| online  |      33  |                               |
```

```
+-----+-----  
+-----+-----+-----+
```

Al eliminar el `TridentBackendConfig` objeto, Trident simplemente lo elimina sin eliminar realmente el backend en sí.

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.