



# Configurar los back-ends

## Astra Trident

NetApp  
April 04, 2024

# Tabla de contenidos

- Configurar los back-ends ..... 1
  - Configurar los back-ends ..... 1
  - Azure NetApp Files ..... 1
  - Configure un back-end de Cloud Volumes Service para Google Cloud ..... 13
  - Configure un back-end de NetApp HCI o SolidFire ..... 30
- Controladores para SAN de ONTAP ..... 37
- Unidades NAS de ONTAP ..... 59
- Amazon FSX para ONTAP de NetApp ..... 89

# Configurar los back-ends

## Configurar los back-ends

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

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

- ["Configure un back-end de Azure NetApp Files"](#)
- ["Configure un back-end de Cloud Volumes Service para Google Cloud Platform"](#)
- ["Configure un back-end de NetApp HCI o SolidFire"](#)
- ["Configure un back-end con controladores NAS ONTAP o Cloud Volumes ONTAP"](#)
- ["Configurar un back-end con controladores SAN ONTAP o Cloud Volumes ONTAP"](#)
- ["Utilice Astra Trident con Amazon FSX para ONTAP de NetApp"](#)

## Azure NetApp Files

### Configure un back-end de Azure NetApp Files

Puede configurar Azure NetApp Files (ANF) como back-end de Astra Trident. Puede asociar volúmenes de NFS y SMB con un back-end de ANF.

#### Consideraciones

- El servicio Azure NetApp Files no admite volúmenes de menos de 100 GB. Astra Trident crea automáticamente volúmenes de 100 GB si se solicita un volumen más pequeño.
- Astra Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.

### Prepárese para configurar un back-end de Azure NetApp Files

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

#### Requisitos previos para volúmenes NFS y SMB



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

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

- Un pool de capacidad. Consulte ["Microsoft: Cree un pool de capacidad para Azure NetApp Files"](#).

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

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

```

```

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

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

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/GetMetadata/action",

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

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

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

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

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

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

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

```

- Azure location que contiene al menos uno ["subred delegada"](#). A partir de Trident 22.01, la location parámetro es un campo obligatorio en el nivel superior del archivo de configuración del back-end. Los valores de ubicación especificados en los pools virtuales se ignoran.

## Requisitos adicionales para volúmenes SMB

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

- Active Directory configurado y conectado a Azure NetApp Files. Consulte ["Microsoft: Cree y gestione conexiones de Active Directory para Azure NetApp Files"](#).
- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2019. Astra Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto de Astra Trident que contiene sus credenciales de Active Directory para que Azure NetApp Files pueda autenticarse en Active Directory. Generar secreto smbcreds:

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

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

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

Obtenga más información acerca de las opciones de configuración de back-end de NFS y SMB para ANF y revise ejemplos de configuración.

### Opciones de configuración del back-end

Astra Trident utiliza la configuración de back-end (subred, red virtual, nivel de servicio y ubicación) para crear volúmenes ANF en pools de capacidad disponibles en la ubicación solicitada y que coincidan con el nivel de servicio y la subred solicitados.



Astra Trident no admite pools de capacidad de calidad de servicio manual.

Los back-ends DE ANF proporcionan estas opciones de configuración.

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	"azure-netapp-files"
<code>backendName</code>	Nombre personalizado o el back-end de almacenamiento	Nombre del controlador + "_" + caracteres aleatorios
<code>subscriptionID</code>	El ID de suscripción de su suscripción de Azure	
<code>tenantID</code>	El ID de inquilino de un registro de aplicación	
<code>clientID</code>	El ID de cliente de un registro de aplicación	

Parámetro	Descripción	Predeterminado
<code>clientSecret</code>	El secreto de cliente de un registro de aplicaciones	
<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	
<code>resourceGroups</code>	Lista de grupos de recursos para filtrar los recursos detectados	[] (sin filtro)
<code>netappAccounts</code>	Lista de cuentas de NetApp para filtrar los recursos detectados	[] (sin filtro)
<code>capacityPools</code>	Lista de pools de capacidad para filtrar los recursos detectados	[] (sin filtro, aleatorio)
<code>virtualNetwork</code>	Nombre de una red virtual con una subred delegada	""
<code>subnet</code>	Nombre de una subred delegada a. Microsoft.Netapp/volumes	""
<code>networkFeatures</code>	<p>Puede que el conjunto de funciones de vnet para un volumen sea Basic o. Standard.</p> <p>Las funciones de red no están disponibles en todas las regiones y es posible que tengan que activarse en una suscripción. Especificando <code>networkFeatures</code> cuando la funcionalidad no está habilitada, hace que no se pueda realizar el aprovisionamiento del volumen.</p>	""
<code>nfsMountOptions</code>	<p>Control preciso de las opciones de montaje NFS.</p> <p>Ignorada para volúmenes de SMB.</p> <p>Para montar volúmenes con NFS versión 4.1, incluya <code>nfsvers=4</code> En la lista de opciones de montaje delimitadas por comas para elegir NFS v4.1.</p> <p>Las opciones de montaje establecidas en una definición de clase de almacenamiento anulan las opciones de montaje establecidas en la configuración de back-end.</p>	"nfsvers=3"

Parámetro	Descripción	Predeterminado
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo: <code>\{"api": false, "method": true, "discovery": true\}</code> . No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo
nasType	Configure la creación de volúmenes NFS o SMB.  Las opciones son <code>nfs</code> , <code>smb</code> o <code>nulo</code> . El valor predeterminado es <code>nulo</code> en volúmenes de NFS.	<code>nfs</code>



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

#### Permisos y recursos necesarios

Si recibe un error que indica que no se han encontrado pools de capacidad al crear un PVC, es probable que el registro de aplicaciones no tenga asociados los permisos y recursos necesarios (subred, red virtual o pool de capacidad). Si la depuración está habilitada, Astra Trident registrará los recursos de Azure detectados cuando se cree el back-end. Compruebe que se está utilizando un rol adecuado.

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

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

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

#### Aprovisionamiento de volúmenes

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



detalles.

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

## Configuraciones de ejemplo

### Ejemplo 1: Configuración mínima

Ésta es la configuración mínima absoluta del back-end. Con esta configuración, Astra Trident descubre todas sus cuentas, pools de capacidad y subredes de NetApp delegadas en ANF en la ubicación configurada, y coloca nuevos volúmenes en uno de estos pools y subredes de forma aleatoria. Porque `nasType` se omite, la `nfs` El valor predeterminado es aplicable, y el back-end aprovisionará para volúmenes NFS.

Esta configuración es ideal cuando simplemente va a empezar con ANF e intentar cosas, pero en la práctica va a querer proporcionar un ámbito adicional para los volúmenes que debe aprovisionar.

```
---
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
```

## Ejemplo 2: Configuración específica de nivel de servicio con filtros de pool de capacidad

Esta configuración de back-end coloca volúmenes en las de Azure `eastus` ubicación en una `Ultra` pool de capacidad. Astra Trident descubre automáticamente todas las subredes delegadas a ANF en esa ubicación y coloca un nuevo volumen en una de ellas de forma aleatoria.

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

### Ejemplo 3: Configuración avanzada

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

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

## Ejemplo 4: Configuración de pool virtual

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

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

## Definiciones de clase de almacenamiento

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

### Definiciones de ejemplo mediante `parameter.selector` campo

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

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

### Definiciones de ejemplo de volúmenes SMB

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

### Ejemplo 1: Configuración básica del 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"
```

### Ejemplo 2: Uso de distintos 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}
```

### Ejemplo 3: Uso de distintos secretos por volumen

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



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

## Cree el back-end

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

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

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

```
tridentctl logs
```

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

## Configure un back-end de Cloud Volumes Service para Google Cloud

Descubra cómo configurar Cloud Volumes Service de NetApp para Google Cloud como back-end para su instalación de Astra Trident con las configuraciones de ejemplo proporcionadas.

### Obtenga más información sobre la compatibilidad de Astra Trident con Cloud Volumes Service para Google Cloud

Astra Trident puede crear volúmenes de Cloud Volumes Service en uno de dos ["tipos de servicio"](#):

- **CVS-Performance:** El tipo de servicio predeterminado Astra Trident. Este tipo de servicio optimizado para el rendimiento es más adecuado para cargas de trabajo de producción que valoran el rendimiento. El tipo de servicio CVS-Performance es una opción de hardware que admite volúmenes con un tamaño mínimo de 100 GiB. Puede elegir uno de ["tres niveles de servicio"](#):
  - standard
  - premium
  - extreme
- **CVS:** El tipo de servicio CVS proporciona una alta disponibilidad zonal con niveles de rendimiento limitados a moderados. El tipo de servicio CVS es una opción de software que usa pools de almacenamiento para admitir volúmenes de solo 1 GiB. El pool de almacenamiento puede contener hasta 50 volúmenes en los que todos los volúmenes comparten la capacidad y el rendimiento del pool. Puede elegir uno de ["dos niveles de servicio"](#):
  - standardsw
  - zoneredundantstandardsw

## Lo que necesitará

Para configurar y usar el "Cloud Volumes Service para Google Cloud" back-end, necesita lo siguiente:

- Una cuenta de Google Cloud configurada con Cloud Volumes Service de NetApp
- Número de proyecto de su cuenta de Google Cloud
- Cuenta de servicio de Google Cloud con el `netappcloudvolumes.admin` función
- Archivo de claves API para la cuenta de Cloud Volumes Service

## Opciones de configuración del back-end

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

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	"gcp-cvs"
<code>backendName</code>	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + "_" + parte de la clave de API
<code>storageClass</code>	Parámetro opcional utilizado para especificar el tipo de servicio CVS.  Uso <code>software</code> Para seleccionar el tipo de servicio CVS. De lo contrario, Astra Trident asume el tipo de servicio CVS-Performance ( <code>hardware</code> ).	
<code>storagePools</code>	Solo tipo de servicio CVS. Parámetro opcional que se utiliza para especificar pools de almacenamiento para la creación del volumen.	
<code>projectNumber</code>	Número de proyecto de cuenta de Google Cloud. El valor está disponible en la página de inicio del portal de Google Cloud.	
<code>hostProjectNumber</code>	Se requiere si se utiliza una red VPC compartida. En este escenario, <code>projectNumber</code> es el proyecto de servicio, y <code>hostProjectNumber</code> es el proyecto anfitrión.	



Parámetro	Descripción	Predeterminado
apiRegion	<p>Región de Google Cloud en la que Astra Trident crea volúmenes de Cloud Volumes Service. Cuando se crean clústeres de Kubernetes de diversas regiones, se crean volúmenes en un apiRegion Se puede utilizar en cargas de trabajo programadas en nodos en varias regiones de Google Cloud.</p> <p>El tráfico entre regiones conlleva un coste adicional.</p>	
apiKey	<p>Clave de API para la cuenta de servicio de Google Cloud con el netappcloudvolumes.admin función.</p> <p>Incluye el contenido en formato JSON del archivo de clave privada de una cuenta de servicio de Google Cloud (copiado literal en el archivo de configuración de back-end).</p>	
proxyURL	<p>URL de proxy si se requiere servidor proxy para conectarse a la cuenta CVS. El servidor proxy puede ser un proxy HTTP o HTTPS.</p> <p>En el caso de un proxy HTTPS, se omite la validación de certificados para permitir el uso de certificados autofirmados en el servidor proxy.</p> <p>No se admiten los servidores proxy con autenticación habilitada.</p>	
nfsMountOptions	Control preciso de las opciones de montaje NFS.	"nfsvers=3"
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor.	"" (no se aplica de forma predeterminada)

Parámetro	Descripción	Predeterminado
serviceLevel	<p>El nivel de servicio CVS-Performance o CVS para nuevos volúmenes.</p> <p>Los valores de CVS-Performance son standard, premium, o. extreme.</p> <p>Los valores CVS son standardsw o. zoneredundantstandardsw.</p>	<p>El valor predeterminado de CVS-Performance es "estándar".</p> <p>El valor predeterminado de CVS es "standardsw".</p>
network	Se utiliza la red de Google Cloud para Cloud Volumes Service Volumes.	"predeterminado"
debugTraceFlags	<p>Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo:</p> <pre>\{"api":false, "method":true}.</pre> <p>No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.</p>	nulo
allowedTopologies	<p>Para habilitar el acceso a varias regiones, se debe definir StorageClass para allowedTopologies debe incluir todas las regiones.</p> <p>Por ejemplo:</p> <pre>- key: topology.kubernetes.io/reg ion values: - us-east1 - europe-west1</pre>	

## Opciones de aprovisionamiento de volúmenes

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

Parámetro	Descripción	Predeterminado
exportRule	Las reglas de exportación de nuevos volúmenes. Debe ser una lista separada por comas con cualquier combinación de direcciones IPv4 o subredes IPv4 en notación CIDR.	"0.0.0.0/0"

Parámetro	Descripción	Predeterminado
snapshotDir	Acceso a la .snapshot directorio	"falso"
snapshotReserve	Porcentaje de volumen reservado para las Snapshot	"" (Aceptar CVS por defecto de 0)
size	El tamaño de los volúmenes nuevos.  CVS-Performance mínimo es 100 GIB.  El mínimo de CVS es 1 GIB.	El tipo de servicio CVS-Performance se establece de manera predeterminada en "100GIB".  El tipo de servicio CVS no establece un valor predeterminado, pero requiere un mínimo de 1 GIB.

## Ejemplos de tipo de servicio CVS-Performance

Los siguientes ejemplos proporcionan ejemplos de configuraciones para el tipo de servicio CVS-Performance.

## Ejemplo 1: Configuración mínima

Esta es la configuración de back-end mínima usando el tipo de servicio CVS-Performance predeterminado con el nivel de servicio "estándar" predeterminado.

```
---  
version: 1  
storageDriverName: gcp-cvs  
projectNumber: '012345678901'  
apiRegion: us-west2  
apiKey:  
  type: service_account  
  project_id: my-gcp-project  
  private_key_id: "<id_value>"  
  private_key: |  
    -----BEGIN PRIVATE KEY-----  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m  
    XsYg6gyxy4zq70lwWgLwGa==  
    -----END PRIVATE KEY-----  
  client_email: cloudvolumes-admin-sa@my-gcp-  
  project.iam.gserviceaccount.com  
  client_id: '123456789012345678901'
```

```
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/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
```

## Ejemplo 2: Configuración de nivel de servicio

Este ejemplo muestra las opciones de configuración del back-end, incluidos el nivel de servicio y los valores predeterminados de volumen.

```
---  
version: 1  
storageDriverName: gcp-cvs  
projectNumber: '012345678901'  
apiRegion: us-west2  
apiKey:  
  type: service_account  
  project_id: my-gcp-project  
  private_key_id: "<id_value>"  
  private_key: |  
    -----BEGIN PRIVATE KEY-----  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3b1/qp8B4Kws8zX5ojY9m  
    XsYg6gyxy4zq70lwWgLwGa==  
    -----END PRIVATE KEY-----  
  client_email: cloudvolumes-admin-sa@my-gcp-  
  project.iam.gserviceaccount.com  
  client_id: '123456789012345678901'
```

```
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/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
proxyURL: http://proxy-server-hostname/
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 10Ti
serviceLevel: premium
defaults:
  snapshotDir: 'true'
  snapshotReserve: '5'
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  size: 5Ti
```





```

znHczZsrtrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
XsYg6gyxy4zq7OlwWgLwGa==
-----END PRIVATE KEY-----
client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
client_id: '123456789012345678901'
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/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
nfsMountOptions: vers=3,proto=tcp,timeo=600
defaults:
  snapshotReserve: '5'
  exportRule: 0.0.0.0/0
labels:
  cloud: gcp
  region: us-west2
storage:
- labels:
  performance: extreme
  protection: extra
  serviceLevel: extreme
  defaults:
  snapshotDir: 'true'
  snapshotReserve: '10'
  exportRule: 10.0.0.0/24
- labels:
  performance: extreme
  protection: standard
  serviceLevel: extreme
- labels:
  performance: premium
  protection: extra
  serviceLevel: premium
  defaults:
  snapshotDir: 'true'
  snapshotReserve: '10'
- labels:
  performance: premium
  protection: standard
  serviceLevel: premium
- labels:
  performance: standard

```

```
serviceLevel: standard
```

### **Definiciones de clases de almacenamiento**

Las siguientes definiciones de StorageClass se aplican al ejemplo de configuración de pool virtual. Uso `parameters.selector`, Puede especificar para cada clase de almacenamiento el pool virtual utilizado para alojar un volumen. Los aspectos definidos en el pool elegido serán el volumen.

## Ejemplo de clase de almacenamiento

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=extreme; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-standard-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-standard
provisioner: netapp.io/trident
parameters:
  selector: "performance=standard"
allowVolumeExpansion: true
```

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "protection=extra"
allowVolumeExpansion: true
```

- El primer tipo de almacenamiento (`cvs-extreme-extra-protection`) se asigna al primer grupo virtual. Se trata del único pool que ofrece un rendimiento extremo con una reserva Snapshot del 10%.
- El último tipo de almacenamiento (`cvs-extra-protection`) llama a cualquier agrupación de almacenamiento que ofrezca una reserva de instantáneas del 10%. Astra Trident decide qué pool virtual se selecciona y garantiza que se cumpla el requisito de reserva de Snapshot.

## Ejemplos de tipo de servicio CVS

Los siguientes ejemplos proporcionan configuraciones de ejemplo para el tipo de servicio CVS.

## Ejemplo 1: Configuración mínima

Esta es la configuración mínima del back-end mediante `storageClass` Para especificar el tipo de servicio CVS y el valor predeterminado `standardsw` nivel de servicio.

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
storageClass: software
apiRegion: us-east4
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    znHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m
    XsYg6gyxy4zq70lwWgLwGa==
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@my-gcp-
    project.iam.gserviceaccount.com
```

```
client_id: '123456789012345678901'  
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/cloudvolumes-admin-  
sa%40my-gcp-project.iam.gserviceaccount.com  
serviceLevel: standardsw
```

## Ejemplo 2: Configuración del pool de almacenamiento

Esta configuración de entorno de administración de ejemplo utiliza `storagePools` para configurar un pool de almacenamiento.

```
---
version: 1
storageDriverName: gcp-cvs
backendName: gcp-std-so-with-pool
projectNumber: '531265380079'
apiRegion: europe-west1
apiKey:
  type: service_account
  project_id: cloud-native-data
  private_key_id: "<id_value>"
  private_key: |-
    -----BEGIN PRIVATE KEY-----
    MIIEvAIBADANBgkqhkiG9w0BAQEFAASCbKwggSiAgEAAoIBAQDaT+Oui9FBAw19
    L1AGEkrYU5xd9K5NlO5jMkIFND5wCD+Nv+jd1GvtFRLaLK5RvXyF5wzvztmODNS+
    qtScpQ+5cFpQkuGtv9U9+N6qtuVYYO3b504Kp5CtqVPJCgMJaK2j8pZTIqUiMum/
    5/Y9oTbZrjAHSMsgJm2nHzFq2X0rqVMAHghI6ATm4DOuWx8XGWKGTGIPlc0qPqJlqS
    LLaWOH4VIZQZCAyW5IU99CAMwqHgdG0uhFNfCgMmED6PBUvVLsLvcq86X+QSWR9k
    ETqElj/sGCenPF7ti1DhGBFafd9hPnxg9PZY29ArEZwY9G/ZjZQX7WPgs0VvxiNR
    DxZRC3GXAgMBAECggEACn5c59bG/qnVEVI1CwMAalM5M2z09JFh1L1ljKwntNPj
    Vilw2eTW2+UE7HbJru/S7KQgA5Dnn9kvCraEahPRuddUMrD0vG4kTl/IODV6uFuk
    Y0sZfbqd4jMUQ21smvGsqFzwloYWS5qzO1W83ivXH/HW/iqkmY2eW+EPRS/hwSSu
    SscR+Soji7PB0BWSJhlV4yqYf3vcd/D95el2CVHfRCkL85DKumeZ+yHENpiXGZAE
    t8xSs4a500Pm6NHhevCw2a/UQ95/foXNUR450HtbjieJo5o+FF6EYZQGfU2ZHZO8
    37FBKuaJkdGW5xqaI9TL7aqkGkFMF4F2qvOZM+vy8QKBgQD4oVuOkJDlhkTHP86W
    esFlw1kpWyJR9ZA7LI0g/rVpslnX+XdDq0WQf4umdLNau5hYEH9LU6ZSGs1Xk3/B
    NHwR6OXFuqEKNiu83d0zSlHhTy7PZpOZdj5a/vVvQfPDMz7OvsqLRd7YCAbdzuQ0
    +Ahq0Ztwvg0HQ64hdW0ukpYRRwKBgQDgyHj98oqswoYuIa+pPlyS0pPwLmjwKyNm
    /HayzCp+Qjiiyy7Tzg8AUqlH1Ou83XbV428jvg7kDhO7PCCKFq+mMmfqHmTpb0Maq
    KpKnZg4ipsqPlyHNNNEoRmcailXbwIhCLewMqMrggUiLOmCw4PscL5nK+4GKu2XE1
    jLqjWAZFMQKBgFHkQ9XXRAJ1kR3XpGHOgn890pZOkCVSrqju6aUef/5KY1FCt8ew
    F/+aIxM2iQsvmWQYOvVCnhuY/F2GfAQ7d0om3decuwI0CX/xy7PjHmLXa2uaZs4
    WR17sLduj62RqXRLX0c0QkwBiNFyHbRcpdkZJQujbyMhBa+7j7SxT4BtAoGAWMWT
    UucocRXZm/pdvz9wteNH3YDwnJLMxm1KC06qMXbBoYrliY4sm3ywJWMC+iCd/H8A
    Gecxd/xVu5mA2L2N3KMq18Zhz8Th0G5DwKyDRJgOQ0Q46yuNXOoYEjlo4Wjyk8Me
    +tlQ8iK98E0UmZnhTgfsSpSNElbz2AqnzQ3MN9uECgYAqdvvdVPnKGFvdtZ2DjyMoJ
    E89UIC41WjjJGmHsd8W65+3X0RwMzKMT6aZc5tK9J5dHvmWIETnbM+1TImdBbFga
    NWOC6f3r2xbGXHhaWSl+nobpTuvlo56ZRJVvVk7lFMsiddzMuHH8pxfgNjemwA4P
    ThDHcejv035NNV6Kyo00tA==
    -----END PRIVATE KEY-----
  client_email: cloudvolumes-admin-sa@cloud-native-
  data.iam.gserviceaccount.com
```

```
client_id: '107071413297115343396'  
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/cloudvolumes-admin-  
sa%40cloud-native-data.iam.gserviceaccount.com  
storageClass: software  
zone: europe-west1-b  
network: default  
storagePools:  
- 1bc7f380-3314-6005-45e9-c7dc8c2d7509  
serviceLevel: Standardsw
```

## El futuro

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

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

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

```
tridentctl logs
```

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

## Configure un back-end de NetApp HCI o SolidFire

Descubra cómo crear y usar un back-end de Element con su instalación de Astra Trident.

### Antes de empezar

Necesitarás lo siguiente antes de crear un backend de elemento.

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



## Modos de volumen

La `solidfire-san` el controlador de almacenamiento admite ambos modos de volumen: archivo y bloque. Para la `Filesystem VolumeMode`, Astra Trident crea un volumen y crea un sistema de archivos. El tipo de sistema de archivos se especifica mediante `StorageClass`.

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



Astra Trident utiliza CHAP cuando funciona como un proveedor CSI mejorado. Si está utilizando CHAP (que es el valor predeterminado para CSI), no es necesario realizar ninguna otra preparación. Se recomienda establecer explícitamente el `UseCHAP` Opción para utilizar CHAP con Trident que no sea CSI. De lo contrario, consulte ["aquí"](#).



Los grupos de acceso de volúmenes solo son compatibles con el marco convencional que no es CSI para Astra Trident. Cuando se configura para funcionar en el modo CSI, Astra Trident utiliza CHAP.

Si ninguno `AccessGroups` o `UseCHAP` están definidas, se aplica una de las siguientes reglas:

- Si es el valor predeterminado `trident` se ha detectado el grupo de acceso; se utilizan los grupos de acceso.
- Si no se detecta ningún grupo de acceso y la versión de Kubernetes es 1.7 o posterior, se utiliza CHAP.

## Opciones de configuración del back-end

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

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	Siempre "solidfire-san"
<code>backendName</code>	Nombre personalizado o el back-end de almacenamiento	Dirección IP "SolidFire_" + almacenamiento (iSCSI)

Parámetro	Descripción	Predeterminado
Endpoint	MVIP para el clúster de SolidFire con credenciales de inquilino	
SVIP	La dirección IP y el puerto de almacenamiento (iSCSI)	
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes.	""
TenantName	Nombre de inquilino que se va a usar (creado si no se encuentra)	
InitiatorIFace	Restringir el tráfico de iSCSI a una interfaz de host específica	"predeterminado"
UseCHAP	Utilice CHAP para la autenticación de iSCSI	verdadero
AccessGroups	Lista de ID de grupos de acceso que se van a usar	Busca el código de un grupo de acceso denominado "trident".
Types	Especificaciones de calidad de servicio	
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}	nulo



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

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

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

```

---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: "<svip>:3260"
TenantName: "<tenant>"
labels:
  k8scluster: dev1
  backend: dev1-element-cluster
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000

```

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

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

Astra Trident copia las etiquetas presentes en un pool de almacenamiento a la LUN de almacenamiento del entorno de administración al aprovisionar. Para mayor comodidad, los administradores de almacenamiento pueden definir etiquetas por pool virtual y agrupar volúmenes por etiqueta.

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

```

---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0

```

```

SVIP: "<svip>:3260"
TenantName: "<tenant>"
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
type: Silver
labels:
  store: solidfire
  k8scluster: dev-1-cluster
region: us-east-1
storage:
- labels:
  performance: gold
  cost: '4'
  zone: us-east-1a
  type: Gold
- labels:
  performance: silver
  cost: '3'
  zone: us-east-1b
  type: Silver
- labels:
  performance: bronze
  cost: '2'
  zone: us-east-1c
  type: Bronze
- labels:
  performance: silver
  cost: '1'
  zone: us-east-1d

```

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

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

El primer tipo de almacenamiento (`solidfire-gold-four`) se asignará al primer grupo virtual. Este es el único pool que ofrece rendimiento de oro con un `Volume Type QoS` De oro. El último tipo de almacenamiento (`solidfire-silver`) llama a cualquier pool de almacenamiento que ofrezca un rendimiento elevado. Astra Trident decidirá qué pool virtual se selecciona y garantizará que se cumplan los requisitos de almacenamiento.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-gold-four
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold; cost=4"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-three
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=3"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-bronze-two
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze; cost=2"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-one
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=1"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
  fsType: "ext4"
```

## Obtenga más información

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

# Controladores para SAN de ONTAP

## Información general del controlador de SAN de ONTAP

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

## Información importante sobre los controladores de SAN de ONTAP

Astra Control proporciona una protección fluida, recuperación ante desastres y movilidad (mover volúmenes entre clústeres de Kubernetes) para los volúmenes creados con el `ontap-nas`, `ontap-nas-flexgroup`, y `ontap-san` de windows Consulte ["Requisitos previos de replicación de Astra Control"](#) para obtener más detalles.

- Debe usar `ontap-nas` para cargas de trabajo de producción que requieren protección de datos, recuperación ante desastres y movilidad.
- Uso `ontap-san-economy` Cuando se espera que el uso previsto de volumen sea mucho superior al soporte de ONTAP.
- Uso `ontap-nas-economy` Únicamente en los casos en los que se espera que el uso previsto del volumen sea mucho superior al soporte de ONTAP y la `ontap-san-economy` no se puede utilizar el conductor.
- No utilizar `ontap-nas-economy` si prevé la necesidad de protección de datos, recuperación ante desastres o movilidad.

## Permisos de usuario

Astra Trident espera que se ejecute como administrador de ONTAP o SVM, normalmente mediante el `admin` usuario del clúster o un `vsadmin` Usuario de SVM o un usuario con un nombre diferente que tenga el mismo rol. Para puestas en marcha de Amazon FSX para ONTAP de NetApp, Astra Trident espera que se ejecute como administrador de ONTAP o SVM, mediante el clúster `fsxadmin` usuario o un `vsadmin` Usuario de SVM o un usuario con un nombre diferente que tenga el mismo rol. La `fsxadmin` el usuario es un reemplazo limitado para el usuario administrador del clúster.



Si utiliza la `limitAggregateUsage` parámetro, se necesitan permisos de administrador de clúster. Cuando se utiliza Amazon FSX para ONTAP de NetApp con Astra Trident, el `limitAggregateUsage` el parámetro no funciona con el `vsadmin` y `fsxadmin` cuentas de usuario. La operación de configuración generará un error si se especifica este parámetro.

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

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

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

## Requisitos

Para todos los back-ends de ONTAP, Astra Trident requiere al menos un agregado asignado a la SVM.

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

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

## Autentique el backend de ONTAP

Astra Trident ofrece dos modos de autenticación de un back-end de ONTAP.

- Basado en credenciales: El nombre de usuario y la contraseña de un usuario ONTAP con los permisos requeridos. Se recomienda utilizar un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin`. Garantizar la máxima compatibilidad con versiones de ONTAP.
- Basado en certificados: Astra Trident también puede comunicarse con un clúster de ONTAP mediante un certificado instalado en el back-end. Aquí, la definición de backend debe contener valores codificados en Base64 del certificado de cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

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



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

## Habilite la autenticación basada en credenciales

Astra Trident requiere las credenciales a un administrador con ámbito de SVM o clúster para comunicarse con el back-end de ONTAP. Se recomienda utilizar funciones estándar predefinidas como `admin` o `vsadmin`. De este modo se garantiza la compatibilidad con futuras versiones de ONTAP que puedan dar a conocer API de funciones que podrán utilizarse en futuras versiones de Astra Trident. Se puede crear y utilizar una función de inicio de sesión de seguridad personalizada con Astra Trident, pero no es recomendable.

Una definición de backend de ejemplo tendrá este aspecto:



## YAML

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

## JSON

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

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

### Habilite la autenticación basada en certificados

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

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

Un flujo de trabajo típico implica los pasos siguientes.

### Pasos

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

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

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

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

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

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

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

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

5. Probar la autenticación mediante un certificado generado. Reemplace <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre de SVM.

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

6. Codifique certificados, claves y certificados de CA de confianza con Base64.

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

## 7. Cree un backend utilizando los valores obtenidos del paso anterior.

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

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

### Actualice los métodos de autenticación o gire las credenciales

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

```

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

#Update backend with tridentctl
tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |          UUID          |
STATE | VOLUMES |
+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |      9 |
+-----+-----+-----+
+-----+-----+

```



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

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

### Autentica conexiones con CHAP bidireccional

Astra Trident puede autenticar sesiones iSCSI con CHAP bidireccional para `ontap-san` y `ontap-san-economy` de windows. Esto requiere habilitar el `useCHAP` opción en su definición de backend. Cuando se establece en `true`, Astra Trident configura la seguridad del iniciador predeterminada de la SVM en CHAP bidireccional y establece el nombre de usuario y los secretos del archivo de entorno de administración. NetApp recomienda utilizar CHAP bidireccional para autenticar las conexiones. Consulte la siguiente configuración de ejemplo:

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



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

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

### Cómo funciona

Mediante ajuste `useCHAP` Para `true`, el administrador de almacenamiento ordena a Astra Trident que configure CHAP en el back-end de almacenamiento. Esto incluye lo siguiente:

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

Una vez creado el back-end, Astra Trident crea una correspondiente `tridentbackend` CRD y almacena los secretos y nombres de usuario de CHAP como secretos de Kubernetes. Todos los VP creados por Astra Trident en este back-end se montarán y se conectan mediante CHAP.

### Rotar las credenciales y actualizar los back-ends

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



Al actualizar los secretos CHAP para un back-end, debe utilizar `tridentctl` para actualizar el back-end. No actualice las credenciales en el clúster de almacenamiento a través de la interfaz de usuario de CLI/ONTAP, ya que Astra Trident no podrá recoger estos cambios.

```
cat backend-san.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap_san_chap",
  "managementLIF": "192.168.0.135",
  "svm": "ontap_iscsi_svm",
  "useCHAP": true,
  "username": "vsadmin",
  "password": "password",
  "chapInitiatorSecret": "cl9qxUpDaTeD",
  "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
}

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

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

## Opciones y ejemplos de configuración DE SAN ONTAP

Descubra cómo crear y usar controladores SAN de ONTAP con su instalación de Astra Trident. En esta sección, se ofrecen ejemplos de configuración del back-end y detalles sobre cómo asignar back-ends a StorageClasses.

### Opciones de configuración del back-end

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

Parámetro	Descripción	Predeterminado
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre del conductor + “_” + dataLIF
managementLIF	<p>La dirección IP de una LIF de gestión de clústeres o SVM</p> <p>Para lograr un cambio de MetroCluster sin problemas, debe especificar una LIF de gestión de SVM.</p> <p>Se puede especificar un nombre de dominio completo (FQDN).</p> <p>Se puede configurar para que utilice direcciones IPv6 si se instaló Astra Trident mediante el <code>--use-ipv6</code> bandera. Las direcciones IPv6 deben definirse entre corchetes, como <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>.</p>	“10.0.0.1”, “[2001:1234:abcd::fefef]”
dataLIF	<p>Dirección IP de LIF de protocolo.</p> <p><b>No especifique para iSCSI.</b> Astra Trident utiliza <a href="#">"Asignación de LUN selectiva de ONTAP"</a> Para descubrir los LIF iSCSI necesarios para establecer una sesión de ruta múltiple. Se genera una advertencia if <code>dataLIF</code> se define explícitamente.</p>	Derivado del SVM
useCHAP	<p>Use CHAP para autenticar iSCSI para los controladores SAN de ONTAP [Boolean].</p> <p>Establezca en <code>true</code> Para Astra Trident, configure y utilice CHAP bidireccional como autenticación predeterminada para la SVM proporcionada en el back-end. Consulte <a href="#">"Prepárese para configurar el back-end con los controladores SAN de ONTAP"</a> para obtener más detalles.</p>	false

Parámetro	Descripción	Predeterminado
chapInitiatorSecret	Secreto CHAP del iniciador. Obligatorio si useCHAP=true	""
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
chapTargetInitiatorSecret	Secreto CHAP del iniciador de destino. Obligatorio si useCHAP=true	""
chapUsername	Nombre de usuario entrante. Obligatorio si useCHAP=true	""
chapTargetUsername	Nombre de usuario de destino. Obligatorio si useCHAP=true	""
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados.	""
username	El nombre de usuario necesario para comunicarse con el clúster de ONTAP. Se utiliza para autenticación basada en credenciales.	""
password	La contraseña necesaria para comunicarse con el clúster de ONTAP. Se utiliza para autenticación basada en credenciales.	""
svm	Máquina virtual de almacenamiento que usar	Derivado si una SVM managementLIF está especificado
storagePrefix	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM.  No se puede modificar más adelante. Para actualizar este parámetro, deberá crear un nuevo backend.	trident



Parámetro	Descripción	Predeterminado
limitAggregateUsage	<p>Error al aprovisionar si el uso supera este porcentaje.</p> <p>Si utiliza un entorno de administración de Amazon FSX para ONTAP de NetApp, no especifique <code>limitAggregateUsage</code>. El proporcionado <code>fsxadmin</code> y <code>vsadmin</code> No incluya los permisos necesarios para recuperar el uso de agregados y limitarlo mediante Astra Trident.</p>	"" (no se aplica de forma predeterminada)
limitVolumeSize	<p>Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor.</p> <p>También restringe el tamaño máximo de los volúmenes que gestiona para qtrees y LUN.</p>	"" (no se aplica por defecto)
lunsPerFlexvol	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]	100
debugTraceFlags	<p>Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}</p> <p>No lo utilice a menos que esté solucionando problemas y necesite un volcado de log detallado.</p>	null

Parámetro	Descripción	Predeterminado
useREST	<p>Parámetro booleano para usar las API DE REST de ONTAP. <b>Vista previa técnica</b></p> <p>useREST se proporciona como <b>avance técnico</b> que se recomienda para entornos de prueba y no para cargas de trabajo de producción. Cuando se establece en <code>true</code>, Astra Trident utilizará las API DE REST de ONTAP para comunicarse con el back-end. Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap cliente</code> más. Esto está satisfecho por el predefinido <code>vsadmin</code> y <code>cluster-admin</code> funciones.</p> <p>useREST No es compatible con MetroCluster.</p>	false

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

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

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para las LUN	"verdadero"
spaceReserve	Modo de reserva de espacio; "none" (thin) o "VOLUME" (grueso)	"ninguna"
snapshotPolicy	Política de Snapshot que se debe usar	"ninguna"

Parámetro	Descripción	Predeterminado
qosPolicy	<p>Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento.</p> <p>El uso de grupos de políticas de calidad de servicio con Astra Trident requiere ONTAP 9.8 o posterior. Recomendamos utilizar un grupo de políticas QoS no compartido y garantizar que el grupo de políticas se aplique a cada componente por separado. Un grupo de políticas de calidad de servicio compartido hará que se aplique el techo para el rendimiento total de todas las cargas de trabajo.</p>	""
adaptiveQosPolicy	<p>Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento</p>	""
snapshotReserve	<p>Porcentaje de volumen reservado para snapshots «0»</p>	Si snapshotPolicy no es "ninguno", sino ""
splitOnClone	<p>Divida un clon de su elemento principal al crearlo</p>	"falso"
encryption	<p>Habilite el cifrado de volúmenes de NetApp (NVE) en el volumen nuevo; el valor predeterminado es false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster.</p> <p>Si NAE está habilitado en el back-end, cualquier volumen provisionado en Astra Trident estará habilitado para NAE.</p> <p>Para obtener más información, consulte: <a href="#">"Cómo funciona Astra Trident con NVE y NAE"</a>.</p>	"falso"
luksEncryption	<p>Active el cifrado LUKS. Consulte <a href="#">"Usar la configuración de clave unificada de Linux (LUKS)"</a>.</p>	""
securityStyle	<p>Estilo de seguridad para nuevos volúmenes</p>	unix

Parámetro	Descripción	Predeterminado
tieringPolicy	Política de organización en niveles para usar «ninguno»	“Solo Snapshot” para configuración previa a ONTAP 9.5 SVM-DR

### Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los valores predeterminados definidos:

```

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

```



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

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

$$\text{Total volume size} = [(\text{PVC requested size}) / (1 - (\text{snapshotReserve percentage} / 100))] * 1.1$$

El 1.1 es el 10 % adicional que Astra Trident añade a FlexVol para acomodar los metadatos de las LUN. Para `snapshotReserve = 5 %` y la solicitud de PVC = 5GIB, el tamaño total del volumen es de 5.79GIB y el

tamaño disponible es de 5.5GiB. La `volume show` el comando debería mostrar resultados similares a los de este ejemplo:

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

3 entries were displayed.

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

### Ejemplos de configuración mínima

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



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

### Ejemplo de configuración mínima con SAN de ONTAP

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

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

## Ejemplo de configuración mínima de la economía de SAN de ONTAP

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

## Ejemplo de autenticación basada en certificados

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

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

## Ejemplos de CHAP bidireccional

Estos ejemplos crean un backend con `useCHAP` establezca en `true`.

### Ejemplo de CHAP de SAN de ONTAP

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

### Ejemplo de CHAP de economía de SAN ONTAP

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

## Ejemplos de back-ends con pools virtuales

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

Astra Trident establece etiquetas de aprovisionamiento en el campo "Comentarios". Los comentarios se establecen en la FlexVol. Astra 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` y algunos pools sustituyen los valores predeterminados.



**Ejemplo de SAN ONTAP**



```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: '40000'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
    adaptiveQosPolicy: adaptive-extreme
- labels:
  protection: silver
  creditpoints: '20000'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
    qosPolicy: premium
- labels:
  protection: bronze
  creditpoints: '5000'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'
```

## Ejemplo de economía de SAN ONTAP

```
---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: 'false'
  encryption: 'false'
labels:
  store: san_economy_store
region: us_east_1
storage:
- labels:
  app: oracledb
  cost: '30'
  zone: us_east_1a
  defaults:
    spaceAllocation: 'true'
    encryption: 'true'
- labels:
  app: postgresdb
  cost: '20'
  zone: us_east_1b
  defaults:
    spaceAllocation: 'false'
    encryption: 'true'
- labels:
  app: mysqldb
  cost: '10'
  zone: us_east_1c
  defaults:
    spaceAllocation: 'true'
    encryption: 'false'
- labels:
  department: legal
  creditpoints: '5000'
  zone: us_east_1c
```

```
defaults:
  spaceAllocation: 'true'
  encryption: 'false'
```

## Asigne los back-ends a StorageClass

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

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

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

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

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

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

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

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

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

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

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

Astra Trident decidirá qué pool virtual se selecciona y garantizará que se cumplan los requisitos de almacenamiento.

## Unidades NAS de ONTAP

### Información general del controlador NAS de ONTAP

Obtenga más información sobre la configuración de un entorno de administración de

## ONTAP con controladores NAS de ONTAP y Cloud Volumes ONTAP.

### Información importante acerca de los controladores NAS de ONTAP

Astra Control proporciona una protección fluida, recuperación ante desastres y movilidad (mover volúmenes entre clústeres de Kubernetes) para los volúmenes creados con el `ontap-nas`, `ontap-nas-flexgroup`, y `ontap-san` de windows Consulte "[Requisitos previos de replicación de Astra Control](#)" para obtener más detalles.

- Debe usar `ontap-nas` para cargas de trabajo de producción que requieren protección de datos, recuperación ante desastres y movilidad.
- Uso `ontap-san-economy` Cuando se espera que el uso previsto de volumen sea mucho superior al soporte de ONTAP.
- Uso `ontap-nas-economy` Únicamente en los casos en los que se espera que el uso previsto del volumen sea mucho superior al soporte de ONTAP y la `ontap-san-economy` no se puede utilizar el conductor.
- No utilizar `ontap-nas-economy` si prevé la necesidad de protección de datos, recuperación ante desastres o movilidad.

### Permisos de usuario

Astra Trident espera que se ejecute como administrador de ONTAP o SVM, normalmente mediante el `admin` usuario del clúster o un `vsadmin` Usuario de SVM o un usuario con un nombre diferente que tenga el mismo rol.

Para puestas en marcha de Amazon FSX para ONTAP de NetApp, Astra Trident espera que se ejecute como administrador de ONTAP o SVM, mediante el clúster `fsxadmin` usuario o un `vsadmin` Usuario de SVM o un usuario con un nombre diferente que tenga el mismo rol. La `fsxadmin` el usuario es un reemplazo limitado para el usuario administrador del clúster.



Si utiliza la `limitAggregateUsage` parámetro, se necesitan permisos de administrador de clúster. Cuando se utiliza Amazon FSX para ONTAP de NetApp con Astra Trident, el `limitAggregateUsage` el parámetro no funciona con el `vsadmin` y `fsxadmin` cuentas de usuario. La operación de configuración generará un error si se especifica este parámetro.

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

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

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

### Requisitos

- Para todos los back-ends de ONTAP, Astra Trident requiere al menos un agregado asignado a la SVM.
- Puede ejecutar más de un controlador y crear clases de almacenamiento que apunten a uno u otro. Por ejemplo, puede configurar una clase Gold que utilice `ontap-nas` Controlador y clase Bronze que utiliza `ontap-nas-economy` uno.

- Todos sus nodos de trabajo de Kubernetes deben tener instaladas las herramientas NFS adecuadas. Consulte ["aquí"](#) para obtener más detalles.
- Astra Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows. Consulte [Prepárese para aprovisionar los volúmenes de SMB](#) para obtener más detalles.

## Autentique el backend de ONTAP

Astra Trident ofrece dos modos de autenticación de un back-end de ONTAP.

- Basado en credenciales: El nombre de usuario y la contraseña de un usuario ONTAP con los permisos requeridos. Se recomienda utilizar un rol de inicio de sesión de seguridad predefinido, como `admin` o `vsadmin`. Garantizar la máxima compatibilidad con versiones de ONTAP.
- Basado en certificados: Astra Trident también puede comunicarse con un clúster de ONTAP mediante un certificado instalado en el back-end. Aquí, la definición de backend debe contener valores codificados en Base64 del certificado de cliente, la clave y el certificado de CA de confianza si se utiliza (recomendado).

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



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

### Habilite la autenticación basada en credenciales

Astra Trident requiere las credenciales a un administrador con ámbito de SVM o clúster para comunicarse con el back-end de ONTAP. Se recomienda utilizar funciones estándar predefinidas como `admin` o `vsadmin`. De este modo se garantiza la compatibilidad con futuras versiones de ONTAP que puedan dar a conocer API de funciones que podrán utilizarse en futuras versiones de Astra Trident. Se puede crear y utilizar una función de inicio de sesión de seguridad personalizada con Astra Trident, pero no es recomendable.

Una definición de backend de ejemplo tendrá este aspecto:

## YAML

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

## JSON

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "password"
}
```

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

### Habilite la autenticación basada en certificados

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

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

Un flujo de trabajo típico implica los pasos siguientes.

### Pasos

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



de ONTAP para autenticarse como.

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

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

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

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

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

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

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

5. Probar la autenticación mediante un certificado generado. Reemplace <LIF de gestión de ONTAP> y <vserver name> por la IP de LIF de gestión y el nombre de SVM. Debe asegurarse de que la LIF tiene su política de servicio establecida en `default-data-management`.

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

6. Codifique certificados, claves y certificados de CA de confianza con Base64.

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

## 7. Cree un backend utilizando los valores obtenidos del paso anterior.

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "storagePrefix": "myPrefix_"
}

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

NAME	STORAGE DRIVER	UUID
NasBackend	ontap-nas	98e19b74-aec7-4a3d-8dcf-128e5033b214

```

online |          9 |

```

### Actualice los métodos de autenticación o gire las credenciales

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

```

cat cert-backend-updated.json
{
"version": 1,
"storageDriverName": "ontap-nas",
"backendName": "NasBackend",
"managementLIF": "1.2.3.4",
"dataLIF": "1.2.3.8",
"svm": "vserver_test",
"username": "vsadmin",
"password": "password",
"storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+-----+
+-----+-----+
|   NAME   | STORAGE DRIVER |           UUID           |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |      9 |
+-----+-----+-----+-----+
+-----+-----+

```



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

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

### Gestione las políticas de exportación de NFS

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

Astra Trident ofrece dos opciones al trabajar con directivas de exportación:

- Astra Trident puede gestionar dinámicamente la propia política de exportación; en este modo de funcionamiento, el administrador de almacenamiento especifica una lista de bloques CIDR que representan direcciones IP admisibles. Astra Trident agrega automáticamente las IP de nodo que se incluyen en estos rangos a la directiva de exportación. Como alternativa, cuando no se especifican CIDR,

toda IP de unidifusión de ámbito global encontrada en los nodos se agregará a la política de exportación.

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

### Gestione de forma dinámica políticas de exportación

La versión 20.04 de CSI Trident ofrece la capacidad de gestionar dinámicamente políticas de exportación para los back-ends de ONTAP. De este modo, el administrador de almacenamiento puede especificar un espacio de direcciones permitido para las IP de nodos de trabajo, en lugar de definir reglas explícitas de forma manual. Simplifica en gran medida la gestión de políticas de exportación; las modificaciones de la política de exportación ya no requieren intervención manual en el clúster de almacenamiento. Además, esto ayuda a restringir el acceso al clúster de almacenamiento solo a nodos de trabajo con IP en el rango especificado, lo que permite una gestión automatizada y de gran granularidad.



La gestión dinámica de las políticas de exportación sólo está disponible para CSI Trident. Es importante asegurarse de que los nodos de trabajo no estén siendo atados.

### Ejemplo

Hay dos opciones de configuración que deben utilizarse. A continuación se muestra un ejemplo de definición de backend:

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



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

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

- `autoExportPolicy` se establece en `true`. Esto indica que Astra Trident creará una directiva de exportación para `svm1` SVM y gestionan la adición y eliminación de reglas mediante `autoExportCIDRs` bloques de direcciones. Por ejemplo, un back-end con UUID `403b5326-8482-40db-96d0-d83fb3f4daec` y `autoExportPolicy` establezca en `true` crea una política de exportación llamada `trident-403b5326-8482-40db-96d0-d83fb3f4daec` En la SVM.
- `autoExportCIDRs` contiene una lista de bloques de direcciones. Este campo es opcional y se establece de forma predeterminada en `["0.0.0.0/0", "*/0"]`. Si no se define, Astra Trident agrega todas las direcciones

de unidifusión de ámbito global que se encuentran en los nodos de trabajo.

En este ejemplo, la `192.168.0.0/24` se proporciona espacio de dirección. Esto indica que las IP de nodo de Kubernetes que entran dentro de este rango de direcciones se añadirán a la política de exportación que crea Astra Trident. Cuando Astra Trident registra un nodo en el que se ejecuta, recupera las direcciones IP del nodo y las comprueba con respecto a los bloques de direcciones proporcionados en `autoExportCIDRs`. Después de filtrar las IP, Astra Trident crea reglas de política de exportación para las IP de cliente que detecta, con una regla para cada nodo que identifica.

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

Una vez que Astra Trident crea o actualiza un back-end, puede comprobar el backend mediante `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
```

A medida que se añaden nodos a un clúster de Kubernetes y se registran con la controladora Astra Trident, se actualizan las políticas de exportación de los back-ends existentes (siempre que entren en el rango de direcciones especificado en la `autoExportCIDRs` para el back-end).

Cuando se quita un nodo, Astra Trident comprueba todos los back-ends que están en línea para quitar la regla de acceso del nodo. Al eliminar esta IP de nodo de las políticas de exportación de los back-ends gestionados, Astra Trident evita los montajes no autorizados, a menos que se vuelva a utilizar esta IP con un nodo nuevo del clúster.

Para los back-ends anteriores, actualizando el back-end con `tridentctl update backend` Se asegurará de que Astra Trident gestiona las políticas de exportación de forma automática. Esto creará una nueva política de exportación denominada después de que el UUID del back-end y los volúmenes presentes en el back-end utilicen la política de exportación recién creada cuando se vuelvan a montar.



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

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

## Prepárese para aprovisionar los volúmenes de SMB

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



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

### Antes de empezar

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

- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2019. Astra Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto Astra Trident que contiene sus credenciales de Active Directory. Generar secreto `smbcreds`:

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

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

### Pasos

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



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

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

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

La `vserver cifs share create` comando comprueba la ruta especificada en la opción `-path`

durante la creación del recurso compartido. Si la ruta especificada no existe, el comando falla.

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

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

c. Compruebe que se ha creado el recurso compartido:

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



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

2. Al crear el back-end, debe configurar lo siguiente para especificar volúmenes de SMB. Para obtener información sobre todas las opciones de configuración del entorno de administración de ONTAP, consulte "[Opciones y ejemplos de configuración de FSX para ONTAP](#)".

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

Parámetro	Descripción	Ejemplo
Estilo de seguridad para nuevos volúmenes.  <b>Debe estar configurado en <code>ntfs</code> o <code>mixed</code> Para volúmenes SMB.</b>	<code>ntfs</code> o <code>mixed</code> Para volúmenes de SMB	<code>unixPermissions</code>

## Opciones y ejemplos de configuración NAS de ONTAP

Descubre cómo crear y utilizar controladores NAS de ONTAP con tu instalación de Astra Trident. En esta sección, se ofrecen ejemplos de configuración del back-end y detalles sobre cómo asignar back-ends a StorageClasses.

### Opciones de configuración del back-end

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

Parámetro	Descripción	Predeterminado
<code>version</code>		Siempre 1
<code>storageDriverName</code>	Nombre del controlador de almacenamiento	"ontap-nas", "ontap-nas-economy", "ontap-nas-flexgroup", "ontap-san" y "ontap-san-economy"
<code>backendName</code>	Nombre personalizado o el back-end de almacenamiento	Nombre del conductor + "_" + <code>dataLIF</code>
<code>managementLIF</code>	<p>La dirección IP de una LIF de gestión de clústeres o SVM</p> <p>Para lograr un cambio de MetroCluster sin problemas, debe especificar una LIF de gestión de SVM.</p> <p>Se puede especificar un nombre de dominio completo (FQDN).</p> <p>Se puede configurar para que utilice direcciones IPv6 si se instaló Astra Trident mediante el <code>--use-ipv6</code> bandera. Las direcciones IPv6 deben definirse entre corchetes, como <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>.</p>	"10.0.0.1", "[2001:1234:abcd::fefe]"



Parámetro	Descripción	Predeterminado
dataLIF	<p>Dirección IP de LIF de protocolo.</p> <p>Recomendamos especificar <code>dataLIF</code>. En caso de no proporcionar esta información, Astra Trident busca las LIF de datos desde la SVM. Puede especificar un nombre de dominio completo (FQDN) para las operaciones de montaje de NFS, lo que permite crear un DNS round-robin para lograr el equilibrio de carga entre varios LIF de datos.</p> <p>Se puede cambiar después del ajuste inicial. Consulte .</p> <p>Se puede configurar para que utilice direcciones IPv6 si se instaló Astra Trident mediante el <code>--use-ipv6</code> bandera. Las direcciones IPv6 deben definirse entre corchetes, como <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>.</p>	Dirección especificada o derivada de la SVM, si no se especifica (no recomendada)
autoExportPolicy	<p>Habilite la creación y actualización automática de la política de exportación [Boolean].</p> <p>Con el <code>autoExportPolicy</code> y.. <code>autoExportCIDRs</code> Astra Trident puede gestionar automáticamente las políticas de exportación.</p>	falso
autoExportCIDRs	<p>Lista de CIDR para filtrar las IP de nodo de Kubernetes contra cuándo <code>autoExportPolicy</code> está habilitado.</p> <p>Con el <code>autoExportPolicy</code> y.. <code>autoExportCIDRs</code> Astra Trident puede gestionar automáticamente las políticas de exportación.</p>	[“0.0.0.0/0”, “:/0”]
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	””
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	””

Parámetro	Descripción	Predeterminado
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados	""
username	Nombre de usuario para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales	
password	Contraseña para conectarse al clúster/SVM. Se utiliza para autenticación basada en credenciales	
svm	Máquina virtual de almacenamiento que usar	Derivado si una SVM managementLIF está especificado
storagePrefix	El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM. No se puede actualizar después de configurarlo	"trident"
limitAggregateUsage	Error al aprovisionar si el uso supera este porcentaje.  <b>No se aplica a Amazon FSX para ONTAP</b>	"" (no se aplica de forma predeterminada)
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor.	"" (no se aplica por defecto)
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor.  También restringe el tamaño máximo de los volúmenes que gestiona para qtrees y LUN, y la qtreesPerFlexvol Permite personalizar el número máximo de qtrees por FlexVol.	"" (no se aplica por defecto)
lunsPerFlexvol	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]	«100»

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

Parámetro	Descripción	Predeterminado
smbShare	<p>Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado mediante la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP; un nombre para permitir que Astra Trident cree el recurso compartido de SMB; o bien puede dejar el parámetro en blanco para evitar el acceso de recurso compartido común a los volúmenes.</p> <p>Este parámetro es opcional para ONTAP en las instalaciones.</p> <p>Este parámetro es necesario para los back-ends de Amazon FSx para ONTAP y no puede estar en blanco.</p>	smb-share
useREST	<p>Parámetro booleano para usar las API DE REST de ONTAP. <b>Vista previa técnica</b></p> <p>useREST se proporciona como <b>avance técnico</b> que se recomienda para entornos de prueba y no para cargas de trabajo de producción. Cuando se establece en <code>true</code>, Astra Trident utilizará las API DE REST de ONTAP para comunicarse con el back-end. Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap</code> cliente más. Esto está satisfecho por el predefinido <code>vsadmin</code> y.. <code>cluster-admin</code> funciones.</p> <p>useREST No es compatible con MetroCluster.</p>	falso

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

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

Parámetro	Descripción	Predeterminado
spaceAllocation	Asignación de espacio para las LUN	“verdadero”
spaceReserve	Modo de reserva de espacio; “none” (thin) o “VOLUME” (grueso)	“ninguna”
snapshotPolicy	Política de Snapshot que se debe usar	“ninguna”
qosPolicy	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	“”
adaptiveQosPolicy	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento.  no admitido por ontap-nas-Economy.	“”
snapshotReserve	Porcentaje de volumen reservado para snapshots «0»	Si snapshotPolicy no es “ninguno”, sino “”
splitOnClone	Divida un clon de su elemento principal al crearlo	“falso”
encryption	Habilite el cifrado de volúmenes de NetApp (NVE) en el volumen nuevo; el valor predeterminado es false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster.  Si NAE está habilitado en el back-end, cualquier volumen provisionado en Astra Trident estará habilitado para NAE.  Para obtener más información, consulte: <a href="#">"Cómo funciona Astra Trident con NVE y NAE"</a> .	“falso”
tieringPolicy	Política de organización en niveles para usar «ninguno»	“Solo Snapshot” para configuración previa a ONTAP 9.5 SVM-DR
unixPermissions	Modo para volúmenes nuevos	“777” para volúmenes NFS; vacío (no aplicable) para volúmenes SMB
snapshotDir	Controla la visibilidad de .snapshot directorio	“falso”

Parámetro	Descripción	Predeterminado
exportPolicy	Política de exportación que se va a utilizar	“predeterminado”
securityStyle	<p>Estilo de seguridad para nuevos volúmenes.</p> <p>Compatibilidad con NFS <code>mixed</code> y.. <code>unix</code> estilos de seguridad.</p> <p>SMB admite <code>mixed</code> y.. <code>ntfs</code> estilos de seguridad.</p>	<p>El valor predeterminado de NFS es <code>unix</code>.</p> <p>La opción predeterminada de SMB es <code>ntfs</code>.</p>



El uso de grupos de políticas de calidad de servicio con Astra Trident requiere ONTAP 9.8 o posterior. Se recomienda utilizar un grupo de políticas de calidad de servicio no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas de calidad de servicio compartido hará que se aplique el techo para el rendimiento total de todas las cargas de trabajo.

### Ejemplos de aprovisionamiento de volúmenes

Aquí hay un ejemplo con los valores predeterminados definidos:

```

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

```

Para `ontap-nas` y `ontap-nas-flexgroups`, Astra Trident utiliza ahora un nuevo cálculo para garantizar que el tamaño de la FlexVol sea correcto con el porcentaje `snapshotReserve` y la RVP. Cuando el usuario solicita una RVP, Astra Trident crea el FlexVol original con más espacio mediante el nuevo cálculo. Este cálculo garantiza que el usuario recibe el espacio de escritura que solicitó en el PVC y no menos espacio que el que solicitó. Antes de v21.07, cuando el usuario solicita una RVP (por ejemplo, 5GIB) con el 50 por ciento de `snapshotReserve`, solo obtiene 2,5 GIB de espacio editable. Esto se debe a que el usuario solicitó todo el volumen y `snapshotReserve` es un porcentaje de esta situación. Con Trident 21.07, lo que el usuario solicita es el espacio editable y Astra Trident define el `snapshotReserve` número como porcentaje del volumen completo. Esto no se aplica a `ontap-nas-economy`. Vea el siguiente ejemplo para ver cómo funciona:

El cálculo es el siguiente:

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

Para `snapshotReserve` = 50 % y la solicitud de RVP = 5 GIB, el tamaño total del volumen es  $2/5 = 10$  GIB y el tamaño disponible es de 5 GIB, lo que es lo que solicitó el usuario en la solicitud de RVP. La `volume show` el comando debería mostrar resultados similares a los de este ejemplo:

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

2 entries were displayed.

Los back-ends existentes de instalaciones anteriores aprovisionan volúmenes como se explicó anteriormente al actualizar Astra Trident. En el caso de los volúmenes que creó antes de actualizar, debe cambiar el tamaño de sus volúmenes para que se observe el cambio. Por ejemplo, una RVP de 2 GIB con `snapshotReserve=50` Anteriormente, se produjo un volumen que proporciona 1 GIB de espacio editable. Cambiar el tamaño del volumen a 3 GIB, por ejemplo, proporciona a la aplicación 3 GIB de espacio editable en un volumen de 6 GIB.

### Ejemplos de configuración mínima

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



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

### Configuración mínima para `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
```

### Configuración mínima para `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
```

### Configuración mínima para volúmenes de SMB

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



## Autenticación basada en certificados

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

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

## Política de exportación automática

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

```
---
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
```

## El uso de direcciones IPv6

Este ejemplo muestra managementLIF Uso de una dirección IPv6.

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

## Amazon FSx para ONTAP mediante volúmenes SMB

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

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

## Ejemplos de back-ends con pools virtuales

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

Astra Trident establece etiquetas de aprovisionamiento en el campo "Comentarios". Los comentarios se establecen en FlexVol para `ontap-nas` O FlexGroup para `ontap-nas-flexgroup`. Astra 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` y algunos pools sustituyen los valores predeterminados.

## Ejemplo de NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
svm: svm_nfs
username: admin
password: <password>
nfsMountOptions: nfsvers=4
defaults:
  spaceReserve: none
  encryption: 'false'
  qosPolicy: standard
labels:
  store: nas_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  app: msoffice
  cost: '100'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
    adaptiveQosPolicy: adaptive-premium
- labels:
  app: slack
  cost: '75'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  department: legal
  creditpoints: '5000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  app: wordpress
```

```
    cost: '50'  
    zone: us_east_1c  
    defaults:  
      spaceReserve: none  
      encryption: 'true'  
      unixPermissions: '0775'  
- labels:  
  app: mysqldb  
  cost: '25'  
  zone: us_east_1d  
  defaults:  
    spaceReserve: volume  
    encryption: 'false'  
    unixPermissions: '0775'
```

## Ejemplo de FlexGroup NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-flexgroup
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: flexgroup_store
  k8scluster: prod-cluster-1
region: us_east_1
storage:
- labels:
  protection: gold
  creditpoints: '50000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: gold
  creditpoints: '30000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: silver
  creditpoints: '20000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
  protection: bronze
  creditpoints: '10000'
  zone: us_east_1d
  defaults:
```

```
spaceReserve: volume  
encryption: 'false'  
unixPermissions: '0775'
```

## Ejemplo de economía NAS de ONTAP

```
---
version: 1
storageDriverName: ontap-nas-economy
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: <password>
defaults:
  spaceReserve: none
  encryption: 'false'
labels:
  store: nas_economy_store
region: us_east_1
storage:
- labels:
  department: finance
  creditpoints: '6000'
  zone: us_east_1a
  defaults:
    spaceReserve: volume
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  protection: bronze
  creditpoints: '5000'
  zone: us_east_1b
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0755'
- labels:
  department: engineering
  creditpoints: '3000'
  zone: us_east_1c
  defaults:
    spaceReserve: none
    encryption: 'true'
    unixPermissions: '0775'
- labels:
  department: humanresource
  creditpoints: '2000'
  zone: us_east_1d
  defaults:
    spaceReserve: volume
```



```
encryption: 'false'  
unixPermissions: '0775'
```

## Asigne los back-ends a StorageClass

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

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

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

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

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

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

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

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

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

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

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

Astra Trident decidirá qué pool virtual se selecciona y garantizará que se cumplan los requisitos de almacenamiento.

### **Actualizar dataLIF tras la configuración inicial**

Puede cambiar la LIF de datos tras la configuración inicial ejecutando el siguiente comando para proporcionar el nuevo archivo JSON back-end con LIF de datos actualizadas.

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



Si los RVP están conectados a uno o varios pods, deben recuperar todos los pods correspondientes y, a continuación, traerlos para que surta efecto el nuevo LIF de datos.

## Amazon FSX para ONTAP de NetApp

### Utilice Astra Trident con Amazon FSX para ONTAP de NetApp

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

### Descripción general

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

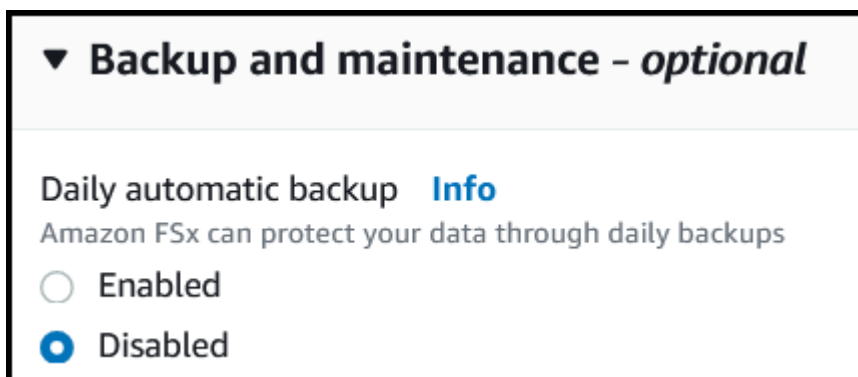
Al utilizar Astra Trident con Amazon FSX para ONTAP de NetApp, puede garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) pueden aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

Usos de Amazon FSX para ONTAP de NetApp "**FabricPool**" para gestionar los niveles de almacenamiento. Le permite almacenar datos en un nivel, según la frecuencia de acceso a estos.

### Consideraciones

- Volúmenes SMB:
  - Se admiten los volúmenes de SMB mediante el `ontap-nas` sólo conductor.
  - Astra Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Trident no puede eliminar los volúmenes creados en sistemas de archivos Amazon FSX con backups automáticos habilitados. Para eliminar las RVP, es necesario eliminar manualmente el VP y el FSX para el volumen ONTAP. Para evitar este problema:
  - No utilice **creación rápida** para crear el sistema de archivos FSX para ONTAP. El flujo de trabajo de creación rápida permite realizar backups automáticos y no ofrece la opción de anulación de suscripción.

- Cuando utilice **Standard create**, desactive la copia de seguridad automática. Al deshabilitar los backups automáticos, Trident puede eliminar correctamente un volumen sin intervención manual adicional.



## De Windows

Puede integrar Astra Trident con Amazon FSX para ONTAP de NetApp mediante los siguientes controladores:

- `ontap-san`: Cada VP aprovisionado es una LUN dentro de su propio Amazon FSX para el volumen ONTAP de NetApp.
- `ontap-san-economy`: Cada VP aprovisionado es un LUN con un número configurable de LUN por Amazon FSX para el volumen ONTAP de NetApp.
- `ontap-nas`: Cada VP aprovisionado es un Amazon FSX completo para el volumen ONTAP de NetApp.
- `ontap-nas-economy`: Cada VP aprovisionado es un qtree, con un número configurable de qtrees por Amazon FSX para el volumen ONTAP de NetApp.
- `ontap-nas-flexgroup`: Cada VP aprovisionado es un Amazon FSX completo para el volumen ONTAP FlexGroup de NetApp.

Para obtener más información sobre el controlador, consulte "[Controladores ONTAP](#)".

## Autenticación

Astra Trident ofrece dos modos de autenticación.

- Basado en certificados: Astra Trident se comunicará con la SVM en su sistema de archivos FSX mediante un certificado instalado en la SVM.
- Basado en credenciales: Puede utilizar el `fsxadmin` usuario del sistema de archivos o del `vsadmin` Usuario configurado para la SVM.



Astra Trident espera que se ejecute como un `vsadmin` Usuario de SVM o como usuario con un nombre diferente que tenga el mismo rol. Amazon FSX para NetApp ONTAP cuenta con una `fsxadmin` Usuario que es una sustitución limitada de ONTAP `admin` usuario de clúster. Le recomendamos encarecidamente que utilice `vsadmin` Con Astra Trident.

Puede actualizar los back-ends para moverse entre los métodos basados en credenciales y los basados en certificados. Sin embargo, si intenta proporcionar **credenciales y certificados**, la creación de backend fallará. Para cambiar a un método de autenticación diferente, debe eliminar el método existente de la configuración del back-end.

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

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

### Obtenga más información

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

## Integración de Amazon FSX para ONTAP de NetApp

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

### Requisitos

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

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



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

- Astra Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows. Consulte [Prepárese para aprovisionar los volúmenes de SMB](#) para obtener más detalles.

## Integración de controladores ONTAP SAN y NAS



Si está configurando para volúmenes SMB, debe leer [Prepárese para aprovisionar los volúmenes de SMB](#) antes de crear el back-end.

### Pasos

1. Ponga en marcha Astra Trident con una de las ["métodos de implementación"](#).
2. Recoja el nombre de DNS del LIF de gestión de SVM. Por ejemplo, si utiliza la CLI de AWS, busque el `DNSName` entrada en `Endpoints` → `Management` tras ejecutar el siguiente comando:

```
aws fsx describe-storage-virtual-machines --region <file system region>
```

3. Cree e instale certificados para ["Autenticación de back-end NAS"](#) o ["Autenticación de entorno de administración DE SAN"](#).



Puede iniciar sesión en el sistema de archivos (por ejemplo, para instalar certificados) con SSH desde cualquier lugar que pueda llegar al sistema de archivos. Utilice la `fsxadmin` Usuario, la contraseña que configuró al crear el sistema de archivos y el nombre DNS de gestión desde `aws fsx describe-file-systems`.

4. Cree un archivo de entorno de administración mediante sus certificados y el nombre DNS de la LIF de gestión, como se muestra en el ejemplo siguiente:

#### YAML

```
---
version: 1
storageDriverName: ontap-san
backendName: customBackendName
managementLIF: svm-XXXXXXXXXXXXXXXXXXXX.fs-XXXXXXXXXXXXXXXXXXXX.fsx.us-
east-2.aws.internal
svm: svm01
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

#### JSON

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "customBackendName",
  "managementLIF": "svm-XXXXXXXXXXXXXXXXXXXX.fs-
XXXXXXXXXXXXXXXXXXXX.fsx.us-east-2.aws.internal",
  "svm": "svm01",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz"
}
```

Para obtener información sobre la creación de back-ends, consulte estos enlaces:

- ["Configurar un back-end con controladores NAS de ONTAP"](#)
- ["Configuración de un back-end con controladores SAN de ONTAP"](#)

#### Resultados

Después de la implementación, puede crear una ["clase de almacenamiento, aprovisiona un volumen y monta el volumen en un pod"](#).

## Prepárese para aprovisionar los volúmenes de SMB

Puede aprovisionar volúmenes SMB mediante el `ontap-nas` controlador. Antes de completar la tarea [Integración de controladores ONTAP SAN y NAS](#) complete los siguientes pasos.

### Antes de empezar

Para poder aprovisionar volúmenes de SMB con el `ontap-nas` conductor, debe tener lo siguiente.

- Un clúster de Kubernetes con un nodo de controladora Linux y al menos un nodo de trabajo de Windows que ejecuta Windows Server 2019. Astra Trident admite volúmenes de SMB montados en pods que se ejecutan solo en nodos de Windows.
- Al menos un secreto Astra Trident que contiene sus credenciales de Active Directory. Generar secreto `smbcreds`:

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

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

### Pasos

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

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

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

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

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

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

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



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

2. Al crear el back-end, debe configurar lo siguiente para especificar volúmenes de SMB. Para obtener información sobre todas las opciones de configuración del entorno de administración de ONTAP, consulte ["Opciones y ejemplos de configuración de FSX para ONTAP"](#).

Parámetro	Descripción	Ejemplo
smbShare	Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado con la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP, o bien un nombre para permitir que Astra Trident cree el recurso compartido de SMB.  Este parámetro es obligatorio para los back-ends de Amazon FSx para ONTAP.	smb-share
nasType	<b>Debe establecer en smb.</b> Si es nulo, el valor predeterminado es nfs.	smb
securityStyle	Estilo de seguridad para nuevos volúmenes.  <b>Debe estar configurado en ntfs o. mixed Para volúmenes SMB.</b>	ntfs o. mixed Para volúmenes de SMB
unixPermissions	Modo para volúmenes nuevos. <b>Se debe dejar vacío para volúmenes SMB.</b>	""

## Opciones y ejemplos de configuración de FSX para ONTAP

Obtenga información acerca de las opciones de configuración de back-end para Amazon FSX para ONTAP. Esta sección proporciona ejemplos de configuración de fondo.

### Opciones de configuración del back-end

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

Parámetro	Descripción	Ejemplo
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre del conductor + “_” + dataLIF



Parámetro	Descripción	Ejemplo
managementLIF	<p>La dirección IP de una LIF de gestión de clústeres o SVM</p> <p>Para lograr un cambio de MetroCluster sin problemas, debe especificar una LIF de gestión de SVM.</p> <p>Se puede especificar un nombre de dominio completo (FQDN).</p> <p>Se puede configurar para que utilice direcciones IPv6 si se instaló Astra Trident mediante el <code>--use-ipv6</code> bandera. Las direcciones IPv6 deben definirse entre corchetes, como <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>.</p>	<p>"10.0.0.1", "[2001:1234:abcd::fefe]"</p>

Parámetro	Descripción	Ejemplo
dataLIF	<p>Dirección IP de LIF de protocolo.</p> <p><b>Controladores NAS de ONTAP:</b> Recomendamos especificar dataLIF. En caso de no proporcionar esta información, Astra Trident busca las LIF de datos desde la SVM. Puede especificar un nombre de dominio completo (FQDN) para las operaciones de montaje de NFS, lo que permite crear un DNS round-robin para lograr el equilibrio de carga entre varios LIF de datos. Se puede cambiar después del ajuste inicial. Consulte .</p> <p><b>Controladores SAN ONTAP:</b> No se especifica para iSCSI. Astra Trident utiliza la asignación selectiva de LUN de ONTAP para descubrir los LIF iSCSI necesarios para establecer una sesión de varias rutas. Se genera una advertencia si dataLIF se define explícitamente.</p> <p>Se puede configurar para que utilice direcciones IPv6 si se instaló Astra Trident mediante el <code>--use-ipv6</code> bandera. Las direcciones IPv6 deben definirse entre corchetes, como <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>.</p>	
autoExportPolicy	<p>Habilite la creación y actualización automática de la política de exportación [Boolean].</p> <p>Con el <code>autoExportPolicy</code> y <code>autoExportCIDRs</code> Astra Trident puede gestionar automáticamente las políticas de exportación.</p>	false

Parámetro	Descripción	Ejemplo
autoExportCIDRs	<p>Lista de CIDR para filtrar las IP de nodo de Kubernetes contra cuándo autoExportPolicy está habilitado.</p> <p>Con el autoExportPolicy y.. autoExportCIDRs Astra Trident puede gestionar automáticamente las políticas de exportación.</p>	"["0.0.0.0/0", ":/0"]"
labels	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes	""
clientCertificate	Valor codificado en base64 del certificado de cliente. Se utiliza para autenticación basada en certificados	""
clientPrivateKey	Valor codificado en base64 de la clave privada de cliente. Se utiliza para autenticación basada en certificados	""
trustedCACertificate	Valor codificado en base64 del certificado de CA de confianza. Opcional. Se utiliza para autenticación basada en certificados.	""
username	El nombre de usuario para conectarse al clúster o SVM. Se utiliza para autenticación basada en credenciales. Por ejemplo, vsadmin.	
password	La contraseña para conectarse al clúster o SVM. Se utiliza para autenticación basada en credenciales.	
svm	Máquina virtual de almacenamiento que usar	Derivado si se especifica una LIF de gestión de SVM.
storagePrefix	<p>El prefijo que se utiliza cuando se aprovisionan volúmenes nuevos en la SVM.</p> <p>No se puede modificar una vez creada. Para actualizar este parámetro, deberá crear un nuevo backend.</p>	trident

Parámetro	Descripción	Ejemplo
limitAggregateUsage	<p><b>No especifique para Amazon FSx para NetApp ONTAP.</b></p> <p>El proporcionado fsxadmin y.. vsadmin No incluya los permisos necesarios para recuperar el uso de agregados y limitarlo mediante Astra Trident.</p>	No utilizar.
limitVolumeSize	<p>Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor.</p> <p>También restringe el tamaño máximo de los volúmenes que gestiona para qtrees y LUN, y la qtreesPerFlexvol Permite personalizar el número máximo de qtrees por FlexVol.</p>	"" (no se aplica de forma predeterminada)
lunsPerFlexvol	<p>El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200].</p> <p>Solo SAN.</p>	100
debugTraceFlags	<p>Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}</p> <p>No utilizar debugTraceFlags a menos que esté solucionando problemas y necesite un volcado de registro detallado.</p>	nulo

Parámetro	Descripción	Ejemplo
nfsMountOptions	<p>Lista de opciones de montaje NFS separadas por comas.</p> <p>Las opciones de montaje para los volúmenes persistentes de Kubernetes se especifican normalmente en tipos de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Astra Trident se pondrá en contacto con las opciones de montaje especificadas en el archivo de configuración del back-end de almacenamiento.</p> <p>Si no se especifican opciones de montaje en la clase de almacenamiento o el archivo de configuración, Astra Trident no configurará ninguna opción de montaje en un volumen persistente asociado.</p>	""
nasType	<p>Configure la creación de volúmenes NFS o SMB.</p> <p>Las opciones son <code>nfs</code>, <code>smb</code>, o nulo.</p> <p><b>Debe establecer en <code>smb</code> Para volúmenes SMB.</b> el valor predeterminado es <code>null</code> en volúmenes NFS.</p>	<code>nfs</code>
qtreesPerFlexvol	El número máximo de qtrees por FlexVol debe estar comprendido entre [50, 300]	200
smbShare	<p>Puede especificar una de las siguientes opciones: El nombre de un recurso compartido de SMB creado con la consola de administración de Microsoft o la interfaz de línea de comandos de ONTAP, o bien un nombre para permitir que Astra Trident cree el recurso compartido de SMB.</p> <p>Este parámetro es obligatorio para los back-ends de Amazon FSx para ONTAP.</p>	<code>smb-share</code>

Parámetro	Descripción	Ejemplo
useREST	<p>Parámetro booleano para usar las API DE REST de ONTAP. <b>Vista previa técnica</b></p> <p>useREST se proporciona como <b>avance técnico</b> que se recomienda para entornos de prueba y no para cargas de trabajo de producción. Cuando se establece en <code>true</code>, Astra Trident utilizará las API DE REST de ONTAP para comunicarse con el back-end.</p> <p>Esta función requiere ONTAP 9.11.1 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap cliente más</code>. Esto está satisfecho por el predeterminado <code>vsadmin</code> y.. <code>cluster-admin</code> funciones.</p>	<code>false</code>

#### Actualizar `dataLIF` tras la configuración inicial

Puede cambiar la LIF de datos tras la configuración inicial ejecutando el siguiente comando para proporcionar el nuevo archivo JSON back-end con LIF de datos actualizadas.

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



Si los RVP están conectados a uno o varios pods, deben recuperar todos los pods correspondientes y, a continuación, traerlos para que surta efecto el nuevo LIF de datos.

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

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

Parámetro	Descripción	Predeterminado
<code>spaceAllocation</code>	Asignación de espacio para las LUN	<code>true</code>
<code>spaceReserve</code>	Modo de reserva de espacio; "none" (thin) o "VOLUME" (grueso)	<code>none</code>
<code>snapshotPolicy</code>	Política de Snapshot que se debe usar	<code>none</code>

Parámetro	Descripción	Predeterminado
qosPolicy	<p>Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o back-end.</p> <p>El uso de grupos de políticas de calidad de servicio con Astra Trident requiere ONTAP 9.8 o posterior.</p> <p>Recomendamos utilizar un grupo de políticas QoS no compartido y garantizar que el grupo de políticas se aplique a cada componente por separado. Un grupo de políticas de calidad de servicio compartido hará que se aplique el techo para el rendimiento total de todas las cargas de trabajo.</p>	""
adaptiveQosPolicy	<p>Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool de almacenamiento o back-end.</p> <p>no admitido por ontap-nas-Economy.</p>	""
snapshotReserve	Porcentaje de volumen reservado para snapshots «0»	Si snapshotPolicy es none, else ""
splitOnClone	Divida un clon de su elemento principal al crearlo	false
encryption	<p>Habilite el cifrado de volúmenes de NetApp (NVE) en el volumen nuevo; el valor predeterminado es false. Para usar esta opción, debe tener una licencia para NVE y habilitarse en el clúster.</p> <p>Si NAE está habilitado en el back-end, cualquier volumen provisionado en Astra Trident estará habilitado para NAE.</p> <p>Para obtener más información, consulte: <a href="#">"Cómo funciona Astra Trident con NVE y NAE"</a>.</p>	false

Parámetro	Descripción	Predeterminado
luksEncryption	Active el cifrado LUKS. Consulte <a href="#">"Usar la configuración de clave unificada de Linux (LUKS)"</a> .  Solo SAN.	""
tieringPolicy	Política de organización en niveles para utilizar none	snapshot-only Para configuraciones anteriores a ONTAP 9,5 SVM-DR
unixPermissions	Modo para volúmenes nuevos.  <b>Dejar vacío para volúmenes SMB.</b>	""
securityStyle	Estilo de seguridad para nuevos volúmenes.  Compatibilidad con NFS mixed y.. unix estilos de seguridad.  SMB admite mixed y.. ntfs estilos de seguridad.	El valor predeterminado de NFS es unix.  La opción predeterminada de SMB es ntfs.

## Ejemplo

Uso `nasType`, `node-stage-secret-name`, y `node-stage-secret-namespace`, Puede especificar un volumen SMB y proporcionar las credenciales necesarias de Active Directory. Se admiten los volúmenes de SMB mediante el `ontap-nas` sólo conductor.

```

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

```



## Información de copyright

Copyright © 2024 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.