



Configurar los back-ends

Astra Trident

NetApp
April 16, 2024

Tabla de contenidos

- Configurar los back-ends 1
 - Configure un back-end de Azure NetApp Files 1
 - Configure un CVS para back-end de GCP 14
 - Configure un back-end de NetApp HCI o SolidFire 25
 - Configuración de un back-end con controladores SAN de ONTAP 31
 - Configure un back-end NAS de ONTAP 51
 - Utilice Astra Trident con Amazon FSX para ONTAP de NetApp 72

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 ofrecerá automáticamente pools de almacenamiento de back-ends que cumplan los requisitos definidos por una clase de almacenamiento. Obtenga más información sobre la configuración del back-end en función del tipo de sistema de almacenamiento que tenga.

- ["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"](#)

Configure un back-end de Azure NetApp Files

Puede configurar Azure NetApp Files (ANF) como back-end de Astra Trident. Puede conectar volúmenes NAS y SMB mediante un back-end ANF.

- ["Preparación"](#)
- ["Opciones de configuración y ejemplos"](#)

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.
- Astra Trident no es compatible con la arquitectura DE Windows ARM.

Prepárese para configurar un back-end de Azure NetApp Files

Antes de configurar el back-end ANF, debe asegurarse de que se cumplen los siguientes requisitos.

Si es la primera vez que utiliza Azure NetApp Files o está en una nueva ubicación, se requiere 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 Azure NetApp Files y añadir un volumen SMB, consulte: ["Azure: Cree un volumen de SMB para Azure NetApp Files"](#).

Requisitos

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

- `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"
        ]
      }
    ]
  }
}
```

```

ete",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/subvolumes/Get
Metadata/action",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/MountTargets/r
ead",
    "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

- 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 para que ANF pueda autenticarse en Active Directory. Generar secreto smbcreds:

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

- 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.

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.

Opciones de configuración del back-end

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	
<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)

Parámetro	Descripción	Predeterminado
<code>capacityPools</code>	Lista de pools de capacidad para filtrar los recursos detectados	<code>[]</code> (sin filtro, aleatorio)
<code>virtualNetwork</code>	Nombre de una red virtual con una subred delegada	""
<code>subnet</code>	Nombre de una subred delegada a. <code>Microsoft.Netapp/volumes</code>	""
<code>networkFeatures</code>	Puede que el conjunto de funciones de vnet para un volumen sea <code>Basic</code> o <code>Standard</code> . 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.	""
<code>nfsMountOptions</code>	Control preciso de las opciones de montaje NFS. Ignorada para volúmenes de SMB. 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. Las opciones de montaje establecidas en una definición de clase de almacenamiento anulan las opciones de montaje establecidas en la configuración de back-end.	<code>"nfsvers=3"</code>
<code>limitVolumeSize</code>	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)
<code>debugTraceFlags</code>	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
<code>nasType</code>	Configure la creación de volúmenes NFS o SMB. Las opciones son <code>nfs</code> , <code>smb</code> o nulo. El valor predeterminado es nulo en volúmenes de NFS.	<code>nfs</code>



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

Aprovisionamiento de volúmenes

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

Parámetro	Descripción	Predeterminado
<code>exportRule</code>	Reglas de exportación de volúmenes nuevos. <code>exportRule</code> 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"
<code>snapshotDir</code>	Controla la visibilidad del directorio <code>.snapshot</code>	"falso"
<code>size</code>	El tamaño predeterminado de los volúmenes nuevos	"100 G"
<code>unixPermissions</code>	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)



Para todos los volúmenes creados en un back-end ANF, Astra Trident copia las etiquetas presentes en un pool de almacenamiento al volumen de almacenamiento en el momento en el que se aprovisiona. Los administradores de almacenamiento pueden definir etiquetas por pool de almacenamiento y agrupar todos los volúmenes creados en un pool de almacenamiento. Esta es una forma cómoda de diferenciar los volúmenes según un conjunto de etiquetas personalizables que se proporcionan en la configuración del back-end.

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 de almacenamiento 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.

```
{
  "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"
  },
  "location": "eastus",

  "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 CVS para back-end de GCP

Descubra cómo configurar NetApp Cloud Volumes Service (CVS) para Google Cloud Platform (GCP) como back-end de su instalación de Astra Trident con las configuraciones de muestra proporcionadas.

Obtenga más información sobre la compatibilidad de Astra Trident con CVS para GCP

Astra Trident admite volúmenes con el tipo de servicio CVS predeterminado "GCP". Astra Trident no admite volúmenes CVS inferiores a 100 GIB independientemente del mínimo permitido por el tipo de servicio CVS. Por lo tanto, Trident crea automáticamente un volumen de 100 GIB si el volumen solicitado es menor que el tamaño mínimo.

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 CVS 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 su cuenta de servicio CVS

Opciones de configuración del back-end

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

Parámetro	Descripción	Predeterminado
version		Siempre 1

Parámetro	Descripción	Predeterminado
storageDriverName	Nombre del controlador de almacenamiento	"gcp-cvs"
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre de controlador + "_" + parte de la clave de API
storageClass	Tipo de almacenamiento. Elija entre <i>hardware</i> (rendimiento optimizado) o <i>software</i> (Tipo de servicio CVS)	
projectNumber	Número de proyecto de cuenta de Google Cloud. El valor se encuentra en la página de inicio del portal de Google Cloud.	
apiRegion	Región de la cuenta CVS. Es la región en la que el back-end aprovisionará los volúmenes.	
apiKey	Clave de API para la cuenta de servicio de Google Cloud con el <code>netappcloudvolumes.admin</code> función. 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).	
proxyURL	URL de proxy si se requiere servidor proxy para conectarse a la cuenta CVS. El servidor proxy puede ser un proxy HTTP o HTTPS. En el caso de un proxy HTTPS, se omite la validación de certificados para permitir el uso de certificados autofirmados en el servidor proxy. No se admiten los servidores proxy con autenticación habilitada.	
nfsMountOptions	Control preciso de las opciones de montaje NFS.	"nfsvers=3"
limitVolumeSize	No se puede aprovisionar si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)
serviceLevel	El nivel de servicio CVS para nuevos volúmenes. Los valores son "estándar", "premium" y "extremo".	"estándar"
network	GCP se utiliza para volúmenes CVS	"predeterminado"

Parámetro	Descripción	Predeterminado
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo: <pre>\{"api":false, "method":true\}</pre> . No lo utilice a menos que esté solucionando problemas y necesite un volcado de registro detallado.	nulo

Si se utiliza una red VPC compartida, ambos `projectNumber` y `hostProjectNumber` debe especificarse. En ese caso, `projectNumber` es el proyecto de servicio, y `hostProjectNumber` es el proyecto anfitrión.

La `apiRegion` Representa la región de GCP en la que Astra Trident crea volúmenes CVS. Cuando se crean clústeres de Kubernetes en varias regiones, los volúmenes CVS se crean en un `apiRegion`. Se puede utilizar en cargas de trabajo programadas en nodos en varias regiones de GCP. Tenga en cuenta que el tráfico entre regiones conlleva un coste adicional.

- Para habilitar el acceso a varias regiones, se debe definir `StorageClass` para `allowedTopologies` debe incluir todas las regiones. Por ejemplo:

```
- key: topology.kubernetes.io/region
  values:
  - us-east1
  - europe-west1
```



- `storageClass` es un parámetro opcional que puede utilizar para seleccionar el deseado "Tipo de servicio CVS". Puede elegir entre el tipo de servicio CVS básico (`storageClass=software`) O el tipo de servicio CVS-Performance (`storageClass=hardware`), que Trident utiliza de forma predeterminada. Asegúrese de especificar un `apiRegion`. Esto proporciona el CVS correspondiente `storageClass` en su definición de backend.



La integración de Astra Trident con el tipo de servicio CVS básico en Google Cloud es una **funcionalidad beta**, no está pensada para cargas de trabajo de producción. Trident es **totalmente compatible** con el tipo de servicio CVS-Performance y lo usa de forma predeterminada.

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

Puede controlar de forma predeterminada el modo en que se aprovisiona cada volumen especificando las siguientes opciones en una sección especial del archivo de configuración. Vea los ejemplos de configuración a continuación.

Parámetro	Descripción	Predeterminado
exportRule	Las reglas de exportación de los nuevos volúmenes	"0.0.0.0/0"


```

bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4
Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5o
jY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nzn
HczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrt
HisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbO
guSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKe
yAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRA
GzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4j
K3bl/qp8B4Kws8zX5ojY9m\nXsYg6gyxy4zq70lwWgLwGa==\n-----END PRIVATE
KEY-----\n",
    "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 del tipo de servicio CVS base

Este ejemplo muestra una definición de back-end que utiliza el tipo de servicio CVS básico, que está pensada para cargas de trabajo de uso general y ofrece rendimiento ligero/moderado, además de una alta disponibilidad zonal.

```

{
  "version": 1,
  "storageDriverName": "gcp-cvs",
  "projectNumber": "012345678901",
  "storageClass": "software",
  "apiRegion": "us-east4",
  "apiKey": {
    "type": "service_account",
    "project_id": "my-gcp-project",
    "private_key_id": "1234567890123456789012345678901234567890",
    "private_key": "-----BEGIN PRIVATE KEY-----
\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZ
srrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisI
sAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSa
PIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZN
chRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllz
ZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl

```

```

/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kw
s8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY
9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHc
zZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHi
sIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOgu
SaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyA
ZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz
llzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3
bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4
Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5o
jY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nzn
HczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrt
HisIsAbOguSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbO
guSaPIKeyAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKe
yAZNchRAGzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRA
GzllzZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzllzZE4j
K3bl/qp8B4Kws8zX5ojY9m\nXsYg6gyxy4zq70lwWgLwGa==\n-----END PRIVATE
KEY-----\n",
    "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 3: Configuración de un solo nivel de servicio

Este ejemplo muestra un archivo de entorno de administración que aplica los mismos aspectos a todo el almacenamiento creado por Astra Trident en la región Google Cloud US-west2. En este ejemplo también se muestra el uso de `proxyURL` en el archivo de configuración del back-end.

```

{
  "version": 1,
  "storageDriverName": "gcp-cvs",
  "projectNumber": "012345678901",
  "apiRegion": "us-west2",
  "apiKey": {
    "type": "service_account",
    "project_id": "my-gcp-project",
    "private_key_id": "1234567890123456789012345678901234567890",

```

```

    "private_key": "-----BEGIN PRIVATE KEY-----
\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZ
srtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisI
sAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSa
PIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZN
chRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzll
ZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl
/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4K
ws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5oj
Y9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznH
czZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtr
HisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbO
guSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKe
yAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRA
GzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4j
K3bl/qp8B4Kws8zX5ojY9m\nXsYg6gyxy4zq70lwWgLwGa==\n-----END PRIVATE
KEY-----\n",
    "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"
  }
}

```



```

KEY-----\n",
  "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"
}
]
}

```

Las siguientes definiciones de StorageClass se refieren a los pools de almacenamiento anteriores. Mediante el uso de `parameters.selector` Campo, se puede especificar para cada clase de almacenamiento el pool virtual que se usa para alojar un volumen. Los aspectos definidos en el pool elegido serán el volumen.

El primer tipo de almacenamiento (`cvs-extreme-extra-protection`) se asigna al primer grupo de almacenamiento 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 de almacenamiento virtual se selecciona y garantiza que se cumpla el requisito de reserva Snapshot.

```

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 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.

Lo que necesitará

- 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](#)".

Lo que usted necesita saber

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
solidfire-san	iSCSI	Bloque	RWO, ROX, RWX	No hay sistema de archivos. Dispositivo de bloque RAW.
solidfire-san	iSCSI	Bloque	RWO, ROX, RWX	No hay sistema de archivos. Dispositivo de bloque RAW.
solidfire-san	iSCSI	Sistema de archivos	RWO, ROX	xfs, ext3, ext4
solidfire-san	iSCSI	Sistema de archivos	RWO, ROX	xfs, ext3, ext4



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)
<code>Endpoint</code>	MVIP para el clúster de SolidFire con credenciales de inquilino	
<code>SVIP</code>	La dirección IP y el puerto de almacenamiento (iSCSI)	
<code>labels</code>	Conjunto de etiquetas con formato JSON arbitrario que se aplica en los volúmenes.	""
<code>TenantName</code>	Nombre de inquilino que se va a usar (creado si no se encuentra)	
<code>InitiatorIFace</code>	Restringir el tráfico de iSCSI a una interfaz de host específica	"predeterminado"
<code>UseCHAP</code>	Utilice CHAP para la autenticación de iSCSI	verdadero
<code>AccessGroups</code>	Lista de ID de grupos de acceso que se van a usar	Busca el código de un grupo de acceso denominado "trident".
<code>Types</code>	Especificaciones de calidad de servicio	
<code>limitVolumeSize</code>	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor	"" (no se aplica de forma predeterminada)

Parámetro	Descripción	Predeterminado
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}	nulo



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



Para todos los volúmenes creados, Astra Trident copiará todas las etiquetas presentes en un pool de almacenamiento a la LUN de almacenamiento de respaldo en el momento en el que se aprovisiona. Los administradores de almacenamiento pueden definir etiquetas por pool de almacenamiento y agrupar todos los volúmenes creados en un pool de almacenamiento. Esto proporciona una forma cómoda de diferenciar los volúmenes basándose en un conjunto de etiquetas personalizables que se proporcionan en la configuración del back-end.

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 de almacenamiento virtual

En este ejemplo, se muestra el archivo de definición del back-end configurado con pools de almacenamiento virtual junto con StorageClasses que se denominan.

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 de almacenamiento virtual se definen en la `storage` sección. En este ejemplo, algunos del pool de almacenamiento establecen su propio tipo, y algunos pools sobrescriben los valores predeterminados establecidos 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 de almacenamiento virtual 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 de almacenamiento 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 de almacenamiento 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"](#)

Configuración de un back-end con controladores SAN de ONTAP

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

- ["Preparación"](#)
- ["Configuración y ejemplos"](#)

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

Descubra cómo preparar un back-end de ONTAP con controladores DE SAN de ONTAP. 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 ["aquí"](#) para obtener más detalles.

Autenticación

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:

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

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=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",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuueeeee",
  "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",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "secret",
  "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.

Especifique iGroups

Astra Trident utiliza iGroups para controlar el acceso a los volúmenes (LUN) que aprovisiona. Los administradores tienen dos opciones cuando se trata de especificar iGroups para los back-ends:

- Astra Trident puede crear y gestionar automáticamente un igroup por back-end. Si `igroupName` No se incluye en la definición de back-end, Astra Trident crea un igroup llamado `trident-<backend-UUID>` En la SVM. De este modo, cada back-end cuenta con un igroup dedicado y manejar la adición/eliminación automatizada de IQN de nodos de Kubernetes.
- De forma alternativa, los iGroups creados previamente también se pueden proporcionar en una definición

de back-end. Esto se puede hacer usando `igroupName` parámetro config. Astra Trident añadirá/eliminará IQN de nodos de Kubernetes al `igroup` preexistente.

Para los back-ends que tengan `igroupName` definida, el `igroupName` se puede eliminar con un `tridentctl backend update` Para tener iGroups de gestión automática Astra Trident. Esto no interrumpirá el acceso a volúmenes que ya están conectados a las cargas de trabajo. Futuras conexiones se gestionarán con el `igroup` Astra Trident creado.



Dedicar un `igroup` para cada instancia única de Astra Trident es una práctica recomendada que beneficia al administrador de Kubernetes y al administrador de almacenamiento. CSI Trident automatiza la adición y la eliminación de IQN de nodos de clúster al `igroup`, por lo que simplifica en gran medida su gestión. Cuando se utiliza la misma SVM en entornos de Kubernetes (y instalaciones de Astra Trident), el uso de un `igroup` dedicado garantiza que los cambios realizados en un clúster de Kubernetes no afecten a los iGroups asociados a otro. Además, también es importante garantizar que cada nodo del clúster de Kubernetes tenga un IQN único. Como se ha mencionado anteriormente, Astra Trident se encarga automáticamente de la adición y eliminación de IQN. La reutilización de IQN entre hosts puede provocar situaciones no deseadas en las que los hosts se confunden entre sí y se deniega el acceso a las LUN.

Si Astra Trident está configurada para que funcione como un proveedor de nodos CSI, los IQN de nodos de Kubernetes se añaden o eliminan automáticamente del `igroup`. Cuando se añaden nodos a un clúster de Kubernetes, `trident-csi` DemonSet despliega un pod (`trident-csi-xxxxx`) en los nodos recién añadidos y registra los nuevos nodos a los que puede asociar volúmenes. Los IQN de nodos también se agregan al `igroup` del backend. Un conjunto de pasos similares tratan de la eliminación de IQN cuando se acortan, drenan y se eliminan nodos de Kubernetes.

Si Astra Trident no se ejecuta como un proveedor CSI, el `igroup` se debe actualizar manualmente para contener los IQN iSCSI de cada nodo de trabajo del clúster de Kubernetes. Se deberán añadir al `igroup` varios IQN de nodos que se unen al clúster de Kubernetes. De igual manera, los IQN de nodos que se quitan del clúster de Kubernetes se deben quitar del `igroup`.

Auténtica 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": "FaKePaSsWoRd",
  "igroupName": "trident",
  "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).
- Gestionar la adición de iniciadores a la igroupName dado en el backend. Si no se especifica, el valor predeterminado es `trident`.

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": "FaKePaSsWoRd",
  "igroupName": "trident",
  "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” y “ontap-san-economy”
backendName	Nombre personalizado o el back-end de almacenamiento	Nombre del conductor + “_” + dataLIF
managementLIF	Dirección IP de un LIF de gestión de SVM o clúster para una conmutación de sitios MetroCluster fluida, debe especificar una LIF de gestión de SVM.	“10.0.0.1”, “[2001:1234:abcd::fefe]”
dataLIF	Dirección IP de LIF de protocolo. Use corchetes para IPv6. No se puede actualizar después de configurarlo	Derivado de la SVM a menos que se especifique
useCHAP	Usar CHAP para la autenticación de iSCSI para los controladores SAN de ONTAP [booleano]	falso
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	""

Parámetro	Descripción	Predeterminado
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
igroupName	Nombre del igroup para volúmenes DE SAN que usar	"Trident-<backend-UUID>"
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. No se aplica a Amazon FSX para ONTAP	"" (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 de forma predeterminada)
lunsPerFlexvol	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]	"100"
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}	nulo
useREST	Parámetro booleano para usar las API DE REST de ONTAP. Vista previa técnica no compatible con MetroCluster.	falso

Consideraciones sobre el `useREST` para el "leeeleee"



- `useREST` se proporciona como **avance técnico** que se recomienda para entornos de prueba y no para cargas de trabajo de producción. Cuando se establece en `true`, Astra Trident utilizará las API DE REST de ONTAP para comunicarse con el back-end. Esta función requiere ONTAP 9.10 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a `ontap` cliente más. Esto está satisfecho por el predeterminado `vsadmin` y `cluster-admin` funciones.
- `useREST` No es compatible con MetroCluster.

Para comunicarse con el clúster ONTAP, debe proporcionar los parámetros de autenticación. Puede ser el nombre de usuario o la contraseña de un inicio de sesión de seguridad o un certificado instalado.



Si utiliza un entorno de administración de Amazon FSX para ONTAP de NetApp, no especifique el `limitAggregateUsage` parámetro. La `fsxadmin` y `vsadmin` Las funciones que ofrece Amazon FSX para ONTAP de NetApp no incluyen los permisos de acceso necesarios para recuperar el uso de agregados y limitarla a través de Astra Trident.



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

Para la `ontap-san` Controladores, el valor predeterminado es utilizar todas las IP de LIF de datos de la SVM y para utilizar la multivía iSCSI. Especificar una dirección IP para la LIF de datos del `ontap-san` los controladores les obligan a deshabilitar la multivía y a usar solo la dirección especificada.



Al crear un back-end, recuerde eso `dataLIF` y `storagePrefix` no se puede modificar una vez creada. Para actualizar estos parámetros, deberá crear un nuevo backend.

`igroupName` Puede establecerse en un `igroup` que ya se creó en el clúster de ONTAP. Si no se especifica, Astra Trident crea automáticamente un `igroup` llamado `Trident-<backend-UUID>`. Si proporciona un nombre de canal medio predeterminado, NetApp recomienda usar un `igroup` por clúster de Kubernetes, si la SVM se va a compartir entre entornos. Esto es necesario para que Astra Trident mantenga automáticamente las adiciones y eliminaciones por IQN.

Los back-ends también pueden tener `iGroups` actualizados después de la creación:

- Se puede actualizar el nombre de `lfe` para que apunte a un nuevo `igroup` que se crea y gestiona en la SVM fuera de Astra Trident.
- Se puede omitir el nombre de la pila. En este caso, Astra Trident creará y gestionará automáticamente un `igroup` `trident-<backend-UUID>`.

En ambos casos, los archivos adjuntos de volumen seguirán siendo accesibles. Los futuros archivos adjuntos de volumen utilizarán el `igroup` actualizado. Esta actualización no interrumpe el acceso a los volúmenes presentes en el back-end.

Se puede especificar un nombre de dominio completo (FQDN) para el `managementLIF` opción.

``managementLIF`` Para todos los controladores ONTAP también se puede establecer en direcciones IPv6. Asegúrese de instalar Trident con el ``--use-ipv6`` bandera. Hay que tener cuidado para definir ``managementLIF`` La dirección IPv6 entre corchetes.



Cuando se usen direcciones IPv6, asegúrese de `managementLIF` y.. `dataLIF` (si se incluye en su definición de backend) se definen entre corchetes, como `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. Si `dataLIF` No se proporciona; Astra Trident recuperará las LIF de datos IPv6 desde la SVM.

Para habilitar los controladores `ontap-san` para que usen CHAP, configure el `useCHAP` parámetro a `true` en su definición de backend. A continuación, Astra Trident configurará y utilizará CHAP bidireccional como la autenticación predeterminada para la SVM proporcionada en el back-end. Consulte "[aquí](#)" para descubrir cómo funciona.

Para la `ontap-san-economy` controlador, el `limitVolumeSize` Opción también restringirá el tamaño máximo de los volúmenes que gestiona para `qtrees` y LUN.



Astra Trident establece etiquetas de aprovisionamiento en el campo "Comentarios" de todos los volúmenes creados mediante `ontap-san` controlador. Para cada volumen creado, el campo "Comentarios" del FlexVol se rellenará con todas las etiquetas presentes en el pool de almacenamiento en el que se haya colocado. Los administradores de almacenamiento pueden definir etiquetas por pool de almacenamiento y agrupar todos los volúmenes creados en un pool de almacenamiento. Esto proporciona una forma cómoda de diferenciar los volúmenes basándose en un conjunto de etiquetas personalizables que se proporcionan en la configuración del back-end.

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

Puede controlar cómo se aprovisiona cada volumen de forma predeterminada mediante estas opciones de una sección especial 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	"verdadero"
<code>spaceReserve</code>	Modo de reserva de espacio; "none" (thin) o "VOLUME" (grueso)	"ninguna"
<code>snapshotPolicy</code>	Política de Snapshot que se debe usar	"ninguna"
<code>qosPolicy</code>	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de <code>qosPolicy</code> o <code>adaptiveQosPolicy</code> por pool/back-end de almacenamiento	""

Parámetro	Descripción	Predeterminado
adaptiveQosPolicy	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	""
snapshotReserve	Porcentaje del volumen reservado para instantáneas "0"	Si snapshotPolicy no es "ninguno", sino ""
splitOnClone	Divida un clon de su elemento principal al crearlo	"falso"
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: " Cómo funciona Astra Trident con NVE y NAE ".	"falso"
luksEncryption	Active el cifrado LUKS. Consulte " Usar la configuración de clave unificada de Linux (LUKS) ".	""
securityStyle	Estilo de seguridad para nuevos volúmenes	"unix"
tieringPolicy	Política de organización en niveles para usar "ninguno"	"Solo Snapshot" para configuración previa a ONTAP 9.5 SVM-DR



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.

A continuación se muestra un ejemplo con valores predeterminados definidos:

```

{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password",
  "labels": {"k8scluster": "dev2", "backend": "dev2-sanbackend"},
  "storagePrefix": "alternate-trident",
  "igroupName": "custom",
  "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 se utiliza Amazon FSX en ONTAP de NetApp con Astra Trident, se recomienda especificar los nombres DNS para las LIF en lugar de las direcciones IP.

ontap-san controlador con 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,
  "storageDriverName": "ontap-san",
  "backendName": "DefaultSANBackend",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz"
}
```

ontap-san Controlador con CHAP bidireccional

Este es un ejemplo de configuración de backend mínima. Esta configuración básica crea un `ontap-san` back-end con `useCHAP` establezca en `true`.

```

{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "labels": {"k8scluster": "test-cluster-1", "backend": "testcluster1-
sanbackend"},
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret"
}

```

ontap-san-economy **controlador**

```

{
  "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",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret"
}

```

Ejemplos de back-ends con pools de almacenamiento virtuales

En el archivo de definición del back-end de ejemplo que se muestra a continuación, se establecen valores predeterminados específicos para todos los grupos de almacenamiento, como `spaceReserve` en ninguno, `spaceAllocation` en falso, y `encryption` en falso. Los pools de almacenamiento virtual se definen en la sección de almacenamiento.

En este ejemplo, algunos de los recursos compartidos de almacenamiento son los suyos propios `spaceReserve`, `spaceAllocation`, y `encryption` los valores y algunos pools sobrescriben los valores predeterminados establecidos anteriormente.


```

{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret",

  "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"
        }
    }
]
}

```

A continuación, se muestra un ejemplo de iSCSI para el `ontap-san-economy` controlador:

```

{
  "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",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret",

  "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"
    }
  }
]
}

```

Asigne los back-ends a StorageClass

Las siguientes definiciones de StorageClass se refieren a los pools de almacenamiento virtual 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 (`protection-gold`) se asignará al primer, segundo grupo de almacenamiento virtual del `ontap-nas-flexgroup` back-end y el primer pool de almacenamiento virtual del `ontap-san` back-end. Se trata de la única piscina que ofrece protección de nivel Gold.
- El segundo tipo de almacenamiento (`protection-not-gold`) se asignará al tercer y cuarto bloque de almacenamiento virtual en `ontap-nas-flexgroup` back-end y el segundo, tercer pool de almacenamiento virtual del `ontap-san` back-end. Estos son los únicos pools que ofrecen un nivel de protección distinto al Gold.
- El tercer tipo de almacenamiento (`app-mysqldb`) se asignará al cuarto bloque de almacenamiento virtual en `ontap-nas` back-end y el tercer pool de almacenamiento virtual de `ontap-san-economy` back-end. Estos son los únicos grupos que ofrecen la configuración del pool de almacenamiento para la aplicación de tipo `mysqldb`.
- El cuarto tipo de almacenamiento (`protection-silver-creditpoints-20k`) se asignará al tercer grupo de almacenamiento virtual en `ontap-nas-flexgroup` back-end y el segundo pool de almacenamiento virtual de `ontap-san` back-end. Estas son las únicas piscinas que ofrecen protección de nivel Gold con 20000 puntos de crédito.
- El quinto tipo de almacenamiento (`creditpoints-5k`) se asignará al segundo grupo de almacenamiento virtual en `ontap-nas-economy` back-end y el tercer pool de almacenamiento virtual de `ontap-san` back-end. Se trata de la única oferta de pool en 5000 puntos de crédito.

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

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
---
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"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

Configure un back-end NAS de ONTAP

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

- ["Preparación"](#)
- ["Configuración y ejemplos"](#)



Los clientes deben utilizar la `ontap-nas` ser el motor de cargas de trabajo de producción que requieren protección de datos, recuperación ante desastres y movilidad. Astra Control proporciona protección, recuperación ante desastres y movilidad fluidas para los volúmenes que se crean con `ontap-nas` controlador. La `ontap-nas-economy` El controlador se debe utilizar solo en casos de uso limitados en los que se espera que el uso previsto de un volumen sea mucho superior al compatible con ONTAP, sin requisitos anticipados de protección de datos, recuperación tras desastres o movilidad (trasladando volúmenes entre clústeres de Kubernetes).

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 un back-end con controladores NAS de ONTAP

Descubra cómo preparar un back-end de ONTAP con controladores NAS de ONTAP. Para todos los back-ends de ONTAP, Astra Trident requiere al menos un agregado asignado a la SVM.

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 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.

Autenticación

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:

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

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           |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| 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 backend update`.

```
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": "secret",
  "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 |
+-----+-----+-----+-----+
+-----+-----+
```



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

La actualización de un back-end no interrumpe el acceso a los volúmenes que se han creado ni afecta a las conexiones de volúmenes realizadas después. Una actualización de back-end correcta indica que 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 que tienen IP en el rango especificado, por lo que admite una gestión automatizada y finegada.



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": "FaKePaSsWoRd",
  "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 predefinida con una regla de exportación que permite al 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.

Opciones y ejemplos de configuración NAS de ONTAP

Obtenga más información sobre cómo crear y utilizar controladores NAS 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
<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>	Dirección IP de un LIF de gestión de SVM o clúster para una conmutación de sitios MetroCluster fluida, debe especificar una LIF de gestión de SVM.	“10.0.0.1”, “[2001:1234:abcd::fefe]”
<code>dataLIF</code>	Dirección IP de LIF de protocolo. Use corchetes para IPv6. No se puede actualizar después de configurarlo	Derivado de la SVM a menos que se especifique

Parámetro	Descripción	Predeterminado
autoExportPolicy	Habilitar la creación y actualización automática de la política de exportación [booleano]	falso
autoExportCIDRs	Lista de CIDR para filtrar las IP de nodo de Kubernetes contra cuándo autoExportPolicy está habilitado	["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	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
igroupName	Nombre del igroup para volúmenes DE SAN que usar	"Trident-<backend-UUID>"
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. No se aplica a Amazon FSX para ONTAP	"" (no se aplica de forma predeterminada)

Parámetro	Descripción	Predeterminado
limitVolumeSize	Error en el aprovisionamiento si el tamaño del volumen solicitado es superior a este valor.	"" (no se aplica de forma predeterminada)
lunsPerFlexvol	El número máximo de LUN por FlexVol debe estar comprendido entre [50 y 200]	"100"
debugTraceFlags	Indicadores de depuración que se deben usar para la solución de problemas. Ejemplo, {"api":false, "method":true}	nulo
nfsMountOptions	Lista de opciones de montaje NFS separadas por comas	""
qtreesPerFlexvol	El número máximo de qtrees por FlexVol debe estar comprendido entre [50, 300]	"200"
useREST	Parámetro booleano para usar las API DE REST de ONTAP. Vista previa técnica no compatible con MetroCluster.	falso

Consideraciones sobre el `useREST` para el "leeeleee"



- `useREST` se proporciona como **avance técnico** que se recomienda para entornos de prueba y no para cargas de trabajo de producción. Cuando se establece en `true`, Astra Trident utilizará las API DE REST de ONTAP para comunicarse con el back-end. Esta función requiere ONTAP 9.10 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a `ontap` cliente más. Esto está satisfecho por el predeterminado `vsadmin` y `cluster-admin` funciones.
- `useREST` No es compatible con MetroCluster.

Para comunicarse con el clúster ONTAP, debe proporcionar los parámetros de autenticación. Puede ser el nombre de usuario o la contraseña de un inicio de sesión de seguridad o un certificado instalado.



Si utiliza un entorno de administración de Amazon FSX para ONTAP de NetApp, no especifique el `limitAggregateUsage` parámetro. La `fsxadmin` y `vsadmin` Las funciones que ofrece Amazon FSX para ONTAP de NetApp no incluyen los permisos de acceso necesarios para recuperar el uso de agregados y limitarla a través de Astra Trident.



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



Al crear un back-end, recuerde que `dataLIF` y `storagePrefix` no se puede modificar una vez creada. Para actualizar estos parámetros, deberá crear un nuevo backend.

Se puede especificar un nombre de dominio completo (FQDN) para el `managementLIF` opción. También se puede especificar un FQDN para el `dataLIF` Opción, en cuyo caso, se utilizará el FQDN para las operaciones de montaje de NFS. De esta forma puede crear un DNS round-robin para lograr un equilibrio entre la carga en

múltiples LIF de datos.

```
`managementLIF` Para todos los controladores ONTAP también se puede establecer en direcciones IPv6. Asegúrese de instalar Astra Trident con el `--use-ipv6` bandera. Hay que tener cuidado para definir el `managementLIF` La dirección IPv6 entre corchetes.
```



Cuando se usen direcciones IPv6, asegúrese de `managementLIF` y.. `dataLIF` (si se incluye en su definición de backend) se definen entre corchetes, como `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. Si `dataLIF` No se proporciona; Astra Trident recuperará las LIF de datos IPv6 desde la SVM.

Con el `autoExportPolicy` y.. `autoExportCIDRs` Opciones, CSI Trident puede gestionar automáticamente las políticas de exportación. Esto es compatible con todos los controladores `ontap-nas-*`.

Para la `ontap-nas-economy` controlador, el `limitVolumeSize` Esta opción también restringirá el tamaño máximo de los volúmenes que gestiona para `qtrees` y LUN, y el `qtreesPerFlexvol` Permite personalizar el número máximo de `qtrees` por FlexVol.

La `nfsMountOptions` el parámetro puede utilizarse para especificar opciones de montaje. Normalmente, las opciones de montaje para los volúmenes persistentes de Kubernetes se especifican 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. Si no se especifican opciones de montaje en la clase de almacenamiento o el archivo de configuración, Astra Trident no establecerá ninguna opción de montaje en un volumen persistente asociado.



Astra Trident establece etiquetas de aprovisionamiento en el campo "Comentarios" de todos los volúmenes creados mediante `ontap-nas` y.. `ontap-nas-flexgroup`. Según el controlador utilizado, los comentarios se establecen en FlexVol (`ontap-nas`) O FlexGroup (`ontap-nas-flexgroup`). Astra Trident copiará todas las etiquetas presentes en un pool de almacenamiento al volumen de almacenamiento en el momento en que se aprovisiona. Los administradores de almacenamiento pueden definir etiquetas por pool de almacenamiento y agrupar todos los volúmenes creados en un pool de almacenamiento. Esto proporciona una forma cómoda de diferenciar los volúmenes basándose en un conjunto de etiquetas personalizables que se proporcionan en la configuración del back-end.

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

Puede controlar cómo se aprovisiona cada volumen de forma predeterminada mediante estas opciones de una sección especial 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	"verdadero"
<code>spaceReserve</code>	Modo de reserva de espacio; "none" (thin) o "VOLUME" (grueso)	"ninguna"
<code>snapshotPolicy</code>	Política de Snapshot que se debe usar	"ninguna"

Parámetro	Descripción	Predeterminado
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 del volumen reservado para instantáneas "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: "Cómo funciona Astra Trident con NVE y NAE" .	"falso"
securityStyle	Estilo de seguridad para nuevos volúmenes	"unix"
tieringPolicy	Política de organización en niveles para usar "ninguno"	"Solo Snapshot" para configuración previa a ONTAP 9.5 SVM-DR
Permisos univalados	Modo para volúmenes nuevos	"777"
Copias Snapshot Dir	Controla la visibilidad de .snapshot directorio	"falso"
Política de exportoPolicy	Política de exportación que se va a utilizar	"predeterminado"
SecurityStyle	Estilo de seguridad para nuevos volúmenes	"unix"



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.

A continuación se muestra un ejemplo con valores predeterminados definidos:

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

Para `ontap-nas` y `ontap-nas-flexgroups`, 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 es 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.

ontap-nas controlador con 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_"
}
```

ontap-nas controlador con 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": "secret",
  "nfsMountOptions": "nfsvers=4",
}

```

ontap-nas-flexgroup **controlador**

```

{
  "version": 1,
  "storageDriverName": "ontap-nas-flexgroup",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "labels": {"k8scluster": "test-cluster-east-1b", "backend": "test1-
ontap-cluster"},
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret",
}

```

ontap-nas **Controlador con 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": "netapp123"
}

```

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

Ejemplos de back-ends con pools de almacenamiento virtuales

En el archivo de definición del back-end de ejemplo que se muestra a continuación, se establecen valores predeterminados específicos para todos los grupos de almacenamiento, como `spaceReserve` en ninguno, `spaceAllocation` en falso, y `encryption` en falso. Los pools de almacenamiento virtual se definen en la sección de almacenamiento.

En este ejemplo, algunos de los recursos compartidos de almacenamiento son los suyos propios `spaceReserve`, `spaceAllocation`, y `encryption` los valores y algunos pools sobrescriben los valores predeterminados establecidos anteriormente.

```
{
  {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "managementLIF": "10.0.0.1",
    "dataLIF": "10.0.0.2",
    "svm": "svm_nfs",
    "username": "admin",
    "password": "secret",
    "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":{"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"
    }
  }
]
}

```

ontap-nas-flexgroup **controlador**

```

{
  "version": 1,
  "storageDriverName": "ontap-nas-flexgroup",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",

```

```

"username": "vsadmin",
"password": "secret",

"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"
    }
  }
]

```

```
]
}
```

ontap-nas-economy **controlador**

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

  "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":{"department":"legal", "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 los pools de almacenamiento virtual 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 (`protection-gold`) se asignará al primer, segundo grupo de almacenamiento virtual del `ontap-nas-flexgroup` back-end y el primer pool de almacenamiento virtual del `ontap-san` back-end. Se trata de la única piscina que ofrece protección de nivel Gold.
- El segundo tipo de almacenamiento (`protection-not-gold`) se asignará al tercer y cuarto bloque de almacenamiento virtual en `ontap-nas-flexgroup` back-end y el segundo, tercer pool de almacenamiento virtual del `ontap-san` back-end. Estos son los únicos pools que ofrecen un nivel de protección distinto al Gold.
- El tercer tipo de almacenamiento (`app-mysqldb`) se asignará al cuarto bloque de almacenamiento virtual en `ontap-nas` back-end y el tercer pool de almacenamiento virtual de `ontap-san-economy` back-end. Estos son los únicos grupos que ofrecen la configuración del pool de almacenamiento para la aplicación de tipo `mysqldb`.
- El cuarto tipo de almacenamiento (`protection-silver-creditpoints-20k`) se asignará al tercer grupo de almacenamiento virtual en `ontap-nas-flexgroup` back-end y el segundo pool de almacenamiento virtual de `ontap-san` back-end. Estas son las únicas piscinas que ofrecen protección de nivel Gold con 20000 puntos de crédito.
- El quinto tipo de almacenamiento (`creditpoints-5k`) se asignará al segundo grupo de almacenamiento virtual en `ontap-nas-economy` back-end y el tercer pool de almacenamiento virtual de `ontap-san` back-end. Se trata de la única oferta de pool en 5000 puntos de crédito.

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


```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
---
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"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"
```

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 lanzar y ejecutar sistemas de archivos con el sistema operativo de almacenamiento ONTAP de NetApp. Amazon FSX para ONTAP de NetApp le permite aprovechar las funciones, el rendimiento y las funcionalidades administrativas de NetApp con las que está familiarizado, a la vez que aprovecha la simplicidad, la agilidad, la seguridad y la escalabilidad de almacenar datos en AWS. FSX es compatible con muchas de las funciones del sistema de archivos y API de administración de ONTAP.

Un sistema de archivos es el recurso principal de Amazon FSX, similar a un clúster de ONTAP en las instalaciones. En cada SVM, se pueden crear uno o varios volúmenes, que son contenedores de datos que almacenan los archivos y las carpetas en el sistema de archivos. Con Amazon FSX para 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.

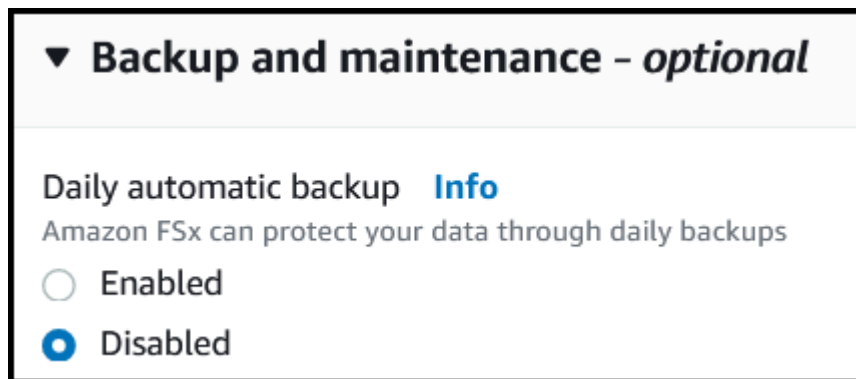
Al utilizar Astra Trident con Amazon FSX para ONTAP de NetApp, puede garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) pueden aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

Creación del sistema de archivos Amazon FSX para ONTAP

Trident no puede eliminar los volúmenes creados en sistemas de archivos Amazon FSX que tienen 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.



Obtenga más información sobre Astra Trident

Si es nuevo en Astra Trident, familiarícese con los siguientes enlaces:

- ["Preguntas frecuentes"](#)

- ["Requisitos para usar Astra Trident"](#)
- ["Ponga en marcha Astra Trident"](#)
- ["Prácticas recomendadas para configurar ONTAP, Cloud Volumes ONTAP y Amazon FSX para ONTAP de NetApp"](#)
- ["Integre Astra Trident"](#)
- ["Configuración de entorno de administración DE SAN ONTAP"](#)
- ["Configuración de back-end NAS de ONTAP"](#)

Obtenga más información sobre las capacidades del controlador ["aquí"](#).

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.

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. No se recomienda utilizar el `fsxadmin` Usuario, con Trident, como `vsadmin` El usuario de SVM tiene acceso a más funcionalidades de Astra Trident.

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.

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.



Le recomendamos encarecidamente que utilice `vsadmin` usuario en lugar de `fsxadmin` para configurar el back-end. Astra Trident se comunicará con el sistema de archivos FSX mediante este nombre de usuario y contraseña.

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.

Para obtener más información acerca de la autenticación, consulte estos enlaces:

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

Ponga en marcha y configure Astra Trident en EKS con Amazon FSX para ONTAP de NetApp

Lo que necesitará

- Un clúster de Amazon EKS existente o un clúster de Kubernetes autogestionado con `kubectl` instalado.
- Un Amazon FSX existente para el sistema de archivos ONTAP de NetApp y una máquina virtual de almacenamiento (SVM) accesible desde los nodos de trabajo del clúster.
- Nodos de trabajo preparados para ["NFS y/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.

Para ver otros requisitos de Astra Trident, consulte ["aquí"](#).

Pasos

1. Ponga en marcha Astra Trident con una de las ["métodos de implementación"](#).
2. Configure Astra Trident de la siguiente manera:
 - a. Recopile el nombre DNS de LIF de gestión de la SVM. Por ejemplo, utilice 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 la autenticación. Si está utilizando un `ontap-san` back-end, consulte ["aquí"](#). Si está utilizando un `ontap-nas` back-end, consulte ["aquí"](#).



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:

```
{
  "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"](#)



No especifique `dataLIF` para la `ontap-san` y.. `ontap-san-economy` Controladores para permitir que Astra Trident utilice multivía.



La `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.

Después de la implementación, lleve a cabo los pasos para crear un ["clase de almacenamiento, aprovisiona un volumen y monte el volumen en un pod"](#).

Obtenga más información

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

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 INTERRUPTIÓN 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.