Configurar un back-end con controladores SAN ONTAP o Cloud Volumes ONTAP

Astra Trident

NetApp
April 16, 2024

Tabla de contenidos

Configuración de un back-end con controladores SAN de ONTAP

Obtenga información acerca de la configuración de un back-end de ONTAP con controladores SAN de ONTAP o 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.

Preparación

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).

Los usuarios también pueden optar por actualizar los back-ends existentes, optar por pasar de basado en credenciales a basado en certificados y viceversa. Si **se proporcionan tanto las credenciales como los certificados**, Astra Trident utilizará por defecto los certificados mientras emite una advertencia para eliminar las credenciales de la definición de backend.

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...Vaaallllluuuueeee",
"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, utilice una actualización `backend.json` archivo 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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

> 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.

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 aprovisionador 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 aprovisionador 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.

Autentica conexiones con CHAP bidireccional

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

```
{
    "version": 1,
    "storageDriverName": "ontap-san",
    "backendName": "ontap_san_chap",
    "managementLIF": "192.168.0.135",
    "svm": "ontap_iscsi_svm",
    "useCHAP": true,
    "username": "vsadmin",
    "password": "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 de configuración y ejemplos

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`	La dirección IP de una LIF de gestión de clústeres o 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**	falso

`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 9.9 o posterior. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a `ontap` cliente más. Esto está satisfecho por el predefinido `vsadmin` y.. `cluster-admin` funciones.

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 predefinido, 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 lle 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
`spaceAllocation`	Asignación de espacio para las LUN	“verdadero”
`spaceReserve`	Modo de reserva de espacio; “none” (thin) o “VOLUME” (grueso)	“ninguna”
`snapshotPolicy`	Política de Snapshot que se debe usar	“ninguna”
`qosPolicy`	Grupo de políticas de calidad de servicio que se asignará a los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	""
`adaptiveQosPolicy`	Grupo de políticas de calidad de servicio adaptativo que permite asignar los volúmenes creados. Elija uno de qosPolicy o adaptiveQosPolicy por pool/back-end de almacenamiento	""
`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	“falso”

Parámetro	Descripción	Predeterminado
`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:

```
Total volume size = [(PVC requested size) / (1 - (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"
```