Pilotes ONTAP NAS

Trident

NetApp
January 15, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/trident-2506/trident-use/ontap-nas.html on January 15, 2026. Always check docs.netapp.com for the latest.

Sommaire

Pilotes ONTAP NAS

Présentation du pilote ONTAP NAS

Découvrez comment configurer un backend ONTAP avec les pilotes NAS ONTAP et Cloud Volumes ONTAP .

Détails du pilote ONTAP NAS

Trident fournit les pilotes de stockage NAS suivants pour communiquer avec le cluster ONTAP . Les modes d'accès pris en charge sont : *ReadWriteOnce* (RWO), *ReadOnlyMany* (ROX), *ReadWriteMany* (RWX), *ReadWriteOncePod* (RWOP).

Conducteur	Protocole	mode de volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
`ontap-nas`	NFS SMB	Système de fichiers	RWO, ROX, RWX, RWOP	"", `nfs` , `smb`
`ontap-nas-economy`	NFS SMB	Système de fichiers	RWO, ROX, RWX, RWOP	"", `nfs` , `smb`
`ontap-nas-flexgroup`	NFS SMB	Système de fichiers	RWO, ROX, RWX, RWOP	"", `nfs` , `smb`

- Utiliser `ontap-san-economy` uniquement si le nombre d'utilisations de volume persistantes devrait être supérieur à"limites de volume ONTAP prises en charge" .
- Utiliser `ontap-nas-economy` uniquement si le nombre d'utilisations de volume persistantes devrait être supérieur à"limites de volume ONTAP prises en charge" et le `ontap-san-economy` Le pilote ne peut pas être utilisé.
- Ne pas utiliser `ontap-nas-economy` si vous prévoyez un besoin en matière de protection des données, de reprise après sinistre ou de mobilité.
- NetApp ne recommande pas l'utilisation de la croissance automatique Flexvol dans tous les pilotes ONTAP , à l'exception de ontap-san. En guise de solution de contournement, Trident prend en charge l'utilisation de la réserve de snapshots et adapte les volumes Flexvol en conséquence.

Autorisations de l'utilisateur

Trident s'attend à être exécuté en tant qu'administrateur ONTAP ou SVM, généralement en utilisant `admin` utilisateur de cluster ou un `vsadmin` Utilisateur SVM, ou un utilisateur portant un nom différent mais ayant le même rôle.

Pour les déploiements Amazon FSx for NetApp ONTAP , Trident s'attend à être exécuté en tant qu'administrateur ONTAP ou SVM, en utilisant le cluster. `fsxadmin` utilisateur ou un `vsadmin` Utilisateur SVM, ou un utilisateur portant un nom différent mais ayant le même rôle. Le `fsxadmin` L'utilisateur est un remplaçant limité pour l'utilisateur administrateur du cluster.

Si vous utilisez le `limitAggregateUsage` Les paramètres suivants sont requis : autorisations d'administrateur de cluster. Lors de l'utilisation Amazon FSx for NetApp ONTAP avec Trident, `limitAggregateUsage` Le paramètre ne fonctionnera pas avec le `vsadmin` et `fsxadmin` comptes utilisateurs. L'opération de configuration échouera si vous spécifiez ce paramètre.

Bien qu'il soit possible de créer un rôle plus restrictif au sein ONTAP qu'un pilote Trident puisse utiliser, nous ne le recommandons pas. La plupart des nouvelles versions de Trident feront appel à des API supplémentaires dont il faudra tenir compte, ce qui rendra les mises à niveau difficiles et sujettes aux erreurs.

Préparez-vous à configurer un serveur dorsal avec des pilotes NAS ONTAP.

Comprendre les exigences, les options d'authentification et les politiques d'exportation pour configurer un backend ONTAP avec les pilotes ONTAP NAS.

Exigences

- Pour tous les backends ONTAP , Trident exige qu'au moins un agrégat soit affecté au SVM.
- Vous pouvez exécuter plusieurs pilotes et créer des classes de stockage qui pointent vers l'un ou l'autre. Par exemple, vous pouvez configurer une classe Gold qui utilise `ontap-nas` pilote et une classe Bronze qui utilise le `ontap-nas-economy` un.
- Tous vos nœuds de travail Kubernetes doivent avoir les outils NFS appropriés installés. Se référer à"ici" pour plus de détails.
- Trident prend uniquement en charge les volumes SMB montés sur des pods exécutés sur des nœuds Windows. Se référer à Préparez-vous à provisionner des volumes PME pour plus de détails.

Authentifier le backend ONTAP

Trident propose deux modes d'authentification pour un système dorsal ONTAP .

- Authentification par identifiants : ce mode nécessite des autorisations suffisantes sur le serveur ONTAP . Il est recommandé d'utiliser un compte associé à un rôle de connexion de sécurité prédéfini, tel que `admin` ou `vsadmin` pour assurer une compatibilité maximale avec les versions ONTAP .
- Mode basé sur un certificat : ce mode nécessite un certificat installé sur le serveur pour que Trident puisse communiquer avec un cluster ONTAP . Ici, la définition du backend doit contenir les valeurs encodées en Base64 du certificat client, de la clé et du certificat d'autorité de certification de confiance si utilisé (recommandé).

Vous pouvez mettre à jour les systèmes d'arrière-plan existants pour passer d'une méthode basée sur les identifiants à une méthode basée sur les certificats. Cependant, une seule méthode d'authentification est prise en charge à la fois. Pour passer à une autre méthode d'authentification, vous devez supprimer la méthode actuelle de la configuration du serveur.

Si vous tentez de fournir **à la fois des identifiants et des certificats**, la création du backend échouera avec une erreur indiquant que plusieurs méthodes d'authentification ont été fournies dans le fichier de configuration.

Activer l'authentification par identifiants

Trident a besoin des identifiants d'un administrateur au niveau SVM/cluster pour communiquer avec le backend ONTAP . Il est recommandé d'utiliser des rôles standard prédéfinis tels que `admin` ou `vsadmin` . Cela garantit la compatibilité ascendante avec les futures versions ONTAP qui pourraient exposer des API de fonctionnalités utilisables par les futures versions de Trident . Il est possible de créer et d'utiliser un rôle de connexion de sécurité personnalisé avec Trident, mais cela n'est pas recommandé.

Voici un exemple de définition de backend :

YAML

```yaml
---
version: 1
backendName: ExampleBackend
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
credentials:
  name: secret-backend-creds
```

JSON

```json
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "credentials": {
        "name": "secret-backend-creds"
    }
}
```

N'oubliez pas que la définition du backend est le seul endroit où les identifiants sont stockés en clair. Une fois le backend créé, les noms d'utilisateur et les mots de passe sont encodés en Base64 et stockés en tant que secrets Kubernetes. La création/mise à jour d'un backend est la seule étape qui nécessite la connaissance des identifiants. Il s'agit donc d'une opération réservée aux administrateurs, qui doit être effectuée par l'administrateur Kubernetes/stockage.

Activer l'authentification par certificat

Les nouveaux et les existants serveurs dorsaux peuvent utiliser un certificat et communiquer avec le serveur dorsal ONTAP . Trois paramètres sont requis dans la définition du backend.

- clientCertificate : valeur du certificat client encodée en Base64.
- clientPrivateKey : valeur encodée en Base64 de la clé privée associée.
- trustedCACertificate : valeur encodée en Base64 du certificat d'autorité de certification de confiance. Si vous utilisez une autorité de certification de confiance, ce paramètre doit être fourni. Ceci peut être ignoré si aucune autorité de certification de confiance n'est utilisée.

Un flux de travail typique comprend les étapes suivantes.

Étapes

1. Générer un certificat client et une clé. Lors de la génération, définissez le nom commun (CN) sur l'utilisateur ONTAP sous lequel s'authentifier.

```
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. Ajouter un certificat d'autorité de certification de confiance au cluster ONTAP . Cela est peut-être déjà géré par l'administrateur du stockage. Ignorer si aucune autorité de certification de confiance n'est utilisée.

```
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. Installez le certificat client et la clé (de l'étape 1) sur le cluster ONTAP .

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

4. Vérifiez que le rôle de connexion de sécurité ONTAP prend en charge `cert` méthode d'authentification.

```
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. Testez l'authentification à l'aide du certificat généré. Remplacez < ONTAP Management LIF> et <nom du serveur virtuel> par l'adresse IP de l'interface de gestion LIF et le nom du SVM. Vous devez vous assurer que le LIF a sa politique de service configurée comme suit : `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. Encodez le certificat, la clé et le certificat d'autorité de certification de confiance au format Base64.

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

7. Créez le backend en utilisant les valeurs obtenues à l'étape précédente.

```
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...Vaaalllluuuueeee",
"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 |
+------------+----------------+--------------------------------------
+--------+---------+
```

Mettez à jour les méthodes d'authentification ou changez les identifiants.

Vous pouvez mettre à jour un système dorsal existant pour utiliser une méthode d'authentification différente ou pour renouveler ses identifiants. Cela fonctionne dans les deux sens : les systèmes d'arrière-plan qui utilisent un nom d'utilisateur/mot de passe peuvent être mis à jour pour utiliser des certificats ; les systèmes d'arrière-plan qui utilisent des certificats peuvent être mis à jour pour utiliser un nom d'utilisateur/mot de passe. Pour ce faire, vous devez supprimer la méthode d'authentification existante et ajouter la nouvelle méthode d'authentification. Utilisez ensuite le fichier backend.json mis à jour contenant les paramètres requis pour exécuter `tridentctl update backend`.

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

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

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

Lors de la rotation des mots de passe, l'administrateur du stockage doit d'abord mettre à jour le mot de passe de l'utilisateur sur ONTAP. Cette étape est suivie d'une mise à jour du système dorsal. Lors de la rotation des certificats, plusieurs certificats peuvent être ajoutés à l'utilisateur. Le système dorsal est ensuite mis à jour pour utiliser le nouveau certificat, après quoi l'ancien certificat peut être supprimé du cluster ONTAP .

La mise à jour d'un système dorsal n'interrompt pas l'accès aux volumes déjà créés et n'a aucun impact sur

les connexions de volumes effectuées ultérieurement. Une mise à jour réussie du système dorsal indique que Trident peut communiquer avec le système dorsal ONTAP et gérer les futures opérations de volume.

Créer un rôle ONTAP personnalisé pour Trident

Vous pouvez créer un rôle de cluster ONTAP avec des privilèges minimaux afin de ne pas avoir à utiliser le rôle d'administrateur ONTAP pour effectuer des opérations dans Trident. Lorsque vous incluez le nom d'utilisateur dans une configuration backend Trident , Trident utilise le rôle de cluster ONTAP que vous avez créé pour effectuer les opérations.

Se référer à"Générateur de rôles personnalisés Trident" pour plus d'informations sur la création de rôles personnalisés Trident .

Utilisation de l'interface de ligne de commande ONTAP

1. Créez un nouveau rôle à l'aide de la commande suivante :

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

2. Créez un nom d'utilisateur pour l'utilisateur Trident :

```
security login create -username <user_name\> -application ontapi
-authmethod <password\> -role <name_of_role_in_step_1\> –vserver
<svm_name\> -comment "user_description"
```

3. Associer le rôle à l'utilisateur :

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

Utilisation du gestionnaire système

Effectuez les étapes suivantes dans ONTAP System Manager :

1. **Créer un rôle personnalisé** :
   a. Pour créer un rôle personnalisé au niveau du cluster, sélectionnez **Cluster > Paramètres**.

      (Ou) Pour créer un rôle personnalisé au niveau de la SVM, sélectionnez **Stockage > Machines virtuelles de stockage > `required SVM` > Paramètres > Utilisateurs et rôles**.

   b. Sélectionnez l'icône flèche (→) à côté de **Utilisateurs et rôles**.
   c. Sélectionnez **+Ajouter** sous **Rôles**.
   d. Définissez les règles du rôle et cliquez sur **Enregistrer**.
2. **Associer le rôle à l'utilisateur Trident * : + Effectuez les étapes suivantes sur la page *Utilisateurs et rôles** :
   a. Sélectionnez l'icône Ajouter **+** sous **Utilisateurs**.
   b. Sélectionnez le nom d'utilisateur requis, puis sélectionnez un rôle dans le menu déroulant **Rôle**.
   c. Cliquez sur **Enregistrer**.

Pour plus d'informations, veuillez consulter les pages suivantes :

- "Rôles personnalisés pour l'administration d' ONTAP"ou"Définir des rôles personnalisés"
- "Collaborer avec les rôles et les utilisateurs"

Gérer les politiques d'exportation NFS

Trident utilise des politiques d'exportation NFS pour contrôler l'accès aux volumes qu'il provisionne.

Trident propose deux options pour la gestion des politiques d'exportation :

- Trident peut gérer dynamiquement la politique d'exportation elle-même ; dans ce mode de fonctionnement, l'administrateur de stockage spécifie une liste de blocs CIDR qui représentent des adresses IP admissibles. Trident ajoute automatiquement à la politique d'exportation, lors de la publication, les adresses IP des nœuds concernés qui se trouvent dans ces plages. Sinon, lorsqu'aucun CIDR n'est spécifié, toutes les adresses IP unicast à portée globale trouvées sur le nœud sur lequel le volume est publié seront ajoutées à la politique d'exportation.
- Les administrateurs de stockage peuvent créer une politique d'exportation et ajouter des règles manuellement. Trident utilise la politique d'exportation par défaut, sauf si un nom de politique d'exportation différent est spécifié dans la configuration.

Gérer dynamiquement les politiques d'exportation

Trident offre la possibilité de gérer dynamiquement les politiques d'exportation pour les systèmes backend ONTAP . Cela permet à l'administrateur du stockage de spécifier un espace d'adressage autorisé pour les adresses IP des nœuds de travail, plutôt que de définir manuellement des règles explicites. Cela simplifie considérablement la gestion des politiques d'exportation ; les modifications apportées à la politique d'exportation ne nécessitent plus d'intervention manuelle sur le cluster de stockage. De plus, cela permet de limiter l'accès au cluster de stockage aux seuls nœuds de travail qui montent des volumes et dont les adresses IP se trouvent dans la plage spécifiée, ce qui permet une gestion précise et automatisée.

> N'utilisez pas la traduction d'adresses réseau (NAT) lorsque vous utilisez des politiques d'exportation dynamiques. Avec NAT, le contrôleur de stockage voit l'adresse NAT frontale et non l'adresse IP réelle de l'hôte ; l'accès sera donc refusé si aucune correspondance n'est trouvée dans les règles d'exportation.

Exemple

Deux options de configuration doivent être utilisées. Voici un exemple de définition de backend :

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

> Lorsque vous utilisez cette fonctionnalité, vous devez vous assurer que la jonction racine de votre SVM dispose d'une stratégie d'exportation préalablement créée avec une règle d'exportation autorisant le bloc CIDR du nœud (telle que la stratégie d'exportation par défaut). Suivez toujours les bonnes pratiques recommandées par NetApp pour dédier une SVM à Trident.

Voici une explication du fonctionnement de cette fonctionnalité à l'aide de l'exemple ci-dessus :

- `autoExportPolicy`est réglé sur `true`. Cela indique que Trident crée une politique d'exportation pour chaque volume provisionné avec ce backend pour le `svm1` SVM et gestion de l'ajout et de la suppression de règles à l'aide de `autoexportCIDRs` blocs d'adresses. Tant qu'un volume n'est pas attaché à un nœud, le volume utilise une politique d'exportation vide, sans aucune règle pour empêcher les accès non autorisés à ce volume. Lorsqu'un volume est publié sur un nœud, Trident crée une politique d'exportation portant le même nom que l'arbre qtree sous-jacent contenant l'adresse IP du nœud dans le bloc CIDR spécifié. Ces adresses IP seront également ajoutées à la politique d'exportation utilisée par le FlexVol volume parent.
  - Par exemple:
    - UUID du serveur dorsal : 403b5326-8482-40db-96d0-d83fb3f4daec
    - `autoExportPolicy`défini à `true`
    - préfixe de stockage `trident`
    - UUID PVC a79bcf5f-7b6d-4a40-9876-e2551f159c1c
    - L'arbre qtree nommé trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c crée une politique d'exportation pour le FlexVol nommé `trident-403b5326-8482-40db96d0-d83fb3f4daec`, une politique d'exportation pour le qtree nommé `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` et une politique d'exportation vide nommée `trident_empty` sur la SVM. Les règles de la politique d'exportation FlexVol seront un sur-ensemble de toutes les règles contenues dans les politiques d'exportation qtree. La stratégie d'exportation vide sera réutilisée par tous les volumes non attachés.
- `autoExportCIDRs`contient une liste de blocs d'adresses. Ce champ est facultatif et sa valeur par défaut est ["0.0.0.0/0", "::/0"]. Si aucune adresse n'est définie, Trident ajoute toutes les adresses unicast à portée globale trouvées sur les nœuds de travail comportant des publications.

Dans cet exemple, le `192.168.0.0/24` Un espace d'adressage est prévu. Cela indique que les adresses IP des nœuds Kubernetes qui se trouvent dans cette plage d'adresses et qui contiennent des publications seront

ajoutées à la politique d'exportation créée par Trident . Lorsque Trident enregistre un nœud sur lequel il s'exécute, il récupère les adresses IP du nœud et les compare aux blocs d'adresses fournis dans `autoExportCIDRs` Au moment de la publication, après avoir filtré les adresses IP, Trident crée les règles de stratégie d'exportation pour les adresses IP clientes du nœud sur lequel il publie.

Vous pouvez mettre à jour `autoExportPolicy` et `autoExportCIDRs` pour les backends une fois que vous les avez créés. Vous pouvez ajouter de nouveaux CIDR pour un backend géré automatiquement ou supprimer les CIDR existants. Soyez prudent lors de la suppression des CIDR afin de vous assurer que les connexions existantes ne sont pas interrompues. Vous pouvez également choisir de désactiver `autoExportPolicy` pour un système dorsal et recourir à une politique d'exportation créée manuellement en cas de besoin. Cela nécessitera de paramétrer le `exportPolicy` paramètre dans votre configuration backend.

Une fois que Trident a créé ou mis à jour un backend, vous pouvez le vérifier à l'aide de `tridentctl` ou le correspondant `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>
      fileSystemType: ext4
```

Lorsqu'un nœud est supprimé, Trident vérifie toutes les politiques d'exportation afin de supprimer les règles d'accès correspondant à ce nœud. En supprimant cette adresse IP de nœud des politiques d'exportation des backends gérés, Trident empêche les montages non autorisés, sauf si cette adresse IP est réutilisée par un nouveau nœud du cluster.

Pour les backends existants, la mise à jour du backend avec `tridentctl update backend` garantit que Trident gère automatiquement les politiques d'exportation. Cela crée deux nouvelles politiques d'exportation nommées d'après l'UUID et le nom qtree du backend lorsque cela est nécessaire. Les volumes présents sur le système dorsal utiliseront les politiques d'exportation nouvellement créées après avoir été démontés puis remontés.

La suppression d'un backend avec des politiques d'exportation gérées automatiquement supprimera la politique d'exportation créée dynamiquement. Si le système dorsal est recréé, il est traité comme un nouveau système dorsal et entraînera la création d'une nouvelle politique d'exportation.

Si l'adresse IP d'un nœud en production est mise à jour, vous devez redémarrer le pod Trident sur ce nœud. Trident mettra ensuite à jour sa politique d'exportation pour les serveurs backend qu'elle gère afin de refléter ce changement d'adresse IP.

Préparez-vous à provisionner des volumes PME

Avec un peu de préparation supplémentaire, vous pouvez provisionner des volumes SMB en utilisant `ontap-nas` conducteurs.

Vous devez configurer les protocoles NFS et SMB/CIFS sur la SVM pour créer un `ontap-nas-economy` Volume SMB pour les clusters ONTAP sur site. Le défaut de configuration de l'un ou l'autre de ces protocoles entraînera l'échec de la création du volume SMB.

`autoExportPolicy`La prise en charge des volumes SMB n'est pas assurée.

Avant de commencer

Avant de pouvoir provisionner des volumes SMB, vous devez disposer des éléments suivants.

- Un cluster Kubernetes avec un nœud contrôleur Linux et au moins un nœud de travail Windows exécutant Windows Server 2022. Trident prend uniquement en charge les volumes SMB montés sur des pods exécutés sur des nœuds Windows.
- Au moins un secret Trident contenant vos informations d'identification Active Directory. Générer des secrets `smbcreds` :

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

- Un proxy CSI configuré comme un service Windows. Pour configurer un `csi-proxy` , se référer à"GitHub : CSI Proxy" ou"GitHub : CSI Proxy pour Windows" pour les nœuds Kubernetes exécutés sous Windows.

Étapes

1. Pour ONTAP sur site, vous pouvez créer un partage SMB en option ou Trident peut en créer un pour vous.

   Les partages SMB sont requis pour Amazon FSx pour ONTAP.

   Vous pouvez créer les partages d'administration SMB de deux manières : soit en utilisant…"Console de gestion Microsoft" composant logiciel enfichable Dossiers partagés ou via l'interface de ligne de commande ONTAP . Pour créer les partages SMB à l'aide de l'interface de ligne de commande ONTAP :

   a. Si nécessaire, créez la structure de chemin d'accès au répertoire partagé.

      Le `vserver cifs share create` Cette commande vérifie le chemin spécifié dans l'option -path lors de la création du partage. Si le chemin spécifié n'existe pas, la commande échoue.

b. Créer un partage SMB associé à la SVM spécifiée :

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

c. Vérifiez que le partage a bien été créé :

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

Se référer à"Créer un partage SMB" pour plus de détails.

2. Lors de la création du backend, vous devez configurer les éléments suivants pour spécifier les volumes SMB. Pour connaître toutes les options de configuration du backend FSx pour ONTAP , veuillez vous référer à"Options et exemples de configuration de FSx pour ONTAP" .

Paramètre	Description	Exemple
`smbShare`	Vous pouvez spécifier l'un des éléments suivants : le nom d'un partage SMB créé à l'aide de la console de gestion Microsoft ou de l'interface de ligne de commande ONTAP ; un nom permettant à Trident de créer le partage SMB ; ou vous pouvez laisser le paramètre vide pour empêcher l'accès aux volumes via un partage commun. Ce paramètre est facultatif pour ONTAP sur site. Ce paramètre est obligatoire pour les serveurs backend Amazon FSx for ONTAP et ne peut pas être vide.	`smb-share`
`nasType`	**Doit être réglé sur `smb` .** Si la valeur est nulle, la valeur par défaut est `nfs` .	`smb`
`securityStyle`	Style de sécurité pour les nouveaux volumes. **Doit être réglé sur `ntfs` ou `mixed` pour les volumes SMB.**	`ntfs`ou `mixed` pour les volumes SMB
`unixPermissions`	Mode pour les nouveaux volumes. **Doit rester vide pour les volumes SMB.**	""

Activer le SMB sécurisé

À partir de la version 25.06, NetApp Trident prend en charge le provisionnement sécurisé des volumes SMB créés à l'aide de `ontap-nas` et `ontap-nas-economy` backends. Lorsque le protocole SMB sécurisé est activé, vous pouvez fournir un accès contrôlé aux partages SMB pour les utilisateurs et les groupes d'utilisateurs Active Directory (AD) à l'aide de listes de contrôle d'accès (ACL).

Points à retenir

- Importer `ontap-nas-economy` Les volumes ne sont pas pris en charge.
- Seuls les clones en lecture seule sont pris en charge pour `ontap-nas-economy` volumes.

- Si le protocole SMB sécurisé est activé, Trident ignorera le partage SMB mentionné dans le système dorsal.
- La mise à jour de l'annotation PVC, de l'annotation de classe de stockage et du champ backend ne met pas à jour la liste de contrôle d'accès (ACL) du partage SMB.
- La liste de contrôle d'accès (ACL) de partage SMB spécifiée dans l'annotation du PVC cloné aura priorité sur celle du PVC source.
- Veillez à fournir des utilisateurs AD valides tout en activant le protocole SMB sécurisé. Les utilisateurs non valides ne seront pas ajoutés à la liste de contrôle d'accès (ACL).
- Si vous fournissez le même utilisateur AD dans le backend, la classe de stockage et le PVC avec des autorisations différentes, la priorité des autorisations sera la suivante : PVC, classe de stockage, puis backend.
- Le protocole SMB sécurisé est pris en charge pour `ontap-nas` S'applique aux importations de volumes gérés et non aux importations de volumes non gérés.

Étapes

1. Spécifiez adAdminUser dans TridentBackendConfig comme indiqué dans l'exemple suivant :

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.193.176.x
  svm: svm0
  useREST: true
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

2. Ajoutez l'annotation dans la classe de stockage.

   Ajoutez le `trident.netapp.io/smbShareAdUser` Annotation à la classe de stockage pour activer le protocole SMB sécurisé sans erreur. La valeur utilisateur spécifiée pour l'annotation `trident.netapp.io/smbShareAdUser` doit être identique au nom d'utilisateur spécifié dans le `smbcreds` secrète. Vous pouvez choisir l'une des options suivantes pour `smbShareAdUserPermission` : `full_control` , `change` , ou `read` . L'autorisation par défaut est `full_control` .

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

1. Créer un PVC.

   L'exemple suivant crée un PVC :

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/snapshotDirectory: "true"
    trident.netapp.io/smbShareAccessControl: |
      read:
        - tridentADtest
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Options et exemples de configuration ONTAP NAS

Apprenez à créer et à utiliser des pilotes ONTAP NAS avec votre installation Trident . Cette section fournit des exemples de configuration backend et des détails sur le mappage des backends aux StorageClasses.

options de configuration du backend

Consultez le tableau suivant pour connaître les options de configuration du backend :

Paramètre	Description	Défaut
`version`		Toujours 1
`storageDriverName`	Nom du pilote de stockage	`ontap-nas`, `ontap-nas-economy` , ou `ontap-nas-flexgroup`
`backendName`	Nom personnalisé ou système de stockage	Nom du conducteur + "_" + dataLIF
`managementLIF`	Adresse IP d'une interface de gestion de cluster ou SVM (LIF) Un nom de domaine pleinement qualifié (FQDN) peut être spécifié. Peut être configuré pour utiliser des adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, comme ceci : `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . Pour une transition MetroCluster sans interruption, consultez la documentation.Exemple de MetroCluster .	"10.0.0.1", "[2001:1234:abcd::fefe]"
`dataLIF`	Adresse IP du protocole LIF. NetApp recommande de spécifier `dataLIF` . Si aucune donnée n'est fournie, Trident récupère les dataLIF à partir du SVM. Vous pouvez spécifier un nom de domaine pleinement qualifié (FQDN) à utiliser pour les opérations de montage NFS, ce qui vous permet de créer un DNS à répartition circulaire pour équilibrer la charge sur plusieurs dataLIF. Peut être modifié après la configuration initiale. Se référer à . Peut être configuré pour utiliser des adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, comme ceci : `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]` . **Omettre pour Metrocluster.** Voir leExemple de MetroCluster .	Adresse spécifiée ou dérivée de la SVM, si non spécifiée (non recommandé)
`svm`	Machine virtuelle de stockage à utiliser **Omettre pour Metrocluster.** Voir leExemple de MetroCluster .	Dérivé d'un SVM `managementLIF` est spécifié
`autoExportPolicy`	Activer la création et la mise à jour automatiques de la politique d'exportation [Booléen]. En utilisant le `autoExportPolicy` et `autoExportCIDRs` Avec certaines options, Trident peut gérer automatiquement les politiques d'exportation.	FAUX
`autoExportCIDRs`	Liste des CIDR à utiliser pour filtrer les adresses IP des nœuds Kubernetes lorsque `autoExportPolicy` est activé. En utilisant le `autoExportPolicy` et `autoExportCIDRs` Avec certaines options, Trident peut gérer automatiquement les politiques d'exportation.	["0.0.0.0/0", "::/0"]`

Paramètre	Description	Défaut
`labels`	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	""
`clientCertificate`	Valeur encodée en Base64 du certificat client. Utilisé pour l'authentification par certificat	""
`clientPrivateKey`	Valeur encodée en Base64 de la clé privée du client. Utilisé pour l'authentification par certificat	""
`trustedCACertificate`	Valeur encodée en Base64 du certificat d'autorité de certification de confiance. Facultatif. Utilisé pour l'authentification par certificat	""
`username`	Nom d'utilisateur pour se connecter au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants. Pour l'authentification Active Directory, voir "Authentifier Trident auprès d'une SVM principale à l'aide des informations d'identification Active Directory".	
`password`	Mot de passe pour se connecter au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants. Pour l'authentification Active Directory, voir "Authentifier Trident auprès d'une SVM principale à l'aide des informations d'identification Active Directory".	
`storagePrefix`	Préfixe utilisé lors de la mise en service de nouveaux volumes dans la SVM. Impossible de le mettre à jour après l'avoir configuré. ⓘ Lors de l'utilisation d'ontap-nas-economy et d'un préfixe de stockage de 24 caractères ou plus, les qtrees n'auront pas le préfixe de stockage intégré, bien qu'il soit présent dans le nom du volume.	"trident"

Paramètre	Description	Défaut
`aggregate`	Agrégat pour le provisionnement (facultatif ; s'il est défini, il doit être affecté au SVM). Pour le `ontap-nas-flexgroup` conducteur, cette option est ignorée. Si aucun agrégat n'est attribué, n'importe lequel des agrégats disponibles peut être utilisé pour provisionner un volume FlexGroup . Lorsque l'agrégat est mis à jour dans SVM, il est automatiquement mis à jour dans Trident par interrogation de SVM sans qu'il soit nécessaire de redémarrer le contrôleur Trident . Lorsque vous avez configuré un agrégat spécifique dans Trident pour provisionner des volumes, si l'agrégat est renommé ou déplacé hors du SVM, le backend passera à l'état d'échec dans Trident lors de l'interrogation de l'agrégat SVM. Vous devez soit modifier l'agrégat pour qu'il soit présent sur la SVM, soit le supprimer complètement pour remettre le serveur en ligne.	""
`limitAggregateUsage`	L'approvisionnement échouera si l'utilisation dépasse ce pourcentage. **Ne s'applique pas à Amazon FSx pour ONTAP**.	"" (non appliqué par défaut)

Paramètre	Description	Défaut
liste d'agrégation flexgroup	Liste des agrégats à provisionner (facultatif ; si défini, doit être affecté au SVM). Tous les agrégats affectés au SVM sont utilisés pour provisionner un volume FlexGroup . Pris en charge par le pilote de stockage **ontap-nas-flexgroup**. Lorsque la liste agrégée est mise à jour dans SVM, la liste est automatiquement mise à jour dans Trident par interrogation de SVM sans qu'il soit nécessaire de redémarrer le contrôleur Trident . Lorsque vous avez configuré une liste d'agrégats spécifique dans Trident pour provisionner des volumes, si la liste d'agrégats est renommée ou déplacée hors de SVM, le backend passera à l'état d'échec dans Trident lors de l'interrogation de l'agrégat SVM. Vous devez soit modifier la liste agrégée pour utiliser une liste présente sur le SVM, soit la supprimer complètement pour remettre le serveur en ligne.	""
`limitVolumeSize`	L'approvisionnement échouera si la taille du volume demandée est supérieure à cette valeur. Il limite également la taille maximale des volumes qu'il gère pour les qtrees, et le `qtreesPerFlexvol` Cette option permet de personnaliser le nombre maximal d'arbres qtree par FlexVol volume	"" (non appliqué par défaut)
`debugTraceFlags`	Indicateurs de débogage à utiliser lors du dépannage. Exemple : {"api":false, "method":true} Ne pas utiliser `debugTraceFlags` sauf si vous effectuez un dépannage et avez besoin d'un journal détaillé.	nul
`nasType`	Configurer la création de volumes NFS ou SMB. Les options sont `nfs` , `smb` ou nul. La valeur nulle correspond par défaut aux volumes NFS.	`nfs`
`nfsMountOptions`	Liste des options de montage NFS séparées par des virgules. Les options de montage des volumes persistants Kubernetes sont normalement spécifiées dans les classes de stockage, mais si aucune option de montage n'est spécifiée dans une classe de stockage, Trident utilisera les options de montage spécifiées dans le fichier de configuration du backend de stockage. Si aucune option de montage n'est spécifiée dans la classe de stockage ou dans le fichier de configuration, Trident ne définira aucune option de montage sur un volume persistant associé.	""

Paramètre	Description	Défaut
`qtreesPerFlexvol`	Nombre maximal d'arbres Q par FlexVol, doit être compris entre 50 et 300.	"200"
`smbShare`	Vous pouvez spécifier l'un des éléments suivants : le nom d'un partage SMB créé à l'aide de la console de gestion Microsoft ou de l'interface de ligne de commande ONTAP ; un nom permettant à Trident de créer le partage SMB ; ou vous pouvez laisser le paramètre vide pour empêcher l'accès aux volumes via un partage commun. Ce paramètre est facultatif pour ONTAP sur site. Ce paramètre est obligatoire pour les serveurs backend Amazon FSx for ONTAP et ne peut pas être vide.	`smb-share`
`useREST`	Paramètre booléen pour utiliser les API REST ONTAP `.useREST`Lorsqu'il est réglé sur `true` Trident utilise les API REST ONTAP pour communiquer avec le système dorsal ; lorsqu'il est configuré pour `false` Trident utilise des appels ONTAPI (ZAPI) pour communiquer avec le backend. Cette fonctionnalité nécessite ONTAP 9.11.1 et versions ultérieures. De plus, le rôle de connexion ONTAP utilisé doit avoir accès à `ontapi` application. Ceci est satisfait par la définition prédéfinie `vsadmin` et `cluster-admin` rôles. À compter de la version Trident 24.06 et ONTAP 9.15.1 ou ultérieure, `useREST` est réglé sur `true` par défaut ; modifier `useREST` à `false` utiliser les appels ONTAPI (ZAPI).	`true`pour ONTAP 9.15.1 ou version ultérieure, sinon `false`.
`limitVolumePoolSize`	Taille maximale de FlexVol pouvant être demandée lors de l'utilisation de Qtrees dans le backend ontap-nas-economy.	"" (non appliqué par défaut)
`denyNewVolumePools`	Restreint `ontap-nas-economy` les backends créant de nouveaux volumes FlexVol pour contenir leurs Qtrees. Seuls les Flexvols préexistants sont utilisés pour provisionner de nouveaux PV.	
`adAdminUser`	Utilisateur administrateur Active Directory ou groupe d'utilisateurs disposant d'un accès complet aux partages SMB. Utilisez ce paramètre pour accorder des droits d'administrateur sur le partage SMB avec un contrôle total.	

Options de configuration backend pour les volumes de provisionnement

Vous pouvez contrôler le provisionnement par défaut à l'aide de ces options dans le `defaults` section de la configuration. Pour un exemple, consultez les exemples de configuration ci-dessous.

Paramètre	Description	Défaut
`spaceAllocation`	Allocation d'espace pour les Qtrees	"vrai"

Paramètre	Description	Défaut
`spaceReserve`	Mode de réservation d'espace ; « aucun » (fin) ou « volume » (épais)	"aucun"
`snapshotPolicy`	Politique d'instantané à utiliser	"aucun"
`qosPolicy`	Groupe de stratégie QoS à attribuer aux volumes créés. Choisissez l'une des options qosPolicy ou adaptiveQosPolicy par pool de stockage/backend.	""
`adaptiveQosPolicy`	Groupe de stratégie QoS adaptatif à attribuer aux volumes créés. Choisissez l'une des options qosPolicy ou adaptiveQosPolicy par pool de stockage/backend. Non pris en charge par ontap-nas-economy.	""
`snapshotReserve`	Pourcentage du volume réservé aux instantanés	"0" si `snapshotPolicy` est « aucun », sinon « »
`splitOnClone`	Séparer un clone de son parent lors de sa création	"FAUX"
`encryption`	Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume ; la valeur par défaut est `false` . Pour utiliser cette option, NVE doit être sous licence et activé sur le cluster. Si NAE est activé sur le système dorsal, tout volume provisionné dans Trident sera compatible NAE. Pour plus d'informations, veuillez consulter :"Comment Trident fonctionne avec NVE et NAE" .	"FAUX"
`tieringPolicy`	Politique de hiérarchisation : utiliser « aucun »	
`unixPermissions`	Mode pour les nouveaux volumes	« 777 » pour les volumes NFS ; vide (non applicable) pour les volumes SMB
`snapshotDir`	Contrôle l'accès à `.snapshot` annuaire	« Vrai » pour NFSv4, « Faux » pour NFSv3
`exportPolicy`	Politique d'exportation à utiliser	"défaut"
`securityStyle`	Style de sécurité pour les nouveaux volumes. NFS prend en charge `mixed` et `unix` Styles de sécurité. Les PME prennent en charge `mixed` et `ntfs` Styles de sécurité.	La valeur par défaut de NFS est `unix` . La valeur par défaut de SMB est `ntfs` .
`nameTemplate`	Modèle pour créer des noms de volumes personnalisés.	""

L'utilisation des groupes de politiques QoS avec Trident nécessite ONTAP 9.8 ou une version ultérieure. Vous devez utiliser un groupe de stratégies QoS non partagé et vous assurer que ce groupe de stratégies est appliqué individuellement à chaque composant. Un groupe de politiques QoS partagé impose un plafond au débit total de toutes les charges de travail.

Exemples de provisionnement de volumes

Voici un exemple avec des valeurs par défaut définies :

```
---
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"
```

Pour `ontap-nas` et `ontap-nas-flexgroups` Trident utilise désormais un nouveau calcul pour garantir que le FlexVol est correctement dimensionné avec le pourcentage snapshotReserve et le PVC. Lorsqu'un utilisateur demande un PVC, Trident crée le FlexVol d'origine avec plus d'espace grâce à ce nouveau calcul. Ce calcul garantit que l'utilisateur reçoit l'espace inscriptible demandé dans le PVC, et non un espace inférieur. Avant la version 21.07, lorsqu'un utilisateur demandait un PVC (par exemple, 5 Gio), avec un snapshotReserve à 50 %, il ne recevait que 2,5 Gio d'espace inscriptible. En effet, l'utilisateur a demandé le volume entier et `snapshotReserve` est un pourcentage de cela. Avec Trident 21.07, ce que l'utilisateur demande, c'est l'espace inscriptible, et Trident définit cet espace. `snapshotReserve` nombre en pourcentage du volume total. Cela ne s'applique pas à `ontap-nas-economy` . Consultez l'exemple suivant pour voir comment cela fonctionne :

Le calcul est le suivant :

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

Pour snapshotReserve = 50 % et une demande PVC = 5 Gio, la taille totale du volume est de 5/0,5 = 10 Gio et la taille disponible est de 5 Gio, ce qui correspond à ce que l'utilisateur a demandé dans la demande PVC Le

`volume show` La commande devrait afficher des résultats similaires à cet exemple :

Les backends existants des installations précédentes provisionneront les volumes comme expliqué ci-dessus lors de la mise à niveau de Trident. Pour les volumes créés avant la mise à niveau, vous devez les redimensionner afin que la modification soit prise en compte. Par exemple, un PVC de 2 Gio avec `snapshotReserve=50` Cela a précédemment abouti à un volume offrant 1 Gio d'espace inscriptible. Par exemple, le redimensionnement à 3 Gio permet à l'application de disposer de 3 Gio d'espace inscriptible sur un volume de 6 Gio.

Exemples de configuration minimale

Les exemples suivants présentent des configurations de base qui laissent la plupart des paramètres par défaut. Voici la manière la plus simple de définir un backend.

> Si vous utilisez Amazon FSx sur NetApp ONTAP avec Trident, il est recommandé de spécifier les noms DNS des LIF au lieu des adresses IP.

Exemple d'économie NAS ONTAP

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

Exemple de groupe flexible ONTAP NAS

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

Exemple de MetroCluster

Vous pouvez configurer le système dorsal pour éviter d'avoir à mettre à jour manuellement sa définition après un basculement et un retour en arrière."Réplication et récupération SVM" .

Pour une transition et un retour en arrière sans interruption, spécifiez le SVM en utilisant `managementLIF` et omettre le `dataLIF` et `svm` paramètres. Par exemple:

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

Exemple de volumes SMB

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

Exemple d'authentification par certificat

Voici un exemple de configuration minimale du backend. `clientCertificate` , `clientPrivateKey` , et `trustedCACertificate` (facultatif, si vous utilisez une autorité de certification de confiance) sont renseignés dans `backend.json` et prendre respectivement les valeurs encodées en base64 du certificat client, de la clé privée et du certificat d'autorité de certification de confiance.

```
---
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_
```

Exemple de politique d'exportation automatique

Cet exemple vous montre comment configurer Trident pour qu'il utilise des politiques d'exportation dynamiques afin de créer et de gérer automatiquement la politique d'exportation. Cela fonctionne de la même manière pour le `ontap-nas-economy` et `ontap-nas-flexgroup` conducteurs.

```
---
version: 1
storageDriverName: ontap-nas
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: svm_nfs
labels:
  k8scluster: test-cluster-east-1a
  backend: test1-nasbackend
autoExportPolicy: true
autoExportCIDRs:
- 10.0.0.0/24
username: admin
password: password
nfsMountOptions: nfsvers=4
```

Exemple d'adresses IPv6

Cet exemple montre `managementLIF` en utilisant une adresse IPv6.

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

Exemple d'utilisation Amazon FSx pour ONTAP avec des volumes SMB

Le `smbShare` Ce paramètre est requis pour FSx for ONTAP utilisant des volumes SMB.

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

Exemple de configuration backend avec nameTemplate

```
---
version: 1
storageDriverName: ontap-nas
backendName: ontap-nas-backend
managementLIF: <ip address>
svm: svm0
username: <admin>
password: <password>
defaults:
  nameTemplate:
"{{.volume.Name}}_{{.labels.cluster}}_{{.volume.Namespace}}_{{.vo\
    lume.RequestName}}"
labels:
  cluster: ClusterA
  PVC: "{{.volume.Namespace}}_{{.volume.RequestName}}"
```

Exemples de serveurs backend avec pools virtuels

Dans les exemples de fichiers de définition de backend présentés ci-dessous, des valeurs par défaut spécifiques sont définies pour tous les pools de stockage, telles que : `spaceReserve` à aucun, `spaceAllocation` à faux, et `encryption` à faux. Les pools virtuels sont définis dans la section stockage.

Trident définit les étiquettes de provisionnement dans le champ « Commentaires ». Des commentaires sont disponibles sur FlexVol pour `ontap-nas` ou FlexGroup pour `ontap-nas-flexgroup` . Lors de la mise en service, Trident copie toutes les étiquettes présentes sur un pool virtuel vers le volume de stockage. Pour plus de commodité, les administrateurs de stockage peuvent définir des étiquettes par pool virtuel et regrouper les volumes par étiquette.

Dans ces exemples, certains pools de stockage définissent leurs propres paramètres `spaceReserve` , `spaceAllocation` , et `encryption` valeurs, et certains pools remplacent les valeurs par défaut.

Exemple de NAS ONTAP

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

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

Exemple de FlexGroup NAS ONTAP

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

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

Exemple d'économie NAS ONTAP

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

```
      encryption: "false"
      unixPermissions: "0775"
```

Associer les backends aux StorageClasses

Les définitions de StorageClass suivantes font référence àExemples de serveurs backend avec pools virtuels . En utilisant le `parameters.selector` Dans ce champ, chaque StorageClass indique quels pools virtuels peuvent être utilisés pour héberger un volume. Le volume aura les aspects définis dans le pool virtuel choisi.

- Le `protection-gold` StorageClass sera associé au premier et au deuxième pool virtuel dans le `ontap-nas-flexgroup` backend. Ce sont les seules piscines à offrir une protection de niveau or.

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

- Le `protection-not-gold` StorageClass sera associé au troisième et au quatrième pool virtuel dans le `ontap-nas-flexgroup` backend. Ce sont les seuls pools offrant un niveau de protection autre que l'or.

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

- Le `app-mysqldb` StorageClass sera associé au quatrième pool virtuel dans le `ontap-nas` backend. Il s'agit du seul pool offrant une configuration de pool de stockage pour les applications de type mysqldb.

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

- Le `protection-silver-creditpoints-20k` StorageClass sera associé au troisième pool virtuel dans le `ontap-nas-flexgroup` backend. Il s'agit du seul fonds de placement offrant une protection de niveau argent et 20 000 points de crédit.

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

- Le `creditpoints-5k` StorageClass sera associé au troisième pool virtuel dans le `ontap-nas` le backend et le deuxième pool virtuel dans le `ontap-nas-economy` backend. Ce sont les seules offres de piscine avec 5000 points de crédit.

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

Trident déterminera quel pool virtuel sera sélectionné et s'assurera que les besoins en stockage sont satisfaits.

Mise à jour `dataLIF` après la configuration initiale

Vous pouvez modifier le dataLIF après la configuration initiale en exécutant la commande suivante pour fournir le nouveau fichier JSON backend avec le dataLIF mis à jour.

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

Si des PVC sont connectés à un ou plusieurs pods, vous devez mettre hors service tous les pods correspondants, puis les remettre en service pour que la nouvelle interface dataLIF prenne effet.

Exemples de PME sécurisées

Configuration du backend avec le pilote ontap-nas

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configuration du backend avec le pilote ontap-nas-economy

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas-economy
  managementLIF: 10.0.0.1
  svm: svm2
  nasType: smb
  defaults:
    adAdminUser: tridentADtest
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Configuration du backend avec pool de stockage

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  svm: svm0
  useREST: false
  storage:
  - labels:
      app: msoffice
    defaults:
      adAdminUser: tridentADuser
  nasType: smb
  credentials:
    name: backend-tbc-ontap-invest-secret
```

Exemple de classe de stockage avec le pilote ontap-nas

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADtest
parameters:
  backendType: ontap-nas
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Assurez-vous d'ajouter `annotations` pour activer le SMB sécurisé. Le protocole SMB sécurisé ne fonctionne pas sans les annotations, quelles que soient les configurations définies dans le backend ou le PVC.

Exemple de classe de stockage avec le pilote ontap-nas-economy

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-smb-sc
  annotations:
    trident.netapp.io/smbShareAdUserPermission: change
    trident.netapp.io/smbShareAdUser: tridentADuser3
parameters:
  backendType: ontap-nas-economy
  csi.storage.k8s.io/node-stage-secret-name: smbcreds
  csi.storage.k8s.io/node-stage-secret-namespace: trident
  trident.netapp.io/nasType: smb
provisioner: csi.trident.netapp.io
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

Exemple de PVC avec un seul utilisateur AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-pvc4
  namespace: trident
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      change:
        - tridentADtest
      read:
        - tridentADuser
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-smb-sc
```

Exemple de PVC avec plusieurs utilisateurs AD

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: my-test-pvc
  annotations:
    trident.netapp.io/smbShareAccessControl: |
      full_control:
        - tridentTestuser
        - tridentuser
        - tridentTestuser1
        - tridentuser1
      change:
        - tridentADuser
        - tridentADuser1
        - tridentADuser4
        - tridentTestuser2
      read:
        - tridentTestuser2
        - tridentTestuser3
        - tridentADuser2
        - tridentADuser3
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.