



Pilotes ONTAP NAS

Trident

NetApp
October 30, 2026

Sommaire

Pilotes ONTAP NAS	1
Présentation du pilote ONTAP NAS	1
Détails du pilote ONTAP NAS	1
Autorisations de l'utilisateur	1
Préparez-vous à configurer un backend avec les pilotes NAS ONTAP	2
Exigences	2
Authentifier le backend ONTAP	2
Gérer les règles d'export NFS	8
Préparez-vous à provisionner des volumes SMB	10
Options et exemples de configuration NAS ONTAP	14
Options de configuration du backend	14
Options de configuration backend pour le provisionnement des volumes	19
Exemples de configuration minimale	22
Exemples de backends avec pools virtuels	26
Map backends vers StorageClasses	29
Mise à jour dataLIF après la configuration initiale	31
Exemples de SMB sécurisés	31

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).

Pilote	Protocole	volumeMode	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



- Utilisez `ontap-san-economy` uniquement si le nombre d'utilisations du volume persistant doit être supérieur à "[limites de volume ONTAP prises en charge](#)".
- Utilisez `ontap-nas-economy` uniquement si le nombre d'utilisations de volumes persistants est censé être supérieur à "[limites de volume ONTAP prises en charge](#)" et que le pilote `ontap-san-economy` ne peut pas être utilisé.
- N'utilisez pas `ontap-nas-economy` si vous prévoyez un besoin de protection des données, de reprise après sinistre ou de mobilité.
- NetApp ne recommande pas d'utiliser la croissance automatique FlexVol® dans tous les pilotes ONTAP, sauf `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 doit être exécuté en tant qu'administrateur ONTAP ou SVM, généralement en utilisant l'``admin`` utilisateur cluster ou un ``vsadmin`` utilisateur SVM, ou un utilisateur avec un nom différent ayant le même rôle.

Pour les déploiements Amazon FSx for NetApp ONTAP, Trident doit être exécuté en tant qu'administrateur ONTAP ou SVM, en utilisant l'utilisateur cluster `fsxadmin` ou un ``vsadmin`` utilisateur SVM, ou un utilisateur avec un nom différent ayant le même rôle. L' `fsxadmin` utilisateur est un remplacement limité pour l'utilisateur administrateur du cluster.



Si vous utilisez le `limitAggregateUsage` paramètre, des autorisations d'administrateur de cluster sont requises. Lors de l'utilisation d'Amazon FSx for NetApp ONTAP avec Trident, le

`limitAggregateUsage` paramètre ne fonctionnera pas avec les comptes d'utilisateur `vsadmin` et `fsxadmin`. L'opération de configuration échouera si vous spécifiez ce paramètre.

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

Préparez-vous à configurer un backend avec les pilotes NAS ONTAP

Comprenez les exigences, les options d'authentification et les règles d'export pour configurer un backend ONTAP avec les pilotes ONTAP NAS. À partir de la version 25.10, NetApp Trident prend en charge ["NetApp système de stockage AFX"](#). Les systèmes de stockage NetApp AFX diffèrent des autres systèmes ONTAP (ASA, AFF et FAS) dans l'implémentation de leur couche de stockage. Dans la configuration du backend Trident, il n'est pas nécessaire de préciser que votre système est AFX. Lorsque vous sélectionnez `ontap-nas` comme `storageDriverName`, Trident détecte automatiquement les systèmes AFX.



Seul le `ontap-nas` driver (avec le protocole NFS) est pris en charge pour les systèmes AFX; le protocole SMB n'est pas pris en charge.

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 le `ontap-nas` driver et une classe Bronze qui utilise le `ontap-nas-economy` driver.
- Tous vos nœuds de travail Kubernetes doivent disposer des outils NFS appropriés. Consultez ["ici"](#) pour plus de détails.
- Trident prend uniquement en charge les volumes SMB montés sur des pods exécutés sur des nœuds Windows. Consultez [Préparez-vous à provisionner des volumes SMB](#) pour plus de détails.

Authentifier le backend ONTAP

Trident propose deux modes d'authentification pour un backend ONTAP.

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

Vous pouvez mettre à jour les backends existants pour basculer entre les méthodes basées sur les identifiants et celles basées 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 existante de la

configuration du backend.



Si vous tentez de fournir **à la fois des informations d'identification et des certificats**, la création du backend échouera avec une erreur indiquant que plus d'une méthode d'authentification a été fournie dans le fichier de configuration.

Activer l'authentification basée sur les identifiants

Trident requiert les identifiants d'un administrateur au niveau SVM ou au niveau 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 avec les futures versions d'ONTAP qui pourraient exposer des API de fonctionnalités à utiliser par les futures versions de Trident. Un rôle de connexion de sécurité personnalisé peut être créé et utilisé avec Trident, mais cela n'est pas recommandé.

Voici un exemple de définition de backend :

YAML

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

JSON

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

Il est important de noter que la définition du backend est le seul endroit où les identifiants sont stockés en clair. Après la création du backend, les noms d'utilisateur et mots de passe sont encodés avec Base64 et stockés comme secrets Kubernetes. La création/la mise à jour d'un backend est la seule étape nécessitant la connaissance des identifiants. En tant que telle, il s'agit d'une opération réservée à l'administrateur Kubernetes/stockage.

Activer l'authentification par certificat

Les nouveaux et les anciens backends peuvent utiliser un certificat et communiquer avec le backend ONTAP. Trois paramètres sont requis dans la définition du backend.

- `clientCertificate`: Valeur codée en Base64 du certificat client.
- `clientPrivateKey` : valeur encodée en Base64 de la clé privée associée.
- `trustedCACertificate` : valeur encodée en Base64 du certificat CA de confiance. Si vous utilisez un CA de confiance, ce paramètre doit être fourni. Cela peut être ignoré si aucun CA de confiance n'est utilisé.

Un workflow typique implique les étapes suivantes.

Étapes

1. Générez un certificat client et une clé. Lors de la génération, définissez le nom commun (CN) sur l'utilisateur ONTAP à 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. Ajoutez un certificat d'autorité de certification de confiance au cluster ONTAP. Cette opération peut déjà être effectuée par l'administrateur de stockage. Ignorez 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. Confirmez que le rôle de connexion de sécurité ONTAP prend en charge cert la 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 <vserver name> par l'adresse IP de la LIF de gestion et le nom SVM. Vous devez vous assurer que le LIF a sa

stratégie de service définie sur 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 avec 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...Vaaalllluuuuueeee",  
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",  
  "storagePrefix": "myPrefix_"  
}  
  
#Update backend with tridentctl  
tridentctl update backend NasBackend -f cert-backend-updated.json -n  
trident  
  
+-----+-----+-----+-----+  
+-----+-----+  
|   NAME   | STORAGE DRIVER |           UUID           |  
STATE | VOLUMES |  
+-----+-----+-----+-----+  
+-----+-----+  
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |  
online |          9 |  
+-----+-----+-----+-----+  
+-----+-----+
```

Mettez à jour les méthodes d'authentification ou faites pivoter les identifiants

Vous pouvez mettre à jour un backend existant pour utiliser une méthode d'authentification différente ou pour faire pivoter ses identifiants. Cela fonctionne dans les deux sens : les backends qui utilisent un nom d'utilisateur/mot de passe peuvent être mis à jour pour utiliser des certificats ; les backends 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. Ensuite, utilisez 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 du renouvellement des mots de passe, l'administrateur du stockage doit d'abord mettre à jour le mot de passe de l'utilisateur sur ONTAP. Cette opération est suivie d'une mise à jour du backend. Lors du renouvellement des certificats, plusieurs certificats peuvent être associés à l'utilisateur. Le backend 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 backend n'interrompt pas l'accès aux volumes déjà créés et n'affecte pas les connexions

de volumes établies ultérieurement. Une mise à jour réussie du backend indique que Trident peut communiquer avec le backend ONTAP et gérer les futures opérations sur les volumes.

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.

Reportez-vous 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. Associez le rôle à l'utilisateur :

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

Utilisation de System Manager

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 > Settings**.

(Ou) Pour créer un rôle personnalisé au niveau de la SVM, sélectionnez **Storage > Storage VMs > required svm > Paramètres > Utilisateurs et rôles**.

- b. Sélectionnez l'icône flèche (→) à côté de **Users and Roles**.
- c. Sélectionnez **+Add** sous **Roles**.
- d. Définissez les règles du rôle et cliquez sur **Save**.

2. **Associez le rôle à l'utilisateur Trident :** + Effectuez les étapes suivantes sur la page **Utilisateurs et rôles** :

- a. Sélectionnez l'icône Ajouter + sous **Users**.
- b. Sélectionnez le nom d'utilisateur requis, puis sélectionnez un rôle dans le menu déroulant pour **Rôle**.
- c. Cliquez sur **Enregistrer**.

Reportez-vous aux pages suivantes pour plus d'informations :

- ["Rôles personnalisés pour l'administration d'ONTAP"](#) ou ["Définir des rôles personnalisés"](#)
- ["Travailler avec les rôles et les utilisateurs"](#)

Gérer les règles d'export NFS

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

Trident propose deux options lors de l'utilisation des règles d'export :

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

Gérer dynamiquement les règles d'export

Trident offre la possibilité de gérer dynamiquement les règles d'export pour les backends ONTAP. Cela donne à l'administrateur de stockage la possibilité de spécifier un espace d'adresses autorisé pour les adresses IP des nœuds de travail, plutôt que de définir manuellement des règles explicites. Cela simplifie grandement la gestion des règles d'export ; les modifications apportées à la règle d'export ne nécessitent plus d'intervention manuelle sur le cluster de stockage. De plus, cela permet de restreindre l'accès au cluster de stockage uniquement aux nœuds de travail qui montent des volumes et dont les adresses IP se trouvent dans la plage spécifiée, ce qui permet une gestion fine et automatisée.



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

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 possède une règle d'export précédemment créée avec une règle d'export autorisant le bloc CIDR du nœud (par exemple, la règle d'export par défaut). Suivez toujours la bonne pratique recommandée 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 défini sur `true`. Cela indique que Trident crée une règle d'export pour chaque volume provisionné avec ce backend pour la `svm1` SVM et gère l'ajout et la suppression de règles à l'aide de blocs d'adresses `autoexportCIDRs`. Jusqu'à ce qu'un volume soit attaché à un nœud, le volume utilise une règle d'export vide sans aucune règle afin d'empêcher tout accès non désiré à ce volume. Lorsqu'un volume est publié sur un nœud, Trident crée une règle d'export portant le même nom que le qtree sous-jacent contenant l'adresse IP du nœud dans le bloc CIDR spécifié. Ces adresses IP seront également ajoutées à la règle d'export utilisée par le volume FlexVol parent.
 - Par exemple :
 - UUID de backend `403b5326-8482-40db-96d0-d83fb3f4daec`
 - `autoExportPolicy` défini sur `true`
 - préfixe de stockage `trident`
 - UUID PVC `a79bcf5f-7b6d-4a40-9876-e2551f159c1c`
 - Le qtree nommé `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c` crée une règle d'export pour le FlexVol nommé `trident-403b5326-8482-40db96d0-d83fb3f4daec`, une règle d'export pour le qtree nommé `trident_pvc_a79bcf5f_7b6d_4a40_9876_e2551f159c1c`, et une règle d'export vide nommée `trident_empty` sur la SVM. Les règles de la règle d'export du FlexVol seront un sur-ensemble de toutes les règles contenues dans les règles d'export du qtree. La règle d'export vide sera réutilisée par tous les volumes qui ne sont pas attachés.
- `autoExportCIDRs` contient une liste de blocs d'adresses. Ce champ est facultatif et il est défini par défaut sur `["0.0.0.0/0", "::/0"]`. S'il n'est pas défini, Trident ajoute toutes les adresses unicast à portée globale trouvées sur les nœuds de travail avec des publications.

Dans cet exemple, l' `192.168.0.0/24` espace d'adresses est fourni. Cela indique que les adresses IP des nœuds Kubernetes qui se trouvent dans cette plage d'adresses avec des publications seront ajoutées à la règles d'export que Trident crée. Lorsque Trident enregistre un nœud sur lequel il s'exécute, il récupère les adresses IP du nœud et les vérifie par rapport aux blocs d'adresses fournis dans `autoExportCIDRs`. Au moment de la publication, après avoir filtré les adresses IP, Trident crée les règles d'export pour les adresses IP clientes du nœud auquel il publie.

Vous pouvez mettre à jour `autoExportPolicy` et `autoExportCIDRs` pour les backends après leur création. Vous pouvez ajouter de nouveaux CIDR pour un backend géré automatiquement ou supprimer les CIDR existants. Faites attention lors de la suppression de CIDR afin de garantir que les connexions existantes ne soient pas interrompues. Vous pouvez également choisir de désactiver `autoExportPolicy` pour un backend et revenir à une règle d'export créée manuellement. Cela nécessitera de définir le paramètre `exportPolicy` dans la configuration de votre backend.

Après que Trident a créé ou mis à jour un backend, vous pouvez vérifier le backend en utilisant `tridentctl` ou le CRD correspondant `tridentbackend` :

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

Lorsqu'un nœud est supprimé, Trident vérifie toutes les règles d'export afin de supprimer les règles d'accès correspondantes au nœud. En supprimant cette adresse IP de nœud des règles d'export des backends gérés, Trident empêche les montages non autorisés, sauf si cette adresse IP est réutilisée par un nouveau nœud dans le cluster.

Pour les backends existants, la mise à jour du backend avec `tridentctl update backend` garantit que Trident gère automatiquement les règles d'export. Cela crée deux nouvelles règles d'export nommées d'après l'UUID du backend et le nom du qtrees lorsqu'elles sont nécessaires. Les volumes présents sur le backend utiliseront les nouvelles règles d'export après avoir été démontés puis remontés.



La suppression d'un backend avec des règles d'export gérées automatiquement supprimera la règle d'export créée dynamiquement. Si le backend est recréé, il est traité comme un nouveau backend et cela entraînera la création d'une nouvelle règle d'export.

Si l'adresse IP d'un nœud en production est modifiée, vous devez redémarrer le pod Trident sur ce nœud. Trident mettra alors à jour la règle d'export pour les backends qu'il gère afin de refléter ce changement d'adresse IP.

Préparez-vous à provisionner des volumes SMB

Avec un peu de préparation supplémentaire, vous pouvez provisionner des volumes SMB à l'aide de `ontap-nas drivers`.



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. L'absence de configuration de l'un ou l'autre de ces protocoles entraînera l'échec de la création du volume SMB.



autoExportPolicy n'est pas pris en charge pour les volumes SMB.

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 identifiants Active Directory. Pour générer le secret `smbcreds` :

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

- Un proxy CSI configuré en tant que service Windows. Pour configurer un `csi-proxy`, reportez-vous 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 éventuellement créer un partage SMB 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 à l'aide du ["Microsoft Management Console"](#) Shared Folders snap-in, soit à l'aide de 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 du chemin d'accès du répertoire pour le partage.

La ``vserver cifs share create`` 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 été créé :

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



Reportez-vous 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 toutes les options de configuration du backend FSx pour ONTAP, reportez-vous à ["Options de](#)

Paramètre	Description	Exemple
smbShare	Vous pouvez spécifier l'une des options suivantes : 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 pour permettre à Trident de créer le partage SMB ; ou vous pouvez laisser le paramètre vide pour empêcher l'accès partagé aux volumes. Ce paramètre est facultatif pour ONTAP sur site. Ce paramètre est obligatoire pour Amazon FSx for ONTAP backends et ne peut pas être vide.	smb-share
nasType	Doit être défini sur smb. Si nul, la valeur par défaut est nfs.	smb
securityStyle	Style de sécurité pour les nouveaux volumes. Doit être défini sur ntfs ou mixed pour les volumes SMB.	ntfs or 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` serveurs backend. Lorsque le protocole SMB sécurisé est activé, vous pouvez fournir un accès contrôlé aux partages SMB pour les utilisateurs et groupes d'utilisateurs Active Directory (AD) à l'aide des listes de contrôle d'accès (ACL).

Points à retenir

- L'importation `ontap-nas-economy` de volumes n'est pas prise 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 backend.
- La mise à jour de l'annotation PVC, de l'annotation de classe de stockage et du champ backend ne met pas à jour l'ACL du partage SMB.
- La liste de contrôle d'accès (ACL) de partage SMB spécifiée dans l'annotation du PVC cloné aura priorité sur celles du PVC source.
- Veillez à fournir des utilisateurs AD valides lors de l'activation du protocole SMB sécurisé. Les utilisateurs non valides ne seront pas ajoutés à l'ACL.
- Si vous fournissez le même utilisateur AD dans le backend, la storage class et le PVC avec des autorisations différentes, la priorité des autorisations sera : PVC, storage class, puis backend.
- Le protocole SMB sécurisé est pris en charge pour `ontap-nas` les importations de volumes gérés et n'est pas applicable 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 l'`trident.netapp.io/smbShareAdUser` annotation à la classe de stockage pour activer SMB sécurisé sans faute. La valeur utilisateur spécifiée pour l'annotation `trident.netapp.io/smbShareAdUser` doit être identique au nom d'utilisateur indiqué dans le `smbcreds` secret. 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 NAS ONTAP

Créez et utilisez les pilotes NAS ONTAP avec votre installation Trident. Cette section fournit des exemples de configuration backend et des détails pour le mappage des backends vers les StorageClasses. À partir de la version 25.10, NetApp Trident prend en charge ["NetApp AFX systèmes de stockage"](#). Les systèmes de stockage NetApp AFX diffèrent des autres systèmes basés sur ONTAP (ASA, AFF et FAS) par l'implémentation de leur couche de stockage.



Seul le `ontap-nas` driver (avec le protocole NFS) est pris en charge pour les systèmes NetApp AFX ; le protocole SMB n'est pas pris en charge.

Options de configuration du backend

Dans la configuration du backend Trident, il n'est pas nécessaire de préciser que votre système est un NetApp AFX storage system. Lorsque vous sélectionnez `ontap-nas` comme `storageDriverName`, Trident détecte automatiquement le système de stockage AFX. Certains paramètres de configuration du backend ne sont pas applicables aux systèmes de stockage AFX.

À partir de la version 26.06, vous pouvez activer le placement équilibré ONTAP afin qu'ONTAP sélectionne l'agrégat pour les nouveaux volumes. Le placement équilibré est requis pour les systèmes de stockage AFX sur ONTAP 9.19.1 ou version ultérieure. Consultez ["Utilisez un placement équilibré avec les backends ONTAP"](#) pour connaître les exigences et obtenir des exemples.

Le tableau suivant présente les options de configuration du backend :

Paramètre	Description	Défaut
version		Toujours 1

Paramètre	Description	Défaut
storageDriverName	<p>Nom du pilote de stockage.</p> <p>Ne peut pas être modifié après création. Pour mettre à jour ce paramètre, vous devez créer un nouveau backend.</p> <div>  <p>Pour les systèmes NetApp AFX, seul <code>ontap-nas</code> est pris en charge.</p> </div>	<code>ontap-nas</code> , <code>ontap-nas-economy</code> , ou <code>ontap-nas-flexgroup</code>
backendName	Nom personnalisé ou le stockage backend	Nom du pilote + "_" + <code>dataLIF</code>
managementLIF	<p>Adresse IP d'un cluster ou d'une LIF de gestion SVM. Un nom de domaine complet (FQDN) peut être spécifié. Il est possible de configurer l'utilisation d'adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, comme <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>. Pour une transition en douceur MetroCluster, consultez le Exemple MetroCluster.</p>	<code>"10.0.0.1"</code> , <code>"[2001:1234:abcd::fefe]"</code>
dataLIF	<p>Adresse IP de l'interface logique de protocole (LIF). NetApp recommande de spécifier <code>dataLIF</code>. Si elle n'est pas fournie, Trident récupère les <code>dataLIF</code> depuis la SVM. Vous pouvez spécifier un nom de domaine complet (FQDN) à utiliser pour les opérations de montage NFS, ce qui vous permet de créer un DNS à répartition de charge (round-robin) entre plusieurs <code>dataLIF</code>. Peut être modifié après la configuration initiale. Reportez-vous à . Il est possible de configurer l'utilisation d'adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, comme <code>[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]</code>. Omettre pour MetroCluster. Voir le Exemple MetroCluster.</p>	Adresse spécifiée ou dérivée de la SVM, si non spécifiée (non recommandé)
svm	Machine virtuelle de stockage à utiliser Omettre pour MetroCluster. Voir le Exemple MetroCluster .	Dérivé si un SVM <code>managementLIF</code> est spécifié
autoExportPolicy	Activer la création et la mise à jour automatiques des règles d'export [Booléen]. En utilisant les options <code>autoExportPolicy</code> et <code>autoExportCIDRs</code> , Trident peut gérer les règles d'export automatiquement.	<code>false</code>
autoExportCIDRs	Liste des CIDR pour filtrer les adresses IP des nœuds Kubernetes lorsque <code>autoExportPolicy</code> est activé. En utilisant les options <code>autoExportPolicy</code> et <code>autoExportCIDRs</code> , Trident peut gérer les règles d'export automatiquement.	<code>["0.0.0.0/0", ":::0"]</code>
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	<code>""</code>

Paramètre	Description	Défaut
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 par identifiants. Pour l'authentification Active Directory, voir "Authentifier Trident auprès d'un SVM backend à l'aide des identifiants Active Directory" .	
password	Mot de passe pour se connecter au cluster/SVM. Utilisé pour l'authentification par identifiants. Pour l'authentification Active Directory, voir "Authentifier Trident auprès d'un SVM backend à l'aide des identifiants Active Directory" .	
storagePrefix	<p>Préfixe utilisé lors du provisionnement de nouveaux volumes dans la SVM. Ne peut pas être modifié après sa définition</p> <div>  <p>Lors de l'utilisation d'ontap-nas-economy et d'un storagePrefix de 24 caractères ou plus, les qtrees n'intègrent pas le préfixe de stockage, bien qu'il soit présent dans le nom du volume.</p> </div>	"Trident"

Paramètre	Description	Défaut
aggregate	<p>Agrégat pour le provisionnement (facultatif ; s'il est défini, il doit être attribué à la SVM). Pour le <code>ontap-nas-flexgroup</code> driver, cette option est ignorée. S'il n'est pas attribué, n'importe quel agrégat disponible peut être utilisé pour provisionner un FlexGroup volume.</p> <div>  <p>Lorsqu'un 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. Si vous avez configuré un agrégat spécifique dans Trident pour provisionner des volumes, et que cet agrégat est renommé ou déplacé hors de la SVM, le backend passe en état d'échec dans Trident lors de l'interrogation de l'agrégat SVM. Vous devez soit remplacer l'agrégat par un agrégat présent sur la SVM, soit le supprimer complètement afin de remettre le backend en ligne.</p> </div> <p>Ne pas spécifier pour les systèmes de stockage AFX.</p> <p>Ne précisez pas quand <code>useBalancedPlacement</code> est défini sur <code>true</code>.</p>	""
useBalancedPlacement	<p>Déléguer la sélection des agrégats pour les nouveaux volumes à ONTAP [Booléen]. Nécessite ONTAP 9.19.1 ou une version ultérieure et <code>useREST</code> défini sur <code>true</code>. Ne peut pas être combiné avec <code>aggregate</code>.</p> <p>Consultez "Utilisez un placement équilibré avec les backends ONTAP" pour connaître les exigences et obtenir des exemples.</p> <p>Si spécifié, définissez toujours sur <code>true</code> pour les systèmes de stockage AFX sur ONTAP 9.19.1 ou version ultérieure.</p>	<code>false</code> ; <code>true</code> pour les systèmes de stockage AFX sur ONTAP 9.19.1 ou version ultérieure
limitAggregateUsage	<p>L'approvisionnement échoue si l'utilisation dépasse ce pourcentage. Ne s'applique pas à Amazon FSx pour ONTAP. Ne pas spécifier pour les systèmes de stockage AFX.</p>	"" (non appliqué par défaut)

Paramètre	Description	Défaut
flexgroupAggregateList	<p>Liste des agrégats à provisionner (facultatif ; si défini, doit être affecté au SVM). Tous les agrégats affectés au SVM sont utilisés pour provisionner un FlexGroup volume. Pris en charge par le pilote de stockage ontap-nas-flexgroup.</p> <div>  <p>Lorsque la liste d'agrégats 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 le provisionnement de volumes, si la liste d'agrégats est renommée ou déplacée hors de SVM, le backend passe à l'état d'échec dans Trident lors de l'interrogation de l'agrégat SVM. Vous devez soit modifier la liste d'agrégats pour en utiliser une présente sur SVM, soit la supprimer complètement afin de remettre le backend en ligne.</p> </div>	""
limitVolumeSize	L'approvisionnement échoue si la taille du volume demandée dépasse cette valeur.	"" (non appliqué par défaut)
debugTraceFlags	Options 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.	null
nasType	Configurez la création de volumes NFS ou SMB. Les options sont <code>nfs</code> , <code>smb</code> ou <code>null</code> . La valeur <code>null</code> correspond par défaut à des volumes NFS. Si spécifié, définissez toujours sur <code>nfs</code> pour les systèmes de stockage AFX.	<code>nfs</code>
nfsMountOptions	Liste d'options de montage NFS séparées par des virgules. Les options de montage des volumes persistants Kubernetes sont généralement spécifiées dans les classes de stockage, mais si aucune option de montage n'est spécifiée dans une classe de stockage, Trident utilise celles définies dans le fichier de configuration du backend de stockage. Si aucune option de montage n'est spécifiée ni dans la classe de stockage ni dans le fichier de configuration, Trident n'applique aucune option de montage au volume persistant associé.	""
qtreesPerFlexvol	Nombre maximal de Qtrees par FlexVol, doit être compris dans la plage [50, 300]	"200"

Paramètre	Description	Défaut
smbShare	Vous pouvez spécifier l'une des options suivantes : 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 pour permettre à Trident de créer le partage SMB ; ou vous pouvez laisser le paramètre vide pour empêcher l'accès partagé aux volumes. Ce paramètre est facultatif pour ONTAP sur site. Ce paramètre est obligatoire pour Amazon FSx for ONTAP backends et ne peut pas être vide.	smb-share
useREST	Paramètre booléen à utiliser pour les API REST ONTAP. <code>useREST</code> Lorsqu'il est défini sur <code>true</code> , Trident utilise les API REST ONTAP pour communiquer avec le backend ; lorsqu'il est défini sur <code>false</code> , Trident utilise les appels ONTAPI (ZAPI) pour communiquer avec le backend. Cette fonctionnalité nécessite ONTAP 9.11.1 ou une version ultérieure. De plus, le rôle de connexion ONTAP utilisé doit avoir accès à l'application <code>ontapi</code> . Cela est satisfait par les rôles prédéfinis <code>vsadmin</code> et <code>cluster-admin</code> . À partir de la version Trident 24.06 et ONTAP 9.15.1 ou version ultérieure, <code>useREST</code> est défini sur <code>true</code> par défaut ; modifiez <code>useREST</code> sur <code>false</code> pour utiliser les appels ONTAPI (ZAPI). Si spécifié, définissez toujours sur <code>true</code> pour les systèmes de stockage AFX.	<code>true</code> pour ONTAP 9.15.1 ou version ultérieure, sinon <code>false</code> .
limitVolumePoolSize	Taille maximale requise de FlexVol lors de l'utilisation de Qtrees dans le backend <code>ontap-nas-economy</code> .	"" (non appliqué par défaut)
denyNewVolumePools	Empêche <code>ontap-nas-economy</code> les serveurs backend de créer de nouveaux volumes FlexVol pour y stocker leurs Qtrees. Seuls les FlexVol® préexistants sont utilisés pour le provisionnement de nouveaux PV.	
adAdminUser	Utilisateur ou groupe d'utilisateurs administrateur Active Directory 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 le provisionnement des volumes

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

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

Paramètre	Description	Défaut
spaceReserve	Mode de réservation d'espace ; "none" (fin) ou "volume" (épais)	"none"
snapshotPolicy	Stratégie de snapshot à utiliser	"none"
qosPolicy	Groupe de règles QoS à attribuer aux volumes créés. Choisissez l'un des deux, qosPolicy ou adaptiveQosPolicy, par pool de stockage/backend	""
adaptiveQosPolicy	Groupe de règles QoS adaptatives à attribuer aux volumes créés. Choisissez l'un de 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	"false"
encryption	Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume ; la valeur par défaut est false. NVE doit être sous licence et activé sur le cluster pour utiliser cette option. Si NAE est activé sur le backend, tout volume provisionné dans Trident est compatible NAE. Pour plus d'informations, consultez : "Comment Trident fonctionne avec NVE et NAE" .	"false"
tieringPolicy	Politique de hiérarchisation à utiliser « none »	
unixPermissions	Mode pour les nouveaux volumes	"777" pour les volumes NFS; vide (non applicable) pour les volumes SMB
snapshotDir	Contrôle l'accès au .snapshot répertoire	true, false (Défini explicitement).
exportPolicy	Règles d'export à utiliser	"default"
securityStyle	Style de sécurité pour les nouveaux volumes. NFS prend en charge mixed et unix styles de sécurité. SMB prend 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 règles QoS avec Trident requiert ONTAP 9.8 ou une version ultérieure. Vous devez utiliser un groupe de règles QoS non partagé et vous assurer que le groupe de règles est appliqué individuellement à chaque composant. Un groupe de règles QoS partagé impose une limite 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 afin de garantir que le FlexVol soit correctement dimensionné avec le pourcentage de `snapshotReserve` et le PVC. Lorsque l'utilisateur demande un PVC, Trident crée le FlexVol initial avec plus d'espace en utilisant le nouveau calcul. Ce calcul garantit que l'utilisateur reçoit l'espace inscriptible qu'il a demandé dans le PVC, et non moins que ce qu'il a demandé. Avant la version v21.07, lorsque l'utilisateur demandait un PVC (par exemple, 5 Gio), avec le `snapshotReserve` à 50 pour cent, il n'obtenait que 2,5 Gio d'espace inscriptible. Cela s'explique par le fait que ce que l'utilisateur demandait était le volume entier et `snapshotReserve` est un pourcentage de celui-ci. Avec Trident 21.07, ce que l'utilisateur demande est l'espace inscriptible et Trident définit le nombre `snapshotReserve` comme le pourcentage du volume entier. Cela ne s'applique pas à `ontap-nas-economy`. Voir l'exemple suivant pour comprendre 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 la demande de l'utilisateur dans la demande PVC. La commande `volume show` devrait afficher des résultats similaires à cet exemple :

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

2 entries were displayed.

Les backends existants issus d'installations précédentes provisionnent les volumes comme expliqué ci-dessus lors de la mise à niveau de Trident. Pour les volumes que vous avez créés avant la mise à niveau, vous devez redimensionner ces volumes pour que la modification soit prise en compte. Par exemple, un PVC de 2 Gio avec `snapshotReserve=50` aboutissait auparavant à un volume offrant 1 Gio d'espace accessible en écriture. En redimensionnant le volume à 3 Gio, par exemple, l'application disposera de 3 Gio d'espace accessible en écriture 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. C'est la manière la plus simple de définir un backend.



Si vous utilisez Amazon FSx sur NetApp ONTAP avec Trident, la recommandation est 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 FlexGroup NAS ONTAP

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

▼ Exemple MetroCluster

Vous pouvez configurer le backend pour éviter d'avoir à mettre à jour manuellement la définition du backend après le basculement et le retour en arrière pendant "[Réplication et récupération de SVM](#)".

Pour une transition et un retour en arrière sans heurt, spécifiez le SVM en utilisant `managementLIF` et omettez les `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 prennent respectivement les valeurs encodées en base64 du certificat client, de la clé privée et du certificat de l'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 règles d'export automatique

Cet exemple vous montre comment vous pouvez demander à Trident d'utiliser des règles d'export dynamiques pour créer et gérer automatiquement la règle d'export. Cela fonctionne de la même manière pour les `ontap-nas-economy` et `ontap-nas-flexgroup` pilotes.

```
---
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 de placement équilibré

Cet exemple active le placement équilibré d'ONTAP afin qu'ONTAP sélectionne l'agrégat pour les nouveaux volumes. Le placement équilibré nécessite ONTAP 9.19.1 ou une version ultérieure. Consultez ["Utilisez un placement équilibré avec les backends ONTAP"](#) pour plus de détails.

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

▼ Exemple d'adresses IPv6

Cet exemple montre `managementLIF` l'utilisation d'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 d'Amazon FSx for ONTAP avec des volumes SMB

Le `smbShare` 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 du 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 backends avec pools virtuels

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

Trident définit les étiquettes de provisionnement dans le champ « Commentaires ». Les commentaires sont définis sur `FlexVol` pour `ontap-nas` ou sur `FlexGroup` pour `ontap-nas-flexgroup`. Trident copie toutes les étiquettes présentes sur un pool virtuel vers le volume de stockage lors du provisionnement. Pour plus de simplicité, 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 `spaceReserve`, `spaceAllocation`, et `encryption` valeurs, et certains pools remplacent les valeurs par défaut.

▼ Exemple 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: mysqlldb
    cost: "25"
zone: us_east_1d
defaults:
    spaceReserve: volume
    encryption: "false"
    unixPermissions: "0775"

```

▼ Exemple de NAS ONTAP FlexGroup

```

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

```

```

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

```

▼ 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"

```

Map backends vers StorageClasses

Les définitions de StorageClass suivantes font référence à [Exemples de backends avec pools virtuels](#). En utilisant le champ `parameters.selector`, chaque StorageClass indique quels pools virtuels peuvent être utilisés pour héberger un volume. Le volume possède les aspects définis dans le pool virtuel choisi.

- Le `protection-gold` StorageClass correspond aux première et deuxième pools virtuelles dans le `ontap-nas-flexgroup` backend. Ce sont les seuls pools offrant 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 correspond 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 gold.

```

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 correspond au quatrième pool virtuel dans le ontap-nas backend. C'est le 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 correspond au troisième pool virtuel dans le ontap-nas-flexgroup backend. C'est le seul pool offrant une protection de niveau argent et 20000 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 correspond au troisième pool virtuel dans le `ontap-nas` backend et au deuxième pool virtuel dans le `ontap-nas-economy` backend. Ce sont les seules offres de pool proposant 5 000 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 détermine quel pool virtuel est sélectionné et veille à ce que l'exigence de stockage soit respectée.

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 afin que la nouvelle dataLIF prenne effet.

Exemples de SMB sécurisés

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 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 DÉLICTELLE (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.