



Pilotes ONTAP SAN

Trident

NetApp
October 30, 2026

Sommaire

Pilotes ONTAP SAN	1
Présentation du pilote ONTAP SAN	1
Détails du pilote ONTAP SAN	1
Autorisations de l'utilisateur	2
Considérations supplémentaires pour NVMe/TCP	2
Préparez-vous à configurer le backend avec les pilotes SAN ONTAP	3
Exigences	3
Authentifier le backend ONTAP	3
Authentifiez les connexions avec CHAP bidirectionnel	9
Options et exemples de configuration SAN ONTAP	11
Options de configuration du backend	11
Options de configuration backend pour le provisionnement des volumes	17
Exemples de configuration minimale	19
Exemples de backends avec pools virtuels	23
Map backends vers StorageClasses	26

Pilotes ONTAP SAN

Présentation du pilote ONTAP SAN

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

Détails du pilote ONTAP SAN

Trident fournit les pilotes de stockage SAN 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	volumeMod e	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
ontap-san	iSCSI SCSI sur FC	Bloc	RWO, ROX, RWX, RWOP	Aucun système de fichiers ; périphérique bloc brut
ontap-san	iSCSI SCSI sur FC	Système de fichiers	RWO, RWOP ROX et RWX ne sont pas disponibles en mode volume du système de fichiers.	xfs, ext3, ext4
ontap-san	NVMe/TCP Reportez- vous à Considérations supplément aires pour NVMe/TCP .	Bloc	RWO, ROX, RWX, RWOP	Aucun système de fichiers ; périphérique bloc brut
ontap-san	NVMe/TCP Reportez- vous à Considérations supplément aires pour NVMe/TCP .	Système de fichiers	RWO, RWOP ROX et RWX ne sont pas disponibles en mode volume du système de fichiers.	xfs, ext3, ext4
ontap-san-economy	iSCSI	Bloc	RWO, ROX, RWX, RWOP	Aucun système de fichiers ; périphérique bloc brut

Pilote	Protocole	volumeMode	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
ontap-san-economy	iSCSI	Système de fichiers	RWO, RWOP ROX et RWX ne sont pas disponibles en mode volume du système de fichiers.	xfss, ext3, ext4



- 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.

Considérations supplémentaires pour NVMe/TCP

Trident prend en charge le protocole non-volatile memory express (NVMe) à l'aide du `ontap-san` driver, notamment :

- IPv6
- Instantanés et clones de volumes NVMe
- Redimensionnement d'un volume NVMe

- Importation d'un volume NVMe créé en dehors de Trident afin que son cycle de vie puisse être géré par Trident
- Multipathing natif NVMe
- Arrêt progressif ou brutal des nœuds K8s (24.06)

Trident ne prend pas en charge :

- DH-HMAC-CHAP pris en charge nativement par NVMe
- Multipathing du device mapper (DM)
- chiffrement LUKS



NVMe est pris en charge uniquement avec les API REST ONTAP et non avec ONTAPI (ZAPI).

Préparez-vous à configurer le backend avec les pilotes SAN ONTAP

Comprenez les exigences et les options d'authentification pour configurer un backend ONTAP avec des pilotes SAN ONTAP.

Exigences

Pour tous les backends ONTAP, Trident exige qu'au moins un agrégat soit affecté au SVM.



"[Systèmes ASA r2](#)" diffèrent des autres systèmes ONTAP (ASA, AFF et FAS) dans l'implémentation de leur couche de stockage. Dans les systèmes ASA r2, des zones de disponibilité de stockage sont utilisées au lieu des agrégats. Consultez l'article de la "[ce](#)" Knowledge Base pour savoir comment affecter des agrégats aux SVM dans les systèmes ASA r2.

N'oubliez pas que vous pouvez également exécuter plusieurs pilotes et créer des classes de stockage qui pointent vers l'un ou l'autre. Par exemple, vous pouvez configurer une `san-dev` classe qui utilise le `ontap-san` pilote et une `san-default` classe qui utilise le `ontap-san-economy` pilote.

Tous vos nœuds de travail Kubernetes doivent disposer des outils iSCSI appropriés. Consultez "[Préparez le nœud de travail](#)" pour plus de détails.

Authentifier le backend ONTAP

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

- Authentification par identifiants : le nom d'utilisateur et le mot de passe d'un utilisateur ONTAP disposant des autorisations requises. Il est recommandé d'utiliser un rôle de connexion de sécurité prédéfini, tel que `admin` ou `vsadmin` pour garantir une compatibilité maximale avec les versions d'ONTAP.
- Authentification par certificat : Trident peut également communiquer avec un cluster ONTAP à l'aide d'un certificat installé sur le backend. 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-san
managementLIF: 10.0.0.1
svm: svm_nfs
username: vsadmin
password: password
```

JSON

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

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 ou la mise à jour d'un backend est la seule étape qui nécessite la connaissance des identifiants. En tant que telle, il s'agit d'une opération réservée à l'administrateur Kubernetes/stockage.

Activer l'authentification basée sur les certificats

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=admin"
```

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
```



Après avoir exécuté cette commande, ONTAP vous invite à saisir un certificat. Collez le contenu du `k8senv.pem` fichier généré à l'étape 1, puis appuyez sur **END** pour terminer l'installation.

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

```
-authentication-method cert
```

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.

```
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.json  
{  
  "version": 1,  
  "storageDriverName": "ontap-san",  
  "backendName": "SanBackend",  
  "managementLIF": "1.2.3.4",  
  "svm": "vserver_test",  
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",  
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",  
  "trustedCACertificate": "QNFinfO...SiqOyN",  
  "storagePrefix": "myPrefix_"  
}  
  
tridentctl create backend -f cert-backend.json -n trident  
+-----+-----+-----+-----+  
+-----+-----+  
|      NAME      | STORAGE DRIVER |                               UUID                               |  
STATE | VOLUMES |  
+-----+-----+-----+-----+  
+-----+-----+  
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |  
online |         0 |  
+-----+-----+-----+-----+  
+-----+-----+  

```

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 backend update`.

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

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



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"

Authentifiez les connexions avec CHAP bidirectionnel

Trident peut authentifier les sessions iSCSI avec CHAP bidirectionnel pour les `ontap-san` et `ontap-san-economy` pilotes. Cela nécessite l'activation de l'option `useCHAP` dans la définition de votre backend. Lorsqu'elle est définie sur `true`, Trident configure la sécurité par défaut de l'initiateur du SVM sur CHAP bidirectionnel et définit le nom d'utilisateur et les secrets à partir du fichier backend. NetApp recommande d'utiliser CHAP bidirectionnel pour authentifier les connexions. Voir l'exemple de configuration suivant :

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



Le `useCHAP` paramètre est une option booléenne qui ne peut être configurée qu'une seule fois. Il est défini sur faux par défaut. Après l'avoir défini sur vrai, vous ne pouvez plus le définir sur faux.

En plus de `useCHAP=true`, les `chapInitiatorSecret`, `chapTargetInitiatorSecret`, `chapTargetUsername` et `chapUsername`, les champs doivent être inclus dans la définition du backend. Les secrets peuvent être modifiés après la création d'un backend en exécutant `tridentctl update`.

Comment ça marche

En définissant `useCHAP` sur `true`, l'administrateur de stockage demande à Trident de configurer CHAP sur le système de stockage. Cela inclut les éléments suivants :

- Configuration de CHAP sur la SVM :
 - Si le type de sécurité par défaut de l'initiateur SVM est « aucun » (défini par défaut) **et** qu'il n'y a pas de LUN préexistants déjà présents dans le volume, Trident définira le type de sécurité par défaut à CHAP et procédera à la configuration du nom d'utilisateur et des secrets de l'initiateur CHAP et de la cible.
 - Si la SVM contient des LUN, Trident n'activera pas CHAP sur la SVM. Cela garantit que l'accès aux LUN déjà présentes sur la SVM n'est pas restreint.
- Configuration du nom d'utilisateur et des secrets de l'initiateur et de la cible CHAP ; ces options doivent être spécifiées dans la configuration du backend (comme indiqué ci-dessus).

Après la création du backend, Trident crée une CRD correspondante `tridentbackend` et stocke les secrets CHAP ainsi que les noms d'utilisateur en tant que secrets Kubernetes. Tous les PV créés par Trident sur ce backend seront montés et attachés via CHAP.

Renouvelez les identifiants et mettez à jour les backends

Vous pouvez mettre à jour les informations d'identification CHAP en modifiant les paramètres CHAP dans le `backend.json` fichier. Cela nécessitera la mise à jour des secrets CHAP et l'utilisation de la `tridentctl update` commande pour appliquer ces modifications.



Lors de la mise à jour des secrets CHAP pour un backend, vous devez utiliser `tridentctl` pour mettre à jour le backend. Ne mettez pas à jour les informations d'identification sur le cluster de stockage à l'aide de l'ONTAP CLI ou d'ONTAP System Manager, car Trident ne pourra pas prendre en compte ces modifications.

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

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

Les connexions existantes restent inchangées ; elles demeureront actives si les identifiants sont mis à jour par Trident sur le SVM. Les nouvelles connexions utilisent les identifiants mis à jour et les connexions existantes demeurent actives. La déconnexion puis la reconnexion d'anciens PV entraînera leur utilisation des identifiants mis à jour.

Options et exemples de configuration SAN ONTAP

Créez et utilisez les pilotes SAN ONTAP avec votre installation Trident. Cette section fournit des exemples de configuration backend et des détails pour le mappage des backends vers les StorageClasses. ["Systèmes ASA r2"](#) diffèrent des autres systèmes ONTAP (ASA, AFF et FAS) dans l'implémentation de leur couche de stockage. Ces variations ont un impact sur l'utilisation de certains paramètres, comme noté. ["En savoir plus sur les différences entre les systèmes ASA r2 et les autres systèmes ONTAP"](#). Dans la configuration backend de Trident, il n'est pas nécessaire de spécifier que votre système est ASA r2. Lorsque vous sélectionnez `ontap-san` comme `storageDriverName`, Trident détecte automatiquement l'ASA r2 ou d'autres systèmes ONTAP. Certains paramètres de configuration backend ne sont pas applicables aux systèmes ASA r2, comme indiqué dans le tableau ci-dessous.



Seul le ``ontap-san`` pilote (avec les protocoles iSCSI, NVMe/TCP et FC) est pris en charge pour les systèmes ASA r2.

Options de configuration du backend

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

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

Paramètre	Description	Défaut
<code>version</code>		Toujours 1
<code>storageDriverName</code>	Nom du pilote de stockage. Ne peut pas être modifié après création. Pour mettre à jour ce paramètre, vous devez créer un nouveau backend.	<code>ontap-san</code> ou <code>ontap-san-economy</code>
<code>backendName</code>	Nom personnalisé ou le stockage backend	Nom du pilote + "_" + <code>dataLIF</code>

Paramètre	Description	Défaut
managementLIF	<p>Adresse IP d'une LIF de gestion de cluster ou de SVM.</p> <p>Un nom de domaine complet (FQDN) peut être spécifié.</p> <p>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 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p> <p>Pour une transition en douceur MetroCluster, consultez le Exemple MetroCluster.</p> <div>  <p>Si vous utilisez les identifiants « vsadmin », managementLIF doit être celui de la SVM ; si vous utilisez les identifiants « admin », managementLIF doit être celui du cluster.</p> </div>	"10.0.0.1", "[2001:1234:abcd::fefe]"
dataLIF	<p>Adresse IP de l'interface logique de protocole (LIF). 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 [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Ne pas spécifier pour iSCSI. Trident utilise "Mappage LUN sélectif ONTAP" pour découvrir les LIF iSCSI nécessaires à l'établissement d'une session multi-chemin. Un avertissement est généré si dataLIF est explicitement défini. Omettre pour MetroCluster. Voir le Exemple MetroCluster.</p>	Dérivé par le SVM
svm	Machine virtuelle de stockage à utiliser Omettre pour MetroCluster. Voir le Exemple MetroCluster .	Dérivé si un SVM managementLIF est spécifié
useCHAP	Utilisez CHAP pour authentifier iSCSI pour les pilotes SAN ONTAP [paramètre booléen]. Définissez sur true pour que Trident configure et utilise CHAP bidirectionnel comme authentification par défaut pour la SVM indiquée dans le backend. Consultez "Préparez-vous à configurer le backend avec les pilotes SAN ONTAP" pour plus de détails. Non pris en charge pour FCP ou NVMe/TCP.	false
chapInitiatorSecret	Secret de l'initiateur CHAP. Obligatoire si useCHAP=true	""
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	""

Paramètre	Description	Défaut
chapTargetInitiatorSecret	Secret de l'initiateur de la cible CHAP. Obligatoire si useCHAP=true	""
chapUsername	Nom d'utilisateur entrant. Obligatoire si useCHAP=true	""
chapTargetUsername	Nom d'utilisateur cible. Obligatoire si useCHAP=true	""
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 requis pour communiquer avec le cluster ONTAP. 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 requis pour communiquer avec le cluster ONTAP. 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" .	""
svm	Machine virtuelle de stockage à utiliser	Dérivé si un SVM managementLIF est spécifié
storagePrefix	Préfixe utilisé lors du provisionnement de nouveaux volumes dans la SVM. Ne peut pas être modifié ultérieurement. Pour mettre à jour ce paramètre, vous devez créer un nouveau backend.	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. Lorsque vous avez configuré un agrégat spécifique dans Trident pour le provisionnement de volumes, si l'agrégat est renommé ou déplacé hors de la SVM, le backend passe à l'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 ASA r2.</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>	false
limitAggregateUsage	<p>L'approvisionnement échoue si l'utilisation dépasse ce pourcentage. Si vous utilisez un Amazon FSx for NetApp ONTAP backend, ne spécifiez pas <code>limitAggregateUsage</code>. Les <code>fsxadmin</code> et <code>vsadmin</code> fournis ne contiennent pas les autorisations requises pour récupérer l'utilisation agrégée et la limiter à l'aide de Trident. Ne pas spécifier pour les systèmes ASA r2.</p>	"" (non appliqué par défaut)
limitVolumeSize	<p>L'approvisionnement échoue si la taille du volume demandée dépasse cette valeur. Limite également la taille maximale des volumes qu'il gère pour les LUN.</p>	"" (non appliqué par défaut)
lunsPerFlexvol	<p>Nombre maximal de LUN par FlexVol®, doit être compris dans la plage [50, 200]</p>	100

Paramètre	Description	Défaut
debugTraceFlags	Options de débogage à utiliser lors du dépannage. Exemple, {"api":false, "method":true} n'utilisez-les que si vous effectuez un dépannage et avez besoin d'un journal détaillé.	null
useREST	<p>Paramètre booléen à utiliser pour les API REST ONTAP.</p> <div> <p><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).</p> </div> <p><code>useREST</code> est entièrement compatible NVMe/TCP.</p> <div>  <p>NVMe est pris en charge uniquement avec les API REST ONTAP et non avec ONTAPI (ZAPI).</p> </div> <p>Si spécifié, toujours définir sur <code>true</code> pour les systèmes ASA r2.</p>	true pour ONTAP 9.15.1 ou version ultérieure, sinon false.
sanType	Utilisez pour sélectionner <code>iscsi</code> pour iSCSI, <code>nvme</code> pour NVMe/TCP ou <code>fc</code> pour SCSI sur Fibre Channel (FC).	iscsi si vide

Paramètre	Description	Défaut
formatOptions	Utilisez formatOptions pour spécifier des arguments de ligne de commandes pour la commande mkfs, qui sont appliqués chaque fois qu'un volume est formaté. Cela vous permet de formater le volume selon vos préférences. Assurez-vous de spécifier les formatOptions de façon similaire aux options de la commande mkfs, à l'exception du chemin du périphérique. Exemple : « -E nodiscard » Pris en charge pour ontap-san et ontap-san-economy pilotes avec le protocole iSCSI. En outre, pris en charge pour les systèmes ASA r2 lors de l'utilisation des protocoles iSCSI et NVMe/TCP.	
limitVolumePoolSize	Taille maximale requise de FlexVol lors de l'utilisation de LUN dans le backend ontap-san-economy.	"" (non appliqué par défaut)
denyNewVolumePools	Limite ontap-san-economy les backends à la création de nouveaux volumes FlexVol® pour contenir leurs LUN. Seuls les FlexVol® préexistants sont utilisés pour le provisionnement de nouveaux PV.	

Recommandations d'utilisation de formatOptions

Trident recommande les options suivantes pour accélérer le processus de mise en forme :

- **-E nodiscard (ext3, ext4)** : Ne pas tenter de supprimer des blocs lors de la création du système de fichiers (la suppression initiale de blocs est utile sur les disques SSD et les systèmes de stockage à provisionnement fin). Cette option remplace l'option obsolète « -K » et s'applique aux systèmes de fichiers ext3 et ext4.
- **-K (xfs)** : Ne pas tenter de supprimer des blocs lors de la création du système de fichiers (mkfs). Cette option s'applique au système de fichiers xfs.

Authentifier Trident auprès d'un SVM backend à l'aide des identifiants Active Directory

Vous pouvez configurer Trident pour qu'il s'authentifie auprès d'une SVM backend à l'aide d'identifiants Active Directory (AD). Avant qu'un compte AD puisse accéder à la SVM, vous devez configurer l'accès des contrôleurs de domaine AD au cluster ou à la SVM. Pour l'administration du cluster avec un compte AD, vous devez créer un tunnel de domaine. Consultez ["Configurer l'accès au contrôleur de domaine Active Directory dans ONTAP"](#) pour plus de détails.

étapes

1. Configurer les paramètres du système de noms de domaine (DNS) pour une SVM backend :

```
vserver services dns create -vserver <svm_name> -dns-servers
<dns_server_ip1>,<dns_server_ip2>
```

2. Exécutez la commande suivante pour créer un compte d'ordinateur pour la SVM dans Active Directory :

```
vserver active-directory create -vserver DataSVM -account-name ADSERVER1
-domain demo.netapp.com
```

3. Utilisez cette commande pour créer un utilisateur ou un groupe AD afin de gérer le cluster ou la SVM

```
security login create -vserver <svm_name> -user-or-group-name  
<ad_user_or_group> -application <application> -authentication-method domain  
-role vsadmin
```

4. Dans le fichier de configuration backend de Trident, définissez les paramètres `username` et `password` sur le nom d'utilisateur ou de groupe AD et le mot de passe, respectivement.

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
<code>spaceAllocation</code>	Allocation d'espace pour les LUNs	"true" Si spécifié, définissez sur true pour les systèmes ASA r2.
<code>spaceReserve</code>	Mode de réservation d'espace : « aucun » (fin) ou « volume » (épais). À définir sur none pour les systèmes ASA r2.	"none"
<code>snapshotPolicy</code>	Stratégie d'instantané à utiliser. À définir sur none pour les systèmes ASA r2.	"none"
<code>qosPolicy</code>	Groupe de règles QoS à attribuer aux volumes créés. Choisissez l'un de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> par pool de stockage/backend. 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.	""
<code>adaptiveQosPolicy</code>	Groupe de règles QoS adaptatives à attribuer aux volumes créés. Choisissez l'un des deux, <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> , par pool de stockage/backend	""
<code>snapshotReserve</code>	Pourcentage du volume réservé aux snapshots. Ne pas spécifier pour les systèmes ASA r2.	"0" si <code>snapshotPolicy</code> est "aucun", sinon ""
<code>splitOnClone</code>	Séparer un clone de son parent lors de sa création	"false"
<code>encryption</code>	Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume ; la valeur par défaut est <code>false</code> . 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" Si spécifié, définissez sur true pour les systèmes ASA r2.
<code>luksEncryption</code>	Activez le chiffrement LUKS. Reportez-vous à "Utilisez Linux Unified Key Setup (LUKS)" .	"" Définir sur false pour les systèmes ASA r2.

Paramètre	Description	Défaut
tieringPolicy	Politique de hiérarchisation à utiliser « none » Ne pas spécifier pour les systèmes ASA r2.	
nameTemplate	Modèle pour créer des noms de volumes personnalisés.	""

Exemples de provisionnement de volumes

Voici un exemple avec des valeurs par défaut définies :

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



Pour tous les volumes créés à l'aide du ontap-san driver, Trident ajoute 10 % de capacité supplémentaire à la FlexVol pour intégrer les métadonnées LUN. La LUN est provisionnée avec la taille exacte demandée par l'utilisateur dans le PVC. Trident ajoute 10 % à la FlexVol (affiché comme taille disponible dans ONTAP). Les utilisateurs obtiennent désormais la capacité utilisable qu'ils ont demandée. Cette modification empêche également les LUN de passer en lecture seule, sauf si l'espace disponible est entièrement utilisé. Ceci ne s'applique pas à ontap-san-economy.

Pour les backends qui définissent snapshotReserve, Trident calcule la taille des volumes comme suit :

```
Total volume size = [(PVC requested size) / (1 - (snapshotReserve
percentage) / 100)] * 1.1
```

Le chiffre 1,1 correspond aux 10 % supplémentaires que Trident ajoute au FlexVol pour prendre en compte les

métadonnées LUN. Pour `snapshotReserve = 5 %`, et une demande PVC = 5 Gio, la taille totale du volume est de 5,79 Gio et la taille disponible est de 5,5 Gio. 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_e42ec6fe_3baa_4af6_996d_134adbbb8e6d	online	RW	5.79GB	5.50GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

3 entries were displayed.

Actuellement, le redimensionnement est le seul moyen d'utiliser le nouveau calcul pour un volume existant.

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, NetApp recommande de spécifier les noms DNS des LIF au lieu des adresses IP.

▼ Exemple SAN ONTAP

Il s'agit d'une configuration de base utilisant le `ontap-san` driver.

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

▼ 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 `svm` paramètres. Par exemple :

```
version: 1
storageDriverName: ontap-san
managementLIF: 192.168.1.66
username: vsadmin
```

```
password: password
```

▼ Exemple d'économie SAN ONTAP

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

▼ Exemple d'authentification par certificat

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

▼ Exemples CHAP bidirectionnels

Ces exemples créent un backend avec `useCHAP` défini sur `true`.

Exemple ONTAP SAN CHAP

```
---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
labels:
  k8scluster: test-cluster-1
  backend: testcluster1-sanbackend
```

```

useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>

```

Exemple d'économie ONTAP SAN CHAP

```

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

```

▼ 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-san
backendName: san-balanced-placement
managementLIF: 10.0.0.1
svm: svm_iscsi
username: vsadmin
password: <password>
useBalancedPlacement: true

```

▼ Exemple NVMe/TCP

Vous devez disposer d'une SVM configurée avec NVMe sur votre backend ONTAP. Il s'agit d'une configuration de base pour NVMe/TCP.

```

---
version: 1

```

```

backendName: NVMeBackend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_nvme
username: vsadmin
password: password
sanType: nvme
useREST: true

```

▼ Exemple de SCSI sur FC (FCP)

Vous devez disposer d'une SVM configurée avec FC sur votre backend ONTAP. Il s'agit d'une configuration de base du backend pour FC.

```

---
version: 1
backendName: fcp-backend
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_fc
username: vsadmin
password: password
sanType: fcp
useREST: true

```

▼ Exemple de configuration du backend avec nameTemplate

```

---
version: 1
storageDriverName: ontap-san
backendName: ontap-san-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}}"

```

▼ formatOptions exemple pour le pilote ontap-san-economy

```

---

```

```

version: 1
storageDriverName: ontap-san-economy
managementLIF: ""
svm: svm1
username: ""
password: "!"
storagePrefix: whelk_
debugTraceFlags:
  method: true
  api: true
defaults:
  formatOptions: -E nodiscard

```

Exemples de backends avec pools virtuels

Dans ces exemples de fichiers de définition de backend, 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 le volume FlexVol. 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 SAN ONTAP

```

---
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
svm: svm_iscsi
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
  qosPolicy: standard
labels:
  store: san_store
  kubernetes-cluster: prod-cluster-1

```

```

region: us_east_1
storage:
  - labels:
      protection: gold
      creditpoints: "40000"
    zone: us_east_1a
    defaults:
      spaceAllocation: "true"
      encryption: "true"
      adaptiveQosPolicy: adaptive-extreme
  - labels:
      protection: silver
      creditpoints: "20000"
    zone: us_east_1b
    defaults:
      spaceAllocation: "false"
      encryption: "true"
      qosPolicy: premium
  - labels:
      protection: bronze
      creditpoints: "5000"
    zone: us_east_1c
    defaults:
      spaceAllocation: "true"
      encryption: "false"

```

▼ Exemple d'économie SAN ONTAP

```

---
version: 1
storageDriverName: ontap-san-economy
managementLIF: 10.0.0.1
svm: svm_iscsi_eco
useCHAP: true
chapInitiatorSecret: cl9qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSD6cNwxyz
username: vsadmin
password: <password>
defaults:
  spaceAllocation: "false"
  encryption: "false"
labels:
  store: san_economy_store
region: us_east_1

```

```

storage:
  - labels:
      app: oracledb
      cost: "30"
      zone: us_east_1a
      defaults:
        spaceAllocation: "true"
        encryption: "true"
  - labels:
      app: postgresdb
      cost: "20"
      zone: us_east_1b
      defaults:
        spaceAllocation: "false"
        encryption: "true"
  - labels:
      app: mysqldb
      cost: "10"
      zone: us_east_1c
      defaults:
        spaceAllocation: "true"
        encryption: "false"
  - labels:
      department: legal
      creditpoints: "5000"
      zone: us_east_1c
      defaults:
        spaceAllocation: "true"
        encryption: "false"

```

▼ Exemple NVMe/TCP

```

---
version: 1
storageDriverName: ontap-san
sanType: nvme
managementLIF: 10.0.0.1
svm: nvme_svm
username: vsadmin
password: <password>
useREST: true
defaults:
  spaceAllocation: "false"
  encryption: "true"
storage:
  - labels:

```

```

    app: testApp
    cost: "20"
  defaults:
    spaceAllocation: "false"
    encryption: "false"

```

Map backends vers StorageClasses

Les définitions StorageClass suivantes font référence à l'[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 désormais les caractéristiques définies dans le pool virtuel choisi.

- Le `protection-gold` StorageClass correspond au premier pool virtuel dans le `ontap-san` backend. Il s'agit du seul pool 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 aux deuxième et troisième pools virtuelles dans le `ontap-san` 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 troisième pool virtuel dans le `ontap-san-economy` backend. C'est le seul pool offrant une configuration de pool de stockage pour l'application de type `mysqldb`.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb

```

```
provisioner: csi.trident.netapp.io
parameters:
  selector: "app=mysqlldb"
  fsType: "ext4"
```

- Le protection-silver-creditpoints-20k StorageClass correspond au deuxième pool virtuel dans le ontap-san 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 backend ontap-san et au quatrième pool virtuel dans le backend ontap-san-economy. 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"
```

- Le my-test-app-sc StorageClass correspond au testAPP pool virtuel dans le ontap-san pilote avec sanType: nvme. C'est le seul pool offrant testApp.

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

Trident détermine quel pool virtuel est sélectionné et veille à ce que l'exigence de stockage soit respectée.

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.