



Gérer les backends

Trident

NetApp
October 30, 2026

Sommaire

Gérer les backends	1
Gérer les backends Trident avec kubectl	1
Supprimer un backend	1
Afficher les backends existants	1
Mettre à jour un backend	1
Gérez les backends Trident avec tridentctl	2
Créer un backend	2
Supprimer un backend	2
Afficher les backends existants	3
Mettre à jour un backend	3
Identifiez les classes de stockage qui utilisent un backend	3
Choisissez une méthode de gestion du backend Trident	4
Options pour la gestion des backends	4
Gérer tridentctl les backends à l'aide de TridentBackendConfig	4
Gérer TridentBackendConfig les backends à l'aide de tridentctl	8

Gérer les backends

Gérer les backends Trident avec kubectl

Découvrez comment effectuer des opérations de gestion backend en utilisant `kubectl`.

Supprimer un backend

En supprimant un `TridentBackendConfig`, vous indiquez à Trident de supprimer ou de conserver les backends (selon `deletionPolicy`). Pour supprimer un backend, assurez-vous que `deletionPolicy` est défini sur `delete`. Pour supprimer uniquement le `TridentBackendConfig`, assurez-vous que `deletionPolicy` est défini sur `retain`. Cela garantit que le backend est toujours présent et peut être géré à l'aide de `tridentctl`.

Exécutez la commande suivante :

```
kubectl delete tbc <tbc-name> -n trident
```

Trident ne supprime pas les secrets Kubernetes qui étaient utilisés par `TridentBackendConfig`. L'utilisateur Kubernetes est responsable du nettoyage des secrets. Il faut faire attention lors de la suppression des secrets. Vous ne devez supprimer les secrets que s'ils ne sont pas utilisés par les backends.

Afficher les backends existants

Exécutez la commande suivante :

```
kubectl get tbc -n trident
```

Vous pouvez également exécuter `tridentctl get backend -n trident` ou `tridentctl get backend -o yaml -n trident` pour obtenir une liste de tous les backends existants. Cette liste inclura également les backends qui ont été créés avec `tridentctl`.

Mettre à jour un backend

Il peut exister plusieurs raisons de mettre à jour un backend :

- Les identifiants d'accès au système de stockage ont changé. Pour mettre à jour les identifiants, le Secret Kubernetes utilisé dans l'objet `TridentBackendConfig` doit être mis à jour. Trident mettra automatiquement à jour le backend avec les identifiants les plus récents fournis. Exécutez la commande suivante pour mettre à jour le Secret Kubernetes :

```
kubectl apply -f <updated-secret-file.yaml> -n trident
```

- Les paramètres (tels que le nom de la ONTAP SVM utilisée) doivent être mis à jour.
 - Vous pouvez mettre à jour `TridentBackendConfig` les objets directement via Kubernetes à l'aide de la commande suivante :

```
kubectl apply -f <updated-backend-file.yaml>
```

- Vous pouvez également apporter des modifications à la `TridentBackendConfig` CR existante à l'aide de la commande suivante :

```
kubectl edit tbc <tbc-name> -n trident
```



- En cas d'échec d'une mise à jour du backend, le backend conserve sa dernière configuration connue. Vous pouvez consulter les journaux pour en déterminer la cause en exécutant `kubectl get tbc <tbc-name> -o yaml -n trident` ou `kubectl describe tbc <tbc-name> -n trident`.
- Après avoir identifié et corrigé le problème avec le fichier de configuration, vous pouvez relancer la commande de mise à jour.

Gérez les backends Trident avec tridentctl

Découvrez comment effectuer des opérations de gestion backend en utilisant `tridentctl`.

Créer un backend

Après avoir créé un "[fichier de configuration backend](#)", exécutez la commande suivante :

```
tridentctl create backend -f <backend-file> -n trident
```

Si la création du backend échoue, quelque chose n'allait pas avec la configuration du backend. Vous pouvez consulter les journaux pour en déterminer la cause en exécutant la commande suivante :

```
tridentctl logs -n trident
```

Après avoir identifié et corrigé le problème avec le fichier de configuration, vous pouvez simplement exécuter la commande `create` à nouveau.

Supprimer un backend

Pour supprimer un backend de Trident, procédez comme suit :

1. Récupérer le nom du backend :

```
tridentctl get backend -n trident
```

2. Supprimez le backend :

```
tridentctl delete backend <backend-name> -n trident
```



Si Trident a provisionné des volumes et des instantanés à partir de ce backend qui existent encore, la suppression du backend empêche le provisionnement de nouveaux volumes par celui-ci. Le backend continuera d'exister dans un état « Deleting ».

Afficher les backends existants

Pour afficher les backends que Trident connaît, procédez comme suit :

- Pour obtenir un résumé, exécutez la commande suivante :

```
tridentctl get backend -n trident
```

- Pour obtenir tous les détails, exécutez la commande suivante :

```
tridentctl get backend -o json -n trident
```

Mettre à jour un backend

Après avoir créé un nouveau fichier de configuration, exécutez la commande suivante :

```
tridentctl update backend <backend-name> -f <backend-file> -n trident
```

Si la mise à jour du backend échoue, cela signifie qu'il y a un problème avec la configuration du backend ou que vous avez tenté une mise à jour invalide. Vous pouvez consulter les journaux pour en déterminer la cause en exécutant la commande suivante :

```
tridentctl logs -n trident
```

Après avoir identifié et corrigé le problème avec le fichier de configuration, vous pouvez simplement exécuter la commande `update` à nouveau.

Identifiez les classes de stockage qui utilisent un backend

Voici un exemple du type de questions auxquelles vous pouvez répondre avec le JSON que `tridentctl` génère pour les objets backend. Cela utilise l'outil `jq` utilitaire, que vous devez installer.

```
tridentctl get backend -o json | jq '[.items[] | {backend: .name, storageClasses: [.storage[].storageClasses]|unique}]'
```

Cela s'applique également aux backends qui ont été créés en utilisant `TridentBackendConfig`.

Choisissez une méthode de gestion du backend Trident

Découvrez les différentes manières de gérer les backends dans Trident.

Options pour la gestion des backends

Avec l'introduction de `TridentBackendConfig`, les administrateurs disposent désormais de deux méthodes distinctes pour gérer les backends. Cela soulève les questions suivantes :

- Les backends créés à l'aide de `tridentctl` peuvent-ils être gérés avec `TridentBackendConfig` ?
- Les backends créés à l'aide de `TridentBackendConfig` peuvent-ils être gérés à l'aide de `tridentctl` ?

Gérer `tridentctl` les backends à l'aide de `TridentBackendConfig`

Cette section couvre les étapes nécessaires pour gérer les backends qui ont été créés à l'aide de `tridentctl` directement via l'interface Kubernetes en créant des `TridentBackendConfig` objets.

Cela s'appliquera aux scénarios suivants :

- Les backends préexistants, qui n'ont pas de `TridentBackendConfig` parce qu'ils ont été créés avec `tridentctl`.
- De nouveaux backends ont été créés avec `tridentctl`, tandis que d'autres `TridentBackendConfig` objets existent.

Dans les deux cas, les backends resteront présents, Trident planifiant les volumes et opérant dessus. Les administrateurs ont alors deux choix :

- Continuez à utiliser `tridentctl` pour gérer les backends qui ont été créés avec.
- Liez les backends créés à l'aide de `tridentctl` à un nouvel objet `TridentBackendConfig`. Cela signifie que les backends seront gérés à l'aide de `kubectl` et non `tridentctl`.

Pour gérer un backend préexistant à l'aide de `kubectl`, vous devrez créer un `TridentBackendConfig` qui se lie au backend existant. Voici un aperçu de la façon dont cela fonctionne :

1. Créez un secret Kubernetes. Le secret contient les informations d'identification dont Trident a besoin pour communiquer avec le cluster/service de stockage.
2. Créez un `TridentBackendConfig` objet. Celui-ci contient des informations spécifiques sur le cluster/service de stockage et fait référence au secret créé à l'étape précédente. Veillez à spécifier des paramètres de configuration identiques (tels que `spec.backendName`, `spec.storagePrefix`, `spec.storageDriverName`, etc.). `spec.backendName` doit être défini sur le nom du backend existant.

Étape 0 : Identifier le backend

Pour créer une `TridentBackendConfig` qui se lie à un backend existant, vous devrez obtenir la configuration du backend. Dans cet exemple, supposons qu'un backend ait été créé à l'aide de la définition JSON suivante :

```
tridentctl get backend ontap-nas-backend -n trident
```

```

+-----+-----+
+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID
| STATE | VOLUMES |
+-----+-----+
+-----+-----+-----+
| ontap-nas-backend      | ontap-nas      | 52f2eb10-e4c6-4160-99fc-
96b3be5ab5d7 | online |      25 |
+-----+-----+
+-----+-----+

```

```
cat ontap-nas-backend.json
```

```

{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.10.10.1",
  "dataLIF": "10.10.10.2",
  "backendName": "ontap-nas-backend",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "admin-password",
  "defaults": {
    "spaceReserve": "none",
    "encryption": "false"
  },
  "labels": {
    "store": "nas_store"
  },
  "region": "us_east_1",
  "storage": [
    {
      "labels": {
        "app": "msoffice",
        "cost": "100"
      },
      "zone": "us_east_1a",
      "defaults": {
        "spaceReserve": "volume",
        "encryption": "true",
        "unixPermissions": "0755"
      }
    }
  ],
}

```

```

    "labels": {
      "app": "mysqldb",
      "cost": "25"
    },
    "zone": "us_east_1d",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "false",
      "unixPermissions": "0775"
    }
  }
]
}

```

Étape 1 : Créer un secret Kubernetes

Créez un Secret qui contient les identifiants pour le backend, comme indiqué dans cet exemple :

```
cat tbc-ontap-nas-backend-secret.yaml
```

```

apiVersion: v1
kind: Secret
metadata:
  name: ontap-nas-backend-secret
type: Opaque
stringData:
  username: cluster-admin
  password: admin-password

```

```

kubectl create -f tbc-ontap-nas-backend-secret.yaml -n trident
secret/backend-tbc-ontap-san-secret created

```

Étape 2 : Créer un TridentBackendConfig CR

L'étape suivante consiste à créer un TridentBackendConfig CR qui se liera automatiquement à la ontap-nas-backend préexistante (comme dans cet exemple). Assurez-vous que les conditions suivantes sont remplies :

- Le même nom de backend est défini dans `spec.backendName`.
- Les paramètres de configuration sont identiques à ceux du backend d'origine.
- Les pools virtuels (le cas échéant) doivent conserver le même ordre que dans le backend d'origine.
- Les informations d'identification sont fournies via un Secret Kubernetes et non en texte clair.

Dans ce cas, le TridentBackendConfig ressemblera à ceci :

```
cat backend-tbc-ontap-nas.yaml
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: tbc-ontap-nas-backend
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.10.10.1
  dataLIF: 10.10.10.2
  backendName: ontap-nas-backend
  svm: trident_svm
  credentials:
    name: mysecret
  defaults:
    spaceReserve: none
    encryption: 'false'
  labels:
    store: nas_store
  region: us_east_1
  storage:
  - labels:
      app: msoffice
      cost: '100'
      zone: us_east_1a
      defaults:
        spaceReserve: volume
        encryption: 'true'
        unixPermissions: '0755'
  - labels:
      app: mysqldb
      cost: '25'
      zone: us_east_1d
      defaults:
        spaceReserve: volume
        encryption: 'false'
        unixPermissions: '0775'
```

```
kubectl create -f backend-tbc-ontap-nas.yaml -n trident
```

```
tridentbackendconfig.trident.netapp.io/tbc-ontap-nas-backend created
```

Étape 3 : Vérifiez le statut du `TridentBackendConfig` CR

Après la `TridentBackendConfig` création, sa phase doit être `Bound`. Il doit également refléter le même nom de backend et le même UUID que le backend existant.

```
kubectl get tbc tbc-ontap-nas-backend -n trident
```

NAME	BACKEND NAME	BACKEND UUID
tbc-ontap-nas-backend	ontap-nas-backend	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7
Bound	Success	

#confirm that no new backends were created (i.e., `TridentBackendConfig` did not end up creating a new backend)

```
tridentctl get backend -n trident
```

NAME	STORAGE DRIVER	UUID
ontap-nas-backend	ontap-nas	52f2eb10-e4c6-4160-99fc-96b3be5ab5d7
online	25	

Le backend sera désormais entièrement géré à l'aide de l' `tbc-ontap-nas-backend` `TridentBackendConfig` objet.

Gérer `TridentBackendConfig` les backends à l'aide de `tridentctl`

`tridentctl` peut être utilisé pour lister les backends qui ont été créés à l'aide de `TridentBackendConfig`. De plus, les administrateurs peuvent également choisir de gérer entièrement ces backends via `tridentctl` en supprimant `TridentBackendConfig` et en s'assurant que `spec.deletionPolicy` est défini sur `retain`.

Étape 0 : Identifier le backend

Par exemple, supposons que le backend suivant ait été créé à l'aide de `TridentBackendConfig`:

```
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
```

NAME	BACKEND NAME	BACKEND UUID
------	--------------	--------------

```

PHASE      STATUS      STORAGE DRIVER      DELETION POLICY
backend-tbc-ontap-san  ontap-san-backend  81abcb27-ea63-49bb-b606-
0a5315ac5f82  Bound      Success      ontap-san      delete

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |                      UUID
| STATE  | VOLUMES |
+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |          33 |
+-----+-----+
+-----+-----+-----+-----+

```

D'après le résultat, on constate que TridentBackendConfig a été créé avec succès et est lié à un backend [observer l'UUID du backend].

Étape 1 : Confirmer `deletionPolicy` est défini sur `retain`

Examinons la valeur de `deletionPolicy`. Celle-ci doit être définie sur `retain`. Cela garantit que lorsqu'une TridentBackendConfig CR est supprimée, la définition backend sera toujours présente et pourra être gérée avec `tridentctl`.

```

kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME      BACKEND UUID
PHASE      STATUS      STORAGE DRIVER      DELETION POLICY
backend-tbc-ontap-san  ontap-san-backend  81abcb27-ea63-49bb-b606-
0a5315ac5f82  Bound      Success      ontap-san      delete

# Patch value of deletionPolicy to retain
kubectl patch tbc backend-tbc-ontap-san --type=merge -p
'{"spec":{"deletionPolicy":"retain"}}' -n trident
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-san patched

#Confirm the value of deletionPolicy
kubectl get tbc backend-tbc-ontap-san -n trident -o wide
NAME                                BACKEND NAME      BACKEND UUID
PHASE      STATUS      STORAGE DRIVER      DELETION POLICY
backend-tbc-ontap-san  ontap-san-backend  81abcb27-ea63-49bb-b606-
0a5315ac5f82  Bound      Success      ontap-san      retain

```



Ne passez pas à l'étape suivante à moins que `deletionPolicy` soit défini sur `retain`.

Étape 2 : Supprimer le `TridentBackendConfig` CR

La dernière étape consiste à supprimer le `TridentBackendConfig` CR. Après avoir confirmé que le `deletionPolicy` est défini sur `retain`, vous pouvez procéder à la suppression :

```
kubectl delete tbc backend-tbc-ontap-san -n trident
tridentbackendconfig.trident.netapp.io "backend-tbc-ontap-san" deleted

tridentctl get backend ontap-san-backend -n trident
+-----+-----+
+-----+-----+-----+-----+
|      NAME      | STORAGE DRIVER |                               UUID
| STATE  | VOLUMES |
+-----+-----+
+-----+-----+-----+-----+
| ontap-san-backend | ontap-san      | 81abcb27-ea63-49bb-b606-
0a5315ac5f82 | online |      33 |
+-----+-----+
+-----+-----+-----+-----+
```

Lors de la suppression de l'`TridentBackendConfig` objet, Trident le supprime simplement sans supprimer le backend lui-même.

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.