



Connaissances et support

Trident

NetApp
September 26, 2025

Sommaire

Connaissances et support	1
Foire aux questions	1
Questions générales	1
Installez et utilisez Trident sur un cluster Kubernetes	1
Dépannage et support	3
Mettez à niveau Trident	4
Gestion des systèmes back-end et des volumes	4
Dépannage	8
Dépannage général	8
Échec du déploiement de Trident avec l'opérateur	10
Échec du déploiement Trident avec <code>tridentctl</code>	12
Retirez complètement les Trident et les CRD	12
Échec de l'annulation du transfert de nœud NVMe avec les espaces de noms de bloc bruts RWX o Kubernetes 1.26	13
Assistance	14
Cycle de vie du support Trident	14
Auto-assistance	15
Soutien de la communauté	15
Support technique NetApp	15
Pour en savoir plus	15

Connaissances et support

Foire aux questions

Trouvez les réponses aux questions fréquemment posées sur l'installation, la configuration, la mise à niveau et le dépannage de Trident.

Questions générales

À quelle fréquence le Trident est-il commercialisé ?

Trident est commercialisé tous les quatre mois à partir de la version 24.02 : février, juin et octobre.

Trident prend-il en charge toutes les fonctionnalités publiées dans une version spécifique de Kubernetes ?

Trident ne prend généralement pas en charge les fonctionnalités alpha dans Kubernetes. Trident peut prendre en charge les fonctionnalités bêta dans les deux versions de Trident, qui suivent la version bêta de Kubernetes.

Le fonctionnement de Trident dépend-il d'autres produits NetApp ?

Trident ne dépend d'aucun autre produit logiciel NetApp et fonctionne comme une application autonome. Toutefois, vous devez disposer d'un système de stockage back-end NetApp.

Comment puis-je obtenir des informations complètes sur la configuration de Trident ?

Utilisez `tridentctl get` la commande pour obtenir plus d'informations sur votre configuration Trident.

Puis-je obtenir des indicateurs sur le provisionnement du stockage par Trident ?

Oui. Les terminaux Prometheus peuvent être utilisés pour rassembler des informations sur les opérations Trident, telles que le nombre de systèmes back-end gérés, le nombre de volumes provisionnés, d'octets consommés, etc. Vous pouvez également l'utiliser "[Cloud Insights](#)" pour la surveillance et l'analyse.

L'expérience utilisateur change-t-elle lors de l'utilisation de Trident en tant que mécanisme de provisionnement CSI ?

Non. Il n'y a pas de changement en ce qui concerne l'expérience utilisateur et les fonctionnalités. Le nom de provisionneur utilisé est `csi.trident.netapp.io`. Cette méthode d'installation de Trident est recommandée si vous souhaitez utiliser toutes les nouvelles fonctionnalités fournies par les versions actuelles et futures.

Installez et utilisez Trident sur un cluster Kubernetes

Trident prend-il en charge une installation hors ligne à partir d'un registre privé ?

Oui, Trident peut être installé hors ligne. Reportez-vous à la "[En savoir plus sur l'installation de Trident](#)".

Puis-je installer Trident à distance ?

Oui. Trident 18.10 et les versions ultérieures prennent en charge la fonctionnalité d'installation à distance à partir de n'importe quelle machine ayant `kubectl` accès au cluster. Une fois l' `kubectl` accès vérifié (par exemple, lancez une `kubectl get nodes` commande à partir de l'ordinateur distant pour vérifier), suivez les instructions d'installation.

Puis-je configurer la haute disponibilité avec Trident ?

Trident est installé en tant que déploiement Kubernetes (ReplicaSet) avec une instance. Sa haute disponibilité est donc intégrée. Vous ne devez pas augmenter le nombre de répliques dans le déploiement. Si le nœud sur lequel Trident est installé est perdu ou si le pod est inaccessible, Kubernetes redéploie automatiquement le pod vers un nœud sain dans le cluster. Trident est un plan de contrôle uniquement. Les pods actuellement montés ne sont donc pas affectés si Trident est redéployé.

Trident a-t-il besoin d'accéder à l'espace de noms du système kube ?

Trident lit depuis le serveur d'API Kubernetes pour déterminer quand les applications demandent de nouvelles ESV et doit donc accéder à `kube-system`.

Quels sont les rôles et les Privileges utilisés par Trident ?

Le programme d'installation Trident crée un cluster Kubernetes ClusterRole, qui dispose d'un accès spécifique aux ressources PersistentVolume, PersistentVolumeClaim, StorageClass et Secret du cluster Kubernetes. Reportez-vous à la "[Personnalisez l'installation tridentctl](#)".

Puis-je générer localement les fichiers de manifeste exacts que Trident utilise pour l'installation ?

Vous pouvez, si nécessaire, générer et modifier localement les fichiers de manifeste exacts que Trident utilise pour l'installation. Reportez-vous à la "[Personnalisez l'installation tridentctl](#)".

Puis-je partager le même SVM back-end ONTAP pour deux instances Trident distinctes pour deux clusters Kubernetes distincts ?

Bien qu'il ne soit pas conseillé, vous pouvez utiliser la même SVM back-end pour deux instances Trident. Spécifiez un nom de volume unique pour chaque instance lors de l'installation et/ou spécifiez un paramètre unique `StoragePrefix` dans `setup/backend.json` le fichier. Ceci permet de s'assurer que le même FlexVol n'est pas utilisé pour les deux instances.

Est-il possible d'installer Trident sous ContainerLinux (anciennement CoreOS) ?

Trident est un pod Kubernetes qui peut être installé quel que soit l'emplacement d'exécution de Kubernetes.

Puis-je utiliser Trident avec NetApp Cloud Volumes ONTAP ?

Oui, Trident est pris en charge sur AWS, Google Cloud et Azure.

Trident fonctionne-t-il avec Cloud volumes Services ?

Oui, Trident prend en charge le service Azure NetApp Files dans Azure ainsi que Cloud Volumes Service dans GCP.

Dépannage et support

NetApp prend-il en charge Trident ?

Bien que Trident soit open source et gratuit, NetApp le prend entièrement en charge, à condition que votre back-end NetApp soit pris en charge.

Comment puis-je soulever un dossier de demande de support ?

Pour soulever un dossier de support, effectuez l'une des opérations suivantes :

1. Contactez votre support Account Manager pour obtenir de l'aide pour créer un dossier.
2. Soulevez un dossier de demande de support en contactant "[Support NetApp](#)".

Comment générer un bundle de journaux de support ?

Vous pouvez créer un bundle de support en exécutant `tridentctl logs -a`. Outre les journaux capturés dans le pack, capture le journal kubelet pour diagnostiquer les problèmes de montage côté Kubernetes. Les instructions d'obtention du journal kubelet varient en fonction de l'installation de Kubernetes.

Que faire si j'ai besoin de demander une nouvelle fonctionnalité ?

Créez un problème "[Trident Github](#)" et mentionnez **RFE** dans l'objet et la description du problème.

Où puis-je soulever un défaut ?

Créez un problème sur "[Trident Github](#)". Veillez à inclure toutes les informations et tous les journaux nécessaires concernant le problème.

Que se passe-t-il si j'ai une brève question sur Trident et que j'ai besoin d'éclaircissements ? Y a-t-il une communauté ou un forum ?

Pour toute question, problème ou demande, contactez-nous par le biais de notre Trident "[Déroulez le canal](#)" ou GitHub.

Le mot de passe de mon système de stockage a changé et Trident ne fonctionne plus. Comment puis-je le récupérer ?

Mettez à jour le mot de passe du backend avec `tridentctl update backend myBackend -f </path/to_new_backend.json> -n trident`. Remplacez `myBackend` dans l'exemple par votre nom de back-end et `~/path/to_new_backend.json` par le chemin d'accès au fichier correct `backend.json`.

Trident ne trouve pas mon nœud Kubernetes. Comment résoudre ce problème ?

Trident ne trouve pas de nœud Kubernetes dans deux scénarios possibles. Elle peut être due à un problème de mise en réseau dans Kubernetes ou DNS. Le démonset de nœuds Trident qui s'exécute sur chaque nœud Kubernetes doit pouvoir communiquer avec le contrôleur Trident pour enregistrer le nœud avec Trident. Si des modifications de mise en réseau se sont produites après l'installation de Trident, ce problème survient uniquement avec les nouveaux nœuds Kubernetes ajoutés au cluster.

Si le pod Trident est détruit, ces données seront-elles perdues ?

Les données ne seront pas perdues si le pod Trident est détruit. Les métadonnées Trident sont stockées dans des objets CRD. Tous les volumes persistants provisionnés par Trident fonctionneront normalement.

Mettez à niveau Trident

Est-il possible de mettre à niveau une version plus ancienne directement vers une version plus récente (sans passer par quelques versions) ?

NetApp prend en charge la mise à niveau de Trident d'une version majeure vers la prochaine version majeure immédiate. Vous pouvez effectuer la mise à niveau de la version 18.xx vers la version 19.xx, 19.xx vers la version 20.xx, etc. Il est conseillé de tester la mise à niveau dans un laboratoire avant le déploiement en production.

Est-il possible de revenir à une version antérieure de Trident ?

Si vous avez besoin d'un correctif pour les bogues observés après une mise à niveau, des problèmes de dépendance ou une mise à niveau non réussie ou incomplète, vous devez "[Désinstallez Trident](#)" réinstaller la version précédente en suivant les instructions spécifiques à cette version. Il s'agit de la seule méthode recommandée pour revenir à une version antérieure.

Gestion des systèmes back-end et des volumes

Dois-je définir à la fois des LIF de données et de gestion dans un fichier de définition du back-end ONTAP ?

Le LIF de gestion est obligatoire. Data LIF varie :

- San ONTAP : ne spécifiez pas pour iSCSI. Trident utilise "[Mappage de LUN sélectif ONTAP](#)" pour découvrir les LIF iSCSI nécessaires à l'établissement d'une session à chemins multiples. Un avertissement est généré si `dataLIF` est explicitement défini. Voir "[Options et exemples de configuration du SAN ONTAP](#)" pour plus de détails.
- NAS ONTAP : nous vous recommandons de spécifier `dataLIF`. Si non fourni, Trident récupère les LIFs de données du SVM. Vous pouvez spécifier un nom de domaine complet (FQDN) à utiliser pour les opérations de montage NFS, permettant de créer un DNS Round-Robin pour équilibrer la charge sur plusieurs LIF de données. Voir "[Options et exemples de configuration du NAS ONTAP](#)" pour plus de détails

Trident peut-il configurer CHAP pour les systèmes back-end ONTAP ?

Oui. Trident prend en charge le protocole CHAP bidirectionnel pour les systèmes back-end ONTAP. Ceci nécessite la `useCHAP=true` configuration de votre back-end.

Comment gérer les règles d'exportation avec Trident ?

Trident peut créer et gérer de manière dynamique des règles d'exportation à partir de la version 20.04. Cela permet à l'administrateur de stockage de fournir un ou plusieurs blocs CIDR dans leur configuration backend et de laisser Trident ajouter des adresses IP de nœud comprise dans ces plages à une export policy créée. De cette manière, Trident gère automatiquement l'ajout et la suppression de règles pour les nœuds avec des adresses IP dans les délais de modification donnés.

Les adresses IPv6 peuvent-elles être utilisées pour les LIF de données et de gestion ?

Trident prend en charge la définition des adresses IPv6 pour :

- `managementLIF` Et `dataLIF` pour les systèmes ONTAP back-end NAS.
- `managementLIF` Pour les systèmes SAN ONTAP back-end. Vous ne pouvez pas spécifier `dataLIF` sur un système SAN backend ONTAP.

Trident doit être installé à l'aide de l'indicateur `--use-ipv6` (pour l' `tridentctl`installation`), ``IPv6` (pour l'opérateur Trident) ou `tridentTPv6` (pour l'installation Helm) pour qu'il fonctionne sur IPv6.

Est-il possible de mettre à jour la LIF de gestion en back-end ?

Oui, il est possible de mettre à jour le LIF back-end Management à l'aide de la `tridentctl update backend` commande.

Est-il possible de mettre à jour la LIF de données sur le backend ?

Vous pouvez mettre à jour la LIF Data sur `ontap-nas` et `ontap-nas-economy` uniquement.

Est-il possible de créer plusieurs systèmes back-end dans Trident pour Kubernetes ?

Trident peut prendre en charge plusieurs systèmes back-end simultanément, avec le même pilote ou des pilotes différents.

Comment Trident stocke-t-il les informations d'identification back-end ?

Trident stocke les informations d'identification du back-end en tant que secrets Kubernetes.

Comment Trident sélectionne-t-il un back-end spécifique ?

Si les attributs back-end ne peuvent pas être utilisés pour sélectionner automatiquement les pools appropriés pour une classe, les `storagePools` paramètres et `additionalStoragePools` sont utilisés pour sélectionner un ensemble spécifique de pools.

Comment s'assurer que Trident ne se provisionne pas à partir d'un back-end spécifique ?

Le `excludeStoragePools` paramètre est utilisé pour filtrer l'ensemble de pools que Trident utilise pour le provisionnement et supprime tous les pools correspondant.

En cas de systèmes back-end multiples du même type, comment Trident sélectionne-t-il le système back-end à utiliser ?

S'il existe plusieurs systèmes back-end configurés du même type, Trident sélectionne le back-end approprié en fonction des paramètres présents dans `StorageClass` et `PersistentVolumeClaim`. Par exemple, s'il existe plusieurs systèmes back-end de pilotes ONTAP-nas, Trident tente de faire correspondre les paramètres dans le `StorageClass` et le combiné et `PersistentVolumeClaim` un back-end qui peut répondre aux exigences répertoriées dans `StorageClass` le et ``PersistentVolumeClaim`le` . Si plusieurs systèmes back-end correspondent à la demande, Trident les sélectionne de manière aléatoire.

Trident prend-il en charge le protocole CHAP bidirectionnel avec Element/SolidFire ?

Oui.

Comment Trident déploie-t-il les qtrees sur un volume ONTAP ? Combien de qtrees peuvent-ils être déployés sur un seul volume ?

Le `ontap-nas-economy` pilote crée jusqu'à 200 qtrees dans le même FlexVol (configurable entre 50 et 300), 100,000 qtrees par nœud de cluster et 2,4 millions par cluster. Lorsque vous entrez un nouveau `PersistentVolumeClaim` qui est entretenu par le conducteur économique, le conducteur recherche s'il existe déjà un FlexVol qui peut réparer le nouveau qtree. Si la FlexVol n'existe pas qui peut traiter le qtree, un nouveau FlexVol est créé.

Comment définir des autorisations Unix pour les volumes provisionnés sur ONTAP NAS ?

Vous pouvez définir des autorisations Unix sur le volume provisionné par Trident en définissant un paramètre dans le fichier de définition back-end.

Comment configurer un ensemble explicite d'options de montage NFS ONTAP lors du provisionnement d'un volume ?

Par défaut, Trident ne définit aucune valeur des options de montage sur Kubernetes. Pour spécifier les options de montage dans la classe de stockage Kubernetes, suivez l'exemple donné ["ici"](#).

Comment définir les volumes provisionnés sur une export policy spécifique ?

Pour permettre aux hôtes appropriés d'accéder à un volume, utilisez le `exportPolicy` paramètre configuré dans le fichier de définition back-end.

Comment définir le chiffrement des volumes via Trident avec ONTAP ?

Vous pouvez définir le chiffrement sur le volume provisionné par Trident à l'aide du paramètre de chiffrement dans le fichier de définition back-end. Pour plus d'informations, reportez-vous à : ["Fonctionnement de Trident avec NVE et NAE"](#)

Quel est le meilleur moyen d'implémenter la QoS pour ONTAP via Trident ?

```
`StorageClasses` Permet d'implémenter la QoS pour ONTAP.
```

Comment spécifier le provisionnement fin ou non fin via Trident ?

Les pilotes ONTAP prennent en charge le provisionnement fin ou non fin. Le provisionnement fin est par défaut pour les pilotes ONTAP. Si vous souhaitez effectuer un provisionnement lourd, vous devez configurer le fichier de définition du back-end ou le `StorageClass`. Si les deux sont configurés, `StorageClass` a priorité. Configurez les éléments suivants pour ONTAP :

1. Sur `StorageClass`, définissez l'attribut `provisioningType` sur épais.
2. Dans le fichier de définition back-end, activez les volumes lourds en les définissant `backend spaceReserve parameter` comme volume.

Comment puis-je m'assurer que les volumes utilisés ne sont pas supprimés même si je supprime accidentellement le volume de volume persistant ?

La protection contre la demande de volume persistant est automatiquement activée sur Kubernetes à partir de la version 1.10.

Puis-je augmenter les ESV NFS créées par Trident ?

Oui. Vous pouvez développer une demande de volume persistant créée par Trident. Notez que la croissance automatique de volume est une fonctionnalité ONTAP qui n'est pas applicable à Trident.

Puis-je importer un volume en mode SnapMirror Data protection (DP) ou hors ligne ?

L'importation du volume échoue si le volume externe est en mode DP ou est hors ligne. Vous recevez le message d'erreur suivant :

```
Error: could not import volume: volume import failed to get size of
volume: volume <name> was not found (400 Bad Request) command terminated
with exit code 1.
Make sure to remove the DP mode or put the volume online before importing
the volume.
```

Comment un quota de ressources est-il traduit-il vers un cluster NetApp ?

Le quota de ressources de stockage Kubernetes doit fonctionner tant que le stockage NetApp possède de la capacité. Lorsque le stockage NetApp ne peut pas respecter les paramètres des quotas Kubernetes en raison d'un manque de capacité, Trident tente de se provisionner, mais des erreurs se produisent.

Puis-je créer des copies Snapshot de volume à l'aide de Trident ?

Oui. La création de snapshots de volumes à la demande et de volumes persistants à partir de snapshots sont prises en charge par Trident. Pour créer des volumes persistants à partir de snapshots, assurez-vous que la `VolumeSnapshotDataSource` porte de fonctionnalité a été activée.

Quels sont les pilotes qui prennent en charge les copies Snapshot de volume Trident ?

À partir d'aujourd'hui, la prise en charge de snapshots à la demande est disponible pour nos `ontap-nas`, `ontap-nas-flexgroup` `ontap-san` `ontap-san-economy` `solidfire-san` , , , , `gcp-cvs`, et `azure-netapp-files` pilotes backend.

Comment effectuer une sauvegarde Snapshot d'un volume provisionné par Trident avec ONTAP ?

Cette option est disponible sur les `ontap-nas` pilotes , `ontap-san` et `ontap-nas-flexgroup`. Vous pouvez également spécifier un `snapshotPolicy` pour le `ontap-san-economy` pilote au niveau FlexVol.

Cela est également disponible sur les `ontap-nas-economy` pilotes, mais au niveau de la granularité FlexVol, et non au niveau `qtree`. Pour activer la fonction de snapshot des volumes provisionnés par Trident, définissez l'option du paramètre back-end `snapshotPolicy` sur la règle de snapshot souhaitée, comme défini sur le back-end ONTAP. Les snapshots pris par le contrôleur de stockage ne sont pas connus par Trident.

Puis-je définir un pourcentage de réserve Snapshot pour un volume provisionné via Trident ?

Oui, vous pouvez réserver un pourcentage spécifique d'espace disque pour stocker les copies Snapshot via Trident en définissant l'attribut `snapshotReserve`` dans le fichier de définition back-end. Si vous avez configuré `snapshotPolicy`` et `snapshotReserve`` dans le fichier de définition back-end, le pourcentage de réserve de snapshots est défini en fonction du `snapshotReserve`` pourcentage mentionné dans le fichier back-end. Si le `snapshotReserve`` pourcentage n'est pas mentionné, ONTAP utilise par défaut le pourcentage de réserve d'instantanés à 5. Si l'option `snapshotPolicy`` est définie sur aucun, le pourcentage de réserve d'instantanés est défini sur 0.

Puis-je accéder directement au répertoire de snapshot de volume et copier les fichiers ?

Oui, vous pouvez accéder au répertoire de snapshot sur le volume provisionné par Trident en définissant le `snapshotDir`` paramètre dans le fichier de définition back-end.

Puis-je configurer SnapMirror pour les volumes via Trident ?

Actuellement, SnapMirror doit être défini en externe via l'interface de ligne de commande ONTAP ou OnCommand System Manager.

Comment restaurer des volumes persistants à un snapshot ONTAP spécifique ?

Pour restaurer un volume sur un snapshot ONTAP, effectuez les opérations suivantes :

1. Arrêter le pod d'application qui utilise le volume persistant.
2. Restaurez les données vers le snapshot requis via l'interface de ligne de commande de ONTAP ou OnCommand System Manager.
3. Redémarrez le pod d'application.

Trident peut-il provisionner des volumes sur des SVM dont un miroir de partage de charge est configuré ?

Des miroirs de partage de charge peuvent être créés pour les volumes root des SVM qui fournissent des données sur NFS. ONTAP met automatiquement à jour les miroirs de partage de charge pour les volumes qui ont été créés par Trident. Cela peut entraîner des retards dans le montage des volumes. Lorsque plusieurs volumes sont créés via Trident, le provisionnement d'un volume dépend de la mise à jour par ONTAP du miroir de partage de charge.

Comment puis-je séparer l'utilisation de la classe de stockage pour chaque client/locataire ?

Kubernetes n'autorise pas les classes de stockage dans les espaces de noms. Toutefois, vous pouvez utiliser Kubernetes pour limiter l'utilisation d'une classe de stockage spécifique par espace de noms à l'aide de quotas de ressources de stockage, qui sont par espace de noms. Pour refuser un accès d'espace de noms spécifique à un stockage spécifique, définissez le quota de ressources sur 0 pour cette classe de stockage.

Dépannage

Utilisez les pointeurs fournis ici pour résoudre les problèmes que vous pouvez rencontrer lors de l'installation et de l'utilisation de Trident.

Dépannage général

- Si le pod Trident ne parvient pas à se mettre correctement en place (par exemple, lorsque le pod Trident est bloqué `ContainerCreating` en phase avec moins de deux conteneurs prêts), il s'exécute `kubectl -n trident describe deployment trident` et `kubectl -n trident describe pod trident--**` peut fournir des informations supplémentaires. L'obtention de journaux kubelet (par exemple, via `journalctl -xeu kubelet`) peut également être utile.
- Si les journaux Trident ne contiennent pas suffisamment d'informations, vous pouvez essayer d'activer le mode de débogage pour Trident en transmettant l'indicateur au paramètre d'installation en `-d` fonction de votre option d'installation.

Confirmez ensuite que le débogage est défini à l'aide de `./tridentctl logs -n trident` et en recherchant `level=debug msg` dans le journal.

Installé avec l'opérateur

```
kubectl patch torc trident -n <namespace> --type=merge -p
'{"spec":{"debug":true}}'
```

Cela redémarrera tous les modules Trident, ce qui peut prendre plusieurs secondes. Vous pouvez le vérifier en observant la colonne 'ÂGE' dans la sortie de `kubectl get pod -n trident`.

Pour Trident 20.07 et 20.10, utiliser à la `tprov` place de `torc`.

Installé avec Helm

```
helm upgrade <name> trident-operator-21.07.1-custom.tgz --set
tridentDebug=true`
```

Installé avec tridentctl

```
./tridentctl uninstall -n trident
./tridentctl install -d -n trident
```

- Vous pouvez également obtenir des journaux de débogage pour chaque back-end en les incluant `debugTraceFlags` dans votre définition back-end. Par exemple, inclure `debugTraceFlags: {"api":true, "method":true,}` pour obtenir des appels API et des traversées de méthode dans les journaux Trident. Les systèmes back-end existants peuvent avoir été `debugTraceFlags` configurés avec un `tridentctl backend update`.
- Lorsque vous utilisez RedHat CoreOS, assurez-vous que `iscsid` est activé sur les nœuds worker et démarré par défaut. Pour ce faire, utilisez OpenShift MachineConfiguration ou modifiez les modèles d'allumage.
- Un problème courant que vous pourriez rencontrer lors de l'utilisation de Trident avec ["Azure NetApp Files"](#) est lorsque les secrets du locataire et du client proviennent d'un enregistrement d'application avec des autorisations insuffisantes. Pour obtenir la liste complète des exigences Trident, reportez-vous à la section ["Azure NetApp Files" Configuration](#).
- Si vous rencontrez des problèmes lors du montage d'un PV sur un conteneur, assurez-vous que `rpcbind` est installé et en cours d'exécution. Utilisez le gestionnaire de paquets requis pour le système d'exploitation hôte et vérifiez si `rpcbind` est en cours d'exécution. Vous pouvez vérifier l'état du `rpcbind` service en exécutant un `systemctl status rpcbind` ou son équivalent.
- Si un back-end Trident signale qu'il est dans `failed` l'état malgré ses opérations auparavant, cela est probablement dû à la modification des informations d'identification de SVM/admin associées au back-end. La mise à jour des informations du back-end à l'aide du `tridentctl update backend module Trident` ou son rebond résoudra ce problème.
- Si vous rencontrez des problèmes d'autorisation lors de l'installation de Trident avec Docker comme runtime du conteneur, essayez l'installation de Trident avec `--in cluster=false` l'indicateur. Cela n'utilisera pas de pod d'installation et évitera les problèmes d'autorisation vus par l'`trident-installer` utilisateur.
- Utiliser le `uninstall` parameter `<Uninstalling Trident>` pour le nettoyage après un échec de l'analyse. Par défaut, le script ne supprime pas les CRD créés par Trident, ce qui rend possible leur désinstallation et leur installation en toute sécurité, même dans le cadre d'un déploiement en cours d'exécution.

- Si vous souhaitez revenir à une version antérieure de Trident, exécutez d'abord la `tridentctl uninstall` commande pour supprimer Trident. Téléchargez le "[Version Trident](#)" et installez à l'aide de la `tridentctl install` commande.
- Après une installation réussie, si une demande de volume persistant est bloquée dans la `Pending` phase, l'exécution `kubect1 describe pvc` peut fournir des informations supplémentaires sur les raisons pour lesquelles Trident n'a pas pu provisionner de volume persistant pour cette demande de volume persistant.

Échec du déploiement de Trident avec l'opérateur

Si vous déployez Trident à l'aide de l'opérateur, l'état `TridentOrchestrator` passe de `Installing` à `Installed`. Si vous observez l'`Failed` état et que l'opérateur ne parvient pas à restaurer lui-même, vous devez vérifier les journaux de l'opérateur en exécutant la commande suivante :

```
tridentctl logs -l trident-operator
```

Traînant les journaux du conteneur de l'opérateur `trident` peut pointer vers l'emplacement où se trouve le problème. Par exemple, un tel problème pourrait être l'impossibilité d'extraire les images de conteneur requises des registres en amont dans un environnement mis à l'air.

Pour comprendre pourquoi l'installation de Trident a échoué, consultez l'`TridentOrchestrator` état.

```

kubect1 describe torc trident-2
Name:          trident-2
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Status:
  Current Installation Params:
    IPv6:
    Autosupport Hostname:
    Autosupport Image:
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:
    Image Pull Secrets:          <nil>
    Image Registry:
    k8sTimeout:
    Kubelet Dir:
    Log Format:
    Silence Autosupport:
    Trident Image:
  Message:          Trident is bound to another CR 'trident'
  Namespace:       trident-2
  Status:          Error
  Version:
Events:
  Type          Reason    Age          From          Message
  ----          -
Warning Error    16s (x2 over 16s) trident-operator.netapp.io Trident
is bound to another CR 'trident'

```

Cette erreur indique qu'il existe déjà un `TridentOrchestrator` qui a été utilisé pour installer Trident. Étant donné que chaque cluster Kubernetes ne peut avoir qu'une seule instance de Trident, l'opérateur s'assure qu'à un moment donné il n'existe qu'une instance active qu'`TridentOrchestrator`il peut créer.

De plus, l'observation de l'état des pods Trident peut souvent indiquer si quelque chose n'est pas approprié.

```
kubectl get pods -n trident
```

NAME	READY	STATUS	RESTARTS
trident-csi-4p5kq 5m18s	1/2	ImagePullBackOff	0
trident-csi-6f45bfd8b6-vfrkw 5m19s	4/5	ImagePullBackOff	0
trident-csi-9q5xc 5m18s	1/2	ImagePullBackOff	0
trident-csi-9v95z 5m18s	1/2	ImagePullBackOff	0
trident-operator-766f7b8658-ldzsv 8m17s	1/1	Running	0

Vous pouvez clairement voir que les modules ne peuvent pas être initialisés complètement parce qu'une ou plusieurs images de conteneur n'ont pas été extraites.

Pour résoudre le problème, vous devez modifier la demande de modification `TridentOrchestrator`. Vous pouvez également supprimer `TridentOrchestrator` et en créer un nouveau avec la définition modifiée et précise.

Échec du déploiement Trident avec `tridentctl`

Pour vous aider à comprendre ce qui ne s'est pas passé, vous pouvez exécuter à nouveau le programme d'installation à l'aide de `-d` argument, qui va activer le mode de débogage et vous aider à comprendre le problème :

```
./tridentctl install -n trident -d
```

Après avoir résolu le problème, vous pouvez nettoyer l'installation comme suit, puis exécuter de nouveau la `tridentctl install` commande :

```
./tridentctl uninstall -n trident
INFO Deleted Trident deployment.
INFO Deleted cluster role binding.
INFO Deleted cluster role.
INFO Deleted service account.
INFO Removed Trident user from security context constraint.
INFO Trident uninstallation succeeded.
```

Retirez complètement les Trident et les CRD

Vous pouvez supprimer complètement Trident et tous les CRD créés et les ressources personnalisées associées.



Cette opération ne peut pas être annulée. Ne le faites pas à moins que vous ne souhaitiez une installation entièrement nouvelle de Trident. Pour désinstaller Trident sans supprimer les CRD, reportez-vous "[Désinstaller Trident](#)" à la section .

Opérateur Trident

Pour désinstaller Trident et supprimer complètement les CRD à l'aide de l'opérateur Trident :

```
kubectl patch torc <trident-orchestrator-name> --type=merge -p
'{"spec":{"wipeout":["crds"],"uninstall":true}}'
```

Gouvernail

Pour désinstaller Trident et supprimer complètement les CRD à l'aide de l'assistant :

```
kubectl patch torc trident --type=merge -p
'{"spec":{"wipeout":["crds"],"uninstall":true}}'
```

`<code>` `</code>`

Pour supprimer complètement les CRD après avoir désinstallé Trident à l'aide de `tridentctl`

```
tridentctl obliviate crd
```

Échec de l'annulation du transfert de nœud NVMe avec les espaces de noms de bloc bruts RWX o Kubernetes 1.26

Si vous exécutez Kubernetes 1.26, l'annulation de l'environnement de nœud peut échouer lors de l'utilisation de NVMe/TCP avec les espaces de noms de bloc bruts RWX. Les scénarios suivants offrent une solution de contournement à la défaillance. Vous pouvez également mettre à niveau Kubernetes vers la version 1.27.

Espace de noms et pod supprimés

Imaginez un namespace géré par Trident (volume persistant NVMe) attaché à un pod. Si vous supprimez l'espace de nom directement du back-end ONTAP, le processus de déstaging est bloqué après la tentative de suppression du pod. Ce scénario n'a aucun impact sur le cluster Kubernetes ou tout autre fonctionnement.

Solution de contournement

Démontez le volume persistant (correspondant à cet espace de noms) du nœud respectif et supprimez-le.

DataLIFs bloquées

If you block (or bring down) all the dataLIFs of the NVMe Trident backend, the unstaging process gets stuck when you attempt to delete the pod. In this scenario, you cannot run any NVMe CLI commands on the Kubernetes node.

.Solution de contournement

Afficher les dataLIFS pour restaurer toutes les fonctionnalités.

Mappage de l'espace de noms supprimé

If you remove the `hostNQN` of the worker node from the corresponding subsystem, the unstaging process gets stuck when you attempt to delete the pod. In this scenario, you cannot run any NVMe CLI commands on the Kubernetes node.

.Solution de contournement

Ajoutez le `hostNQN` au sous-système.

Assistance

NetApp prend en charge Trident de plusieurs façons. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un canal discord.

Cycle de vie du support Trident

Trident propose trois niveaux de support en fonction de votre version. Reportez-vous à la ["Prise en charge de la version du logiciel NetApp pour les définitions"](#).

Support complet

Trident offre un support complet pendant douze mois à compter de sa date de sortie.

Prise en charge limitée

Trident offre un support limité pour les mois 13 à 24 à compter de la date de sortie.

Auto-assistance

La documentation Trident est disponible pour les mois 25 à 36 à compter de la date de publication.

Version	Support complet	Prise en charge limitée	Auto-assistance
"24,10"	Octobre 2025	Octobre 2026	Octobre 2027
"24,06"	Juin 2025	Juin 2026	Juin 2027
"24,02"	—	Février 2026	Février 2027
"23,10"	—	Octobre 2025	Octobre 2026

Version	Support complet	Prise en charge limitée	Auto-assistance
"23.07"	—	Juillet 2025	Juillet 2026
"23.04"	—	Avril 2025	Avril 2026
"23.01"	—	—	Janvier 2026
"22.10"	—	—	Octobre 2025
"22.07"	—	—	Juillet 2025
"22.04"	—	—	Avril 2025

Auto-assistance

Pour obtenir une liste complète des articles de dépannage, reportez-vous à ["Base de connaissances NetApp \(identifiant requis\)"](#)la .

Soutien de la communauté

Il existe une communauté publique dynamique d'utilisateurs de conteneurs (y compris les développeurs Trident) sur notre ["Déroulez le canal"](#). C'est un endroit idéal pour poser des questions d'ordre général sur le projet et discuter de sujets connexes avec des pairs partageant des mêmes idées.

Support technique NetApp

Pour obtenir de l'aide sur Trident, créez un bundle de support à l'aide de `tridentctl logs -a -n trident` et envoyez-le à [NetApp Support <Getting Help>](#).

Pour en savoir plus

- ["Ressources Trident"](#)
- ["Kubernetes Hub"](#)

Informations sur le copyright

Copyright © 2025 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.