



# **Documentation d'Astra Trident 24.06**

Astra Trident

NetApp

January 14, 2026

# Sommaire

Documentation d'Astra Trident 24.06 .....	1
Notes de mise à jour .....	2
Quoi de neuf .....	2
Nouveautés de la version 24.06 .....	2
Changements en 24.02 .....	3
Changements en 23.10 .....	3
Changements en 23.07.1 .....	4
Changements en 23.07 .....	4
Changements en 23.04 .....	5
Changements en 23.01.1 .....	7
Changements en 23.01 .....	7
Changements en 22.10 .....	8
Changements en 22.07 .....	9
Changements en 22.04 .....	10
Changements en 22.01.1 .....	11
Changements en 22.01.0 .....	11
Changements en 21.10.1 .....	12
Changements en 21.10.0 .....	12
Problèmes connus .....	13
Trouvez plus d'informations .....	14
Versions antérieures de la documentation .....	14
Commencez .....	15
Découvrez Astra Trident .....	15
Découvrez Astra Trident .....	15
Architecture d'Astra Trident .....	17
Concepts .....	20
Démarrage rapide d'Astra Trident .....	24
Et la suite ? .....	25
De formation .....	25
Informations stratégiques sur Astra Trident .....	26
Systèmes front-end (orchestrateurs) pris en charge .....	26
Systèmes back-end pris en charge (stockage) .....	26
Configuration requise .....	27
Systèmes d'exploitation hôtes testés .....	27
Configuration de l'hôte .....	28
Configuration du système de stockage .....	28
Ports Trident d'Astra .....	28
Images de conteneur et versions Kubernetes correspondantes .....	28
Installer Astra Trident .....	29
Installer à l'aide de l'opérateur Trident .....	29
Installation à l'aide de tridentctl .....	29
Avec Astra Trident .....	30
Préparez le nœud de travail .....	30

Choisir les bons outils	30
Détection des services de nœud	30
Volumes NFS	31
Volumes iSCSI	31
Volumes NVMe/TCP	35
Configuration et gestion des systèmes back-end	36
Configuration des systèmes back-end	36
Azure NetApp Files	37
Google Cloud NetApp volumes	55
Configurer un système Cloud Volumes Service pour Google Cloud backend	67
Configurer un système NetApp HCI ou SolidFire backend	79
Pilotes SAN de ONTAP	85
Pilotes NAS de ONTAP	110
Amazon FSX pour NetApp ONTAP	138
Création de systèmes back-end avec kubectl	170
Gestion des systèmes back-end	177
Créer et gérer des classes de stockage	186
Créer une classe de stockage	186
Gérer les classes de stockage	189
Provisionnement et gestion des volumes	191
Provisionner un volume	191
Développement des volumes	196
Importer des volumes	204
Personnaliser les noms et les étiquettes des volumes	211
Partager un volume NFS entre les espaces de noms	214
Réplication de volumes à l'aide de SnapMirror	218
Utiliser la topologie CSI	234
Travailler avec des instantanés	242
Gestion et contrôle d'Astra Trident	251
Mettez à niveau Astra Trident	251
Mettez à niveau Astra Trident	251
Mise à niveau avec l'opérateur	252
Mise à niveau avec tridentctl	257
Gérez Astra Trident à l'aide de tridentctl	257
Commandes et indicateurs globaux	257
Options et indicateurs de commande	259
Contrôle d'Astra Trident	265
Présentation	265
Étape 1 : définir une cible Prometheus	265
Étape 2 : créer un ServiceMonitor Prometheus	265
Étape 3 : interroger les mesures Trident avec PromQL	266
Découvrez la télémétrie AutoSupport d'Astra Trident	267
Désactivation des metrics d'Astra Trident	268
Désinstaller Astra Trident	268
Déterminez la méthode d'installation d'origine	269

Désinstallez l'installation d'un opérateur Trident	269
Désinstallez une <code>tridentctl</code> installation	270
Astra Trident pour Docker	271
Conditions préalables au déploiement	271
Vérifier les exigences	271
Outils NVMe	273
Déployez Astra Trident	274
Méthode de plug-in géré Docker (version 1.13/17.03 et ultérieure)	274
Méthode traditionnelle (version 1.12 ou antérieure)	276
Commencez avec Astra Trident au démarrage du système	278
Mise à niveau ou désinstallation d'Astra Trident	279
Mise à niveau	279
Désinstaller	280
Utilisation de volumes	281
Créer un volume	281
Supprimer un volume	281
Clonez un volume	281
Accéder aux volumes créés en externe	283
Options de volume spécifiques au conducteur	283
Collecte des journaux	289
Collecte des journaux pour le dépannage	289
Conseils généraux de dépannage	289
Gérez plusieurs instances Trident d'Astra	290
Étapes du plug-in géré par Docker (version 1.13/17.03 ou ultérieure)	290
Étapes pour les versions traditionnelles (version 1.12 ou antérieure)	290
Options de configuration du stockage	291
Options de configuration globale	291
Configuration DE L'INFRASTRUCTURE ONTAP	292
Configuration logicielle Element	299
Problèmes et limites connus	300
La mise à niveau de Trident Docker Volume Plug-in vers la version 20.10 et ultérieure à partir des versions plus anciennes entraîne un échec de mise à niveau, sans erreur de fichier ou de répertoire de ce type.	301
Les noms de volumes doivent comporter au moins 2 caractères.	301
Docker Swarm dispose de certains comportements qui empêchent Astra Trident de les prendre en charge avec chaque combinaison de stockage et de pilote.	301
Si un FlexGroup est provisionné, ONTAP ne provisionne pas un deuxième FlexGroup si le deuxième FlexGroup dispose d'un ou de plusieurs agrégats en commun avec la FlexGroup provisionnée.	301
Meilleures pratiques et recommandations	302
Déploiement	302
Déploiement dans un namespace dédié	302
Utilisez les quotas et les limites des plages pour contrôler la consommation du stockage	302
Configuration de stockage sous-jacente	302
Présentation de la plateforme	302
Meilleures pratiques pour ONTAP et Cloud Volumes ONTAP	302

Les meilleures pratiques pour SolidFire	307
Où trouver plus d'informations ?	309
Intégrer Astra Trident	309
Choix et déploiement du conducteur	309
Conception de classe de stockage	313
Conception de pool virtuel	314
Opérations de volume	315
Le déploiement des services OpenShift	317
Services de metrics	319
Protection des données et reprise d'activité	320
Réplication et restauration d'Astra Trident	320
Réplication et restauration des SVM	321
Réplication et restauration de volume	322
Protection des données Snapshot	322
Réplication des applications Astra Control Center	322
Sécurité	322
Sécurité	323
Configuration de clé unifiée Linux (LUKS)	324
Configuration du chiffrement Kerberos à la volée	329
Connaissances et support	338
Foire aux questions	338
Questions générales	338
Installez et utilisez Astra Trident sur un cluster Kubernetes	338
Dépannage et support	340
Mettez à niveau Astra Trident	341
Gestion des systèmes back-end et des volumes	341
Dépannage	345
Dépannage général	345
Échec du déploiement de Trident avec l'opérateur	347
Échec du déploiement Trident avec <code>tridentctl</code>	349
Retirez complètement Astra Trident et les CRD	349
Échec de l'annulation du transfert de nœud NVMe avec les espaces de noms de bloc bruts RWX ou Kubernetes 1.26	350
Assistance	351
Cycle de vie de prise en charge d'Astra Trident	351
Auto-assistance	352
Soutien de la communauté	352
Support technique NetApp	352
Pour en savoir plus	352
Référence	353
Ports Trident d'Astra	353
Ports Trident d'Astra	353
API REST d'Astra Trident	353
Quand utiliser l'API REST	353
Avec l'API REST	353

Options de ligne de commande .....	354
Journalisation .....	354
Kubernetes .....	354
Docker .....	355
REPOS .....	355
Kubernetes et objets Trident .....	355
Comment les objets interagissent-ils les uns avec les autres ? .....	355
Objets Kubernetes PersistentVolumeClaim .....	356
Objets Kubernetes PersistentVolume .....	358
Objets Kubernetes StorageClass .....	358
Objets Kubernetes VolumeSnapshotClass .....	362
Objets Kubernetes VolumeSnapshot .....	363
Objets Kubernetes VolumeSnapshotContent .....	363
Objets Kubernetes CustomResourceDefinition .....	363
Objets Astra Trident StorageClass .....	364
Objets back-end Astra Trident .....	364
Objets Astra Trident StoragePool .....	364
Objets Astra Trident Volume .....	365
Objets Astra Trident Snapshot .....	366
Objet Astra Trident ResourceQuota .....	367
Normes de sécurité de pod (PSS) et contraintes de contexte de sécurité (SCC) .....	368
Contexte de sécurité Kubernetes requis et champs associés .....	368
Normes de sécurité du pod (PSS) .....	369
Politiques de sécurité des pods (PSP) .....	369
Contraintes de contexte de sécurité (SCC) .....	371
Mentions légales .....	373
Droits d'auteur .....	373
Marques déposées .....	373
Brevets .....	373
Politique de confidentialité .....	373
Source ouverte .....	373

# Documentation d'Astra Trident 24.06

# Notes de mise à jour

## Quoi de neuf

Dans les notes de version, vous trouverez des informations sur les nouvelles fonctionnalités, les améliorations et les correctifs de bogues de la dernière version d'Astra Trident.



Le `tridentctl` fichier binaire pour Linux fourni dans le fichier zip du programme d'installation est la version testée et prise en charge. Notez que le `macos` fichier binaire fourni dans la `/extras` partie du fichier zip n'est pas testé ou pris en charge.

## Nouveautés de la version 24.06

### Améliorations

- **IMPORTANT** : le `limitVolumeSize` paramètre limite désormais la taille qtree/LUN dans les pilotes économiques ONTAP. Utilisez le nouveau `limitVolumePoolSize` paramètre pour contrôler les tailles de FlexVol dans ces pilotes. (["Question no 341"](#)).
- Ajout de la fonctionnalité d'auto-rétablissement iSCSI pour lancer des analyses SCSI par ID de LUN exact si des igroups obsolètes sont en cours d'utilisation (["Question no 883"](#)).
- Prise en charge supplémentaire des opérations de clonage de volume et de redimensionnement même lorsque le back-end est en mode suspendu.
- Ajout de la possibilité de propager les paramètres de journaux configurés par l'utilisateur au contrôleur Trident aux pods de nœuds Astra Trident.
- Ajout de la prise en charge dans Astra Trident pour utiliser REST par défaut au lieu de ZAPI pour ONTAP versions 9.15.1 et ultérieures.
- Prise en charge des noms de volumes et des métadonnées personnalisés sur les systèmes back-end de stockage ONTAP pour les nouveaux volumes persistants.
- Amélioration du `azure-netapp-files` pilote (ANF) pour activer automatiquement le répertoire de snapshots par défaut lorsque les options de montage NFS sont définies pour utiliser la version 4.x.
- Ajout de la prise en charge de BottlerRocket pour les volumes NFS.
- Ajout de la prise en charge des aperçus techniques de Google Cloud NetApp volumes.

### Kubernetes

- Prise en charge de Kubernetes 1.30.
- Ajout de la capacité d'Astra Trident DemonSet à nettoyer les montages zombies et les fichiers de suivi résiduels au démarrage (["Question no 883"](#)).
- Ajout d'une annotation PVC `trident.netapp.io/luksEncryption` pour l'importation dynamique de volumes LUKS (["Question no 849"](#)).
- Prise en compte de la topologie du pilote ANF.
- Ajout de la prise en charge des nœuds Windows Server 2022.

## Correctifs

- Correction des défaillances d'installation d'Astra Trident suite à des transactions obsolètes.
- Correction de tridentctl pour ignorer les messages d'avertissement de Kubernetes (["Question no 892"](#)).
- Priorité du contrôleur Astra Trident modifiée SecurityContextConstraint en 0 (["Question no 887"](#)).
- Les pilotes ONTAP acceptent désormais des volumes inférieurs à 20 Mio (["Problème\[#885\]"](#)).
- Correction d'Astra Trident pour empêcher la diminution des volumes FlexVol lors des opérations de redimensionnement pour le pilote ONTAP-SAN.
- Correction de la défaillance d'importation du volume ANF avec NFS v4.1.

## Dé rá tions

- Suppression de la prise en charge de EOL Windows Server 2019.

## Changements en 24.02

### Améliorations

- Prise en charge supplémentaire de Cloud Identity.
  - AKS avec ANF : Azure Workload Identity sera utilisé comme identité cloud.
  - EKS avec FSxN : le rôle IAM AWS sera utilisé comme identité cloud.
- Ajout de la prise en charge de l'installation d'Astra Trident en tant que module complémentaire sur le cluster EKS depuis la console EKS.
- Ajout de la possibilité de configurer et de désactiver l'auto-rétablissement iSCSI (["Question no 864"](#)).
- Ajout de la personnalité FSX aux pilotes ONTAP pour permettre l'intégration avec AWS IAM et SecretsManager et pour permettre à Astra Trident de supprimer des volumes FSX avec des sauvegardes (["Question no 453"](#)).

## Kubernetes

- Prise en charge de Kubernetes 1.29.

## Correctifs

- Correction des messages d'avertissement ACP lorsque ACP n'est pas activé (["Question no 866"](#)).
- Ajout d'un délai de 10 secondes avant d'effectuer une répartition des clones lors de la suppression d'un snapshot pour les pilotes ONTAP, lorsqu'un clone est associé au snapshot.

## Dé rá tions

- Suppression de l'infrastructure d'attepastes in-to des manifestes d'images multi-plates-formes.

## Changements en 23.10

### Correctifs

- Extension de volume fixe si la nouvelle taille demandée est inférieure à la taille totale du volume pour les pilotes de stockage ONTAP-nas et ONTAP-nas-FlexGroup (["Question no 834"](#)).

- Taille de volume fixe pour afficher uniquement la taille utilisable du volume pendant l'importation pour les pilotes de stockage ONTAP-nas et ONTAP-nas-FlexGroup ("[Question no 722](#)").
- Conversion de noms FlexVol fixes pour ONTAP-NAS-Economy.
- Correction du problème d'initialisation d'Astra Trident sur un nœud Windows lors du redémarrage du nœud.

## Améliorations

### Kubernetes

Prise en charge de Kubernetes 1.28.

### Astra Trident

- Ajout de la prise en charge de l'utilisation d'ami (Azure Managed identités) avec le pilote de stockage Azure-netapp-Files.
- Ajout de la prise en charge de NVMe over TCP pour le pilote ONTAP-SAN
- Ajout de la possibilité de mettre en pause le provisionnement d'un volume lorsque le back-end est défini à l'état suspendu par l'utilisateur ("[Question no 558](#)").

## Fonctionnalités avancées disponibles dans Astra Control

Avec Astra Trident 23.10, un nouveau composant logiciel appelé Astra Control Provisioner est disponible pour les utilisateurs d'Astra Control sous licence. Ce mécanisme de provisionnement permet d'accéder à un ensemble de fonctionnalités avancées de gestion et de provisionnement du stockage qui vont au-delà de celles qu'Astra Trident prend en charge par elle-même. Pour la version 23.10, ces fonctionnalités comprennent :

- Fonctionnalités de sauvegarde et de restauration pour les applications avec des systèmes back-end de stockage ontap-nas économiques basés sur des pilotes
- Sécurité améliorée du back-end de stockage avec le chiffrement Kerberos 5
- Restauration des données à l'aide d'un snapshot
- Améliorations de SnapMirror

["En savoir plus sur Astra Control Provisioner."](#)

## Changements en 23.07.1

**Kubernetes:** Suppression fixe du démonset pour prendre en charge les mises à niveau sans temps d'arrêt ("[Question no 740](#)").

## Changements en 23.07

### Correctifs

### Kubernetes

- Correction de la mise à niveau Trident pour ignorer les anciens modules bloqués en état de fin ("[Question no 740](#)").
- Ajout d'une tolérance à la définition de "transitoire-Trident-version-pod" ("[Question no 795](#)").

## Astra Trident

- Correction des demandes ZAPI ONTAP pour s'assurer que les numéros de série des LUN sont interrogés lors de l'obtention des attributs de LUN pour identifier et corriger les périphériques iSCSI fantômes pendant les opérations de standardisation des nœuds.
- Correction de la gestion des erreurs dans le code du pilote de stockage (["Question no 816"](#)).
- Redimensionnement des quotas fixes lors de l'utilisation de pilotes ONTAP avec use-REST=true.
- Création de clones LUN fixes dans ontap-san-Economy.
- Rétablir le champ d'informations de publication de `rawDevicePath` à `devicePath`; logique ajoutée pour remplir et récupérer (dans certains cas) `devicePath` le champ.

## Améliorations

### Kubernetes

- Prise en charge supplémentaire de l'importation de snapshots prévisionnés.
- Déploiement réduit et autorisations linux diaboloconfigurées (["Question no 817"](#)).

### Astra Trident

- Ne rapporte plus le champ d'état pour les volumes et les snapshots « en ligne ».
- Met à jour l'état du back-end si le back-end ONTAP est hors ligne (["Questions #801", "#543"](#)).
- Le numéro de série de la LUN est toujours récupéré et publié au cours du workflow `ControllerVolumePublish`.
- Ajout d'une logique supplémentaire pour vérifier le numéro de série et la taille du périphérique iSCSI à chemins d'accès multiples.
- Vérification supplémentaire des volumes iSCSI pour s'assurer que le périphérique multiacheminement correct n'est pas mis en place.

## Amélioration expérimentale

Ajout de la prise en charge de la présentation technique de NVMe over TCP pour le pilote ONTAP-SAN.

## Documentation

De nombreuses améliorations de l'organisation et du formatage ont été apportées.

## Dérations

### Kubernetes

- Suppression de la prise en charge des snapshots v1beta1.
- Suppression de la prise en charge des volumes et des classes de stockage pré-CSl.
- Mise à jour de la version 1.22 de Kubernetes minimale prise en charge.

## Changements en 23.04



Forcer le détachement de volume pour les volumes ONTAP-SAN-\* est uniquement pris en charge avec les versions Kubernetes avec le volet fonctionnalité de fermeture de nœud non gracieuse activé. Forcer le détachement doit être activé au moment de l'installation à l'aide de --enable-force-detach l'indicateur Trident installer.

## Correctifs

- Correction de l'opérateur Trident pour utiliser IPv6 localhost pour l'installation lorsqu'il est spécifié dans spec.
- Les autorisations de rôle de cluster opérateur Trident fixes doivent être synchronisées avec les autorisations de bundle (["Question no 799"](#)).
- Résolution du problème de connexion d'un volume de bloc brut sur plusieurs nœuds en mode RWX.
- Prise en charge du clonage FlexGroup fixe et importation de volumes pour les volumes SMB.
- Résolution du problème où le contrôleur Trident n'a pas pu s'arrêter immédiatement (["Question no 811"](#)).
- Correctif ajouté pour afficher la liste de tous les noms de groupes initiateur associés à une LUN spécifiée provisionnée avec des pilotes ontap-san-\*.
- Ajout d'un correctif pour permettre l'exécution des processus externes.
- Erreur de compilation corrigée pour l'architecture s390 (["Question no 537"](#)).
- Correction d'un niveau de journalisation incorrect pendant les opérations de montage de volume (["Question no 781"](#)).
- Correction de l'erreur d'assertion de type de potentiel (["Question no 802"](#)).

## Améliorations

- Kubernetes :
  - Prise en charge de Kubernetes 1.27.
  - Ajout de la prise en charge de l'importation de volumes LUKS.
  - Ajout de la prise en charge du mode d'accès PVC ReadWriteOncePod.
  - Ajout de la prise en charge du détachement forcé pour les volumes ONTAP-SAN-\* lors des scénarios d'arrêt de nœud non gracieuse.
  - Tous les volumes ONTAP-SAN-\* utiliseront désormais les groupes initiateurs par nœud. Les LUN ne seront mappées qu'aux igroups dont la publication est active sur ces nœuds afin d'améliorer notre niveau de sécurité. Les volumes existants seront basculés de manière opportuniste vers le nouveau schéma d'igroup lorsque Trident détermine qu'il est possible de le faire sans incidence sur les charges de travail actives (["Question no 758"](#)).
  - Amélioration de la sécurité de Trident en nettoyant les groupes initiateurs gérés par Trident non utilisés à partir de systèmes back-end ONTAP-SAN-\*.
- Ajout de la prise en charge des volumes SMB avec Amazon FSX aux pilotes de stockage ontap-nas-Economy et ontap-nas-flexgroup.
- Ajout de la prise en charge des partages SMB avec les pilotes de stockage ontap-nas, ontap-nas-Economy et ontap-nas-flexgroup.
- Ajout de la prise en charge des nœuds arm64 (["Question no 732"](#)).
- Amélioration de la procédure d'arrêt de Trident en désactivant d'abord les serveurs API (["Question no 811"](#)).

- Ajout de la prise en charge de la construction multi plate-forme pour les hôtes Windows et arm64 à Makefile ; voir BUILD.md.

## Dé rá tions

**Kubernetes:** les igroups Backend-scoped ne seront plus cr é es lors de la configuration des pilotes ONTAP-san et ONTAP-san-Economy (["Question no 758"](#)).

## Changements en 23.01.1

### Correctifs

- Correction de l'op é rateur Trident pour utiliser IPv6 localhost pour l'installation lorsqu'il est sp é cifi é dans spec.
- Les autorisations de r ô le de cluster op é rateur Trident fixes doivent é tre synchronisées avec les autorisations de bundle ["Question no 799"](#).
- Ajout d'un correctif pour permettre l'exécution des processus externes.
- R é solution du probl è me de connexion d'un volume de bloc brut sur plusieurs n o euds en mode RWX.
- Prise en charge du clonage FlexGroup fixe et importation de volumes pour les volumes SMB.

## Changements en 23.01



Kubernetes 1.27 est d é sormais pris en charge dans Trident. Veuillez mettre à niveau Astra Trident avant de mettre à niveau Kubernetes.

### Correctifs

- Kubernetes : ajout d'options pour exclure la cr é ation d'une strat é gie de s é curit é Pod afin de corriger les installations Trident via Helm (["Questions #783, #794"](#)).

### Améliorations

#### Kubernetes

- Prise en charge ajoutée de Kubernetes 1.26.
- Amélioration de l'utilisation globale des ressources Trident RBAC (["Question no 757"](#)).
- Automatisation ajoutée pour d é tecter et corriger les sessions iSCSI interrompues ou obsol è tes sur les n o euds hô tes.
- Ajout de la prise en charge de l'extension des volumes chiffrés LUKS.
- Kubernetes : ajout de la prise en charge de la rotation des identifiants pour les volumes chiffrés LUKS.

#### Astra Trident

- Ajout de la prise en charge des volumes SMB avec Amazon FSX pour ONTAP au pilote de stockage ontap-nas.
- Ajout de la prise en charge des autorisations NTFS lors de l'utilisation de volumes SMB.
- Ajout de la prise en charge des pools de stockage pour les volumes GCP avec le niveau de service CVS.
- Ajout de la prise en charge de l'utilisation facultative de flexgroupAggregateList lors de la cr é ation de FlexGroups avec le pilote de stockage ontap-nas-flexgroup.

- Amélioration des performances du pilote de stockage économique ontap-nas lors de la gestion de plusieurs volumes FlexVol.
- Mises à jour des donnéesLIF activées pour tous les pilotes de stockage NAS de ONTAP.
- Mise à jour de la convention de nommage Trident Deployment and DemonSet afin de refléter le système d'exploitation du nœud hôte.

## Dé rá tions

- Kubernetes : mise à jour de Kubernetes minimale prise en charge vers la version 1.21.
- Les LIF de données ne doivent plus être spécifiées lors de la configuration des ontap-san pilotes ou ontap-san-economy.

## Changements en 22.10

**Vous devez lire les informations essentielles suivantes avant de passer à Astra Trident 22.10.**

**<strong>, la protection des données essentielles d'Astra Trident 22.10</strong>**

- Kubernetes 1.25 est désormais pris en charge par Trident. Vous devez mettre à niveau Astra Trident vers 22.10 avant de procéder à la mise à niveau vers Kubernetes 1.25.
- ASTRA Trident applique désormais strictement l'utilisation de la configuration de chemins d'accès multiples dans les environnements SAN, avec la valeur recommandée de `find_multipaths: no` dans le fichier multipathing.conf.

 L'utilisation d'une configuration sans chemins d'accès multiples ou l'utilisation d'`find_multipaths: yes` une valeur ou `find_multipaths: smart` dans un fichier multipath.conf entraînera des échecs de montage. Trident recommande l'utilisation de `find_multipaths: no` depuis la version 21.07.

## Correctifs

- Correction du problème spécifique au backend ONTAP créé à l'aide du `credentials` champ ne pouvant pas être mis en ligne pendant la mise à niveau 22.07.0 ("[Question no 759](#)").
- **Docker:** correction d'un problème provoquant l'échec du démarrage du plug-in de volume Docker dans certains environnements ("[Question no 548](#)" et "[Question no 760](#)").
- Résolution du problème SLM spécifique aux systèmes back-end ONTAP pour garantir que seul un sous-ensemble de LIF de données appartenant aux nœuds de reporting est publié.
- Problème de performances résolu lors de la connexion d'un volume à des analyses inutiles des LUN iSCSI.
- Supprimez les tentatives granulaires dans le workflow iSCSI Astra Trident pour connaître un risque d'échec rapide et réduire les intervalles de tentatives externes.
- Résolution du problème lorsqu'une erreur a été renvoyée lors du vidage d'un périphérique iSCSI lorsque le périphérique multivoie correspondant a déjà été rincé.

## Améliorations

- Kubernetes :
  - Prise en charge ajoutée de Kubernetes 1.25. Vous devez mettre à niveau Astra Trident vers 22.10 avant de procéder à la mise à niveau vers Kubernetes 1.25.

- Ajout d'un ServiceAccount, ClusterRole et ClusterRoleBinding distincts pour Trident Deployment et DemonSet afin de permettre des améliorations futures des autorisations.
- Prise en charge de "[partage de volume entre espaces de noms](#)".
- Tous les pilotes de stockage Trident `ontap-*` fonctionnent désormais avec l'API REST ONTAP.
- Ajout d'(bundle\_post\_1\_25.yaml`un nouvel opérateur yaml ) sans a `PodSecurityPolicy pour prendre en charge Kubernetes 1.25.
- Ajouté "[Prise en charge des volumes LUKS-chiffrés](#)" pour `ontap-san` les pilotes de stockage et `ontap-san-economy`.
- Ajout de la prise en charge des nœuds Windows Server 2019.
- Ajouté "[Prise en charge des volumes SMB sur les nœuds Windows](#)" via le `azure-netapp-files` pilote de stockage.
- La détection automatique du basculement MetroCluster pour les pilotes ONTAP est désormais disponible dans l'ensemble.

## Dé rá tions

- **Kubernetes:** mise à jour du nombre minimum de Kubernetes pris en charge vers 1.20.
- Suppression du pilote ADS (Data Store).
- Suppression de la prise en charge yes des options `find_multipaths` et `smart` lors de la configuration du multipathing du nœud worker pour iSCSI.

## Changements en 22.07

### Correctifs

#### Kubernetes

- Problème résolu pour gérer les valeurs booléennes et nombres pour le sélecteur de nœud lors de la configuration de Trident avec Helm ou l'opérateur Trident. ("[Problème GitHub n° 700](#)")
- Résolution du problème lors de la gestion des erreurs provenant d'un chemin non CHAP, de sorte que kubelet réessaie en cas d'échec. ("[Problème GitHub n° 736](#)")

### Améliorations

- Passer de `k8s.gcr.io` au `registry.k8s.io` comme registre par défaut pour les images CSI
- Les volumes ONTAP-SAN utiliseront désormais des igroups par nœud et ne mapperont les LUN aux groupes initiateurs, tout en les ayant été publiés activement à ces nœuds pour améliorer notre sécurité. Les volumes existants sont basculés de manière opportuniste vers le nouveau modèle d'igroup lorsque Astra Trident détermine qu'il est possible de le faire en toute sécurité sans incidence sur les workloads actifs.
- Inclus un quota de `ResourceQuota` avec les installations Trident pour s'assurer que Trident DemonSet est planifié lorsque la consommation `PriorityClass` est limitée par défaut.
- Ajout de la prise en charge des fonctions réseau au pilote Azure NetApp Files. ("[Problème GitHub n° 717](#)")
- Ajout de la détection automatique du basculement MetroCluster dans l'aperçu technique aux pilotes ONTAP. ("[Problème GitHub n° 228](#)")

## Déclarations

- **Kubernetes:** mise à jour du nombre minimum de Kubernetes pris en charge vers 1.19.
- La configuration backend n'autorise plus plusieurs types d'authentification dans la configuration unique.

## Suppressions

- Le pilote CVS AWS (obsolète depuis 22.04) a été supprimé.
- Kubernetes
  - Suppression des capacités SYS\_ADMIN inutiles des modules de nœud.
  - Réduit la préparation des nœuds afin de simplifier les informations sur l'hôte et la détection des services actifs pour obtenir la confirmation de la disponibilité des services NFS/iSCSI sur les nœuds workers.

## Documentation

Une nouvelle "["Normes de sécurité du pod"](#)" section (PSS) a été ajoutée, détaillant les autorisations activées par Astra Trident lors de l'installation.

## Changements en 22.04

NetApp améliore et améliore continuellement ses produits et services. Voici quelques-unes des nouveautés d'Astra Trident. Pour les versions précédentes, reportez-vous à "["Versions antérieures de la documentation"](#)".



Si vous effectuez une mise à niveau à partir d'une version précédente de Trident et que vous utilisez Azure NetApp Files, le `location` paramètre config est désormais un champ obligatoire, singleton.

## Correctifs

- Amélioration de l'analyse des noms d'initiateurs iSCSI. (["Problème GitHub n° 681"](#))
- Problème résolu lorsque les paramètres de classe de stockage CSI n'étaient pas autorisés. (["Problème GitHub n° 598"](#))
- Déclaration de clé en double fixe dans Trident CRD. (["Problème GitHub n° 671"](#))
- Correction des journaux CSI instantanés erronés. (["Problème GitHub n° 629"](#))
- Résolution du problème lié à l'annulation de la publication des volumes sur les nœuds supprimés. (["Problème GitHub n° 691"](#))
- Ajout de la gestion des incohérences du système de fichiers sur les périphériques en bloc. (["Problème GitHub n° 656"](#))
- Résolution du problème d'extraction des images de support automatique lors de la définition de `imageRegistry` l'indicateur pendant l'installation. (["Problème GitHub n° 715"](#))
- Résolution du problème d'échec du clonage d'un volume avec plusieurs règles d'exportation par le pilote Azure NetApp Files.

## Améliorations

- Les connexions entrantes aux terminaux sécurisés de Trident requièrent désormais un minimum de TLS 1.3. (["Problème GitHub n° 698"](#))

- Trident ajoute désormais des en-têtes HSTS aux réponses à partir de ses terminaux sécurisés.
- Trident tente désormais d'activer automatiquement la fonctionnalité d'autorisations unix Azure NetApp Files.
- **Kubernetes:** Trident demonset s'exécute maintenant dans la classe de priorité critique du nœud système. ("[Problème GitHub n° 694](#)")

## Suppressions

Le pilote E-Series (désactivé depuis 20.07) a été supprimé.

## Changements en 22.01.1

### Correctifs

- Résolution du problème lié à l'annulation de la publication des volumes sur les nœuds supprimés. ("[Problème GitHub n° 691](#)")
- Panique fixe lors de l'accès aux champs nuls pour l'espace global dans les réponses de l'API ONTAP.

## Changements en 22.01.0

### Correctifs

- **Kubernetes:** augmentez le temps de rétentative de rétro-enregistrement des nœuds pour les grands clusters.
- Problème résolu dans lequel le pilote Azure-netapp-Files pourrait être confondu avec plusieurs ressources avec le même nom.
- Les LIF de données sur IPv6 SAN de ONTAP fonctionnent désormais si elles sont spécifiées avec des parenthèses.
- Problème résolu lors de la tentative d'importation d'un volume déjà importé renvoie EOF laissant le PVC à l'état en attente. ("[Problème GitHub n° 489](#)")
- Problème résolu lorsque la performance d'Astra Trident ralentit lorsque plus de 32 snapshots sont créés sur un volume SolidFire.
- SHA-1 remplacé par SHA-256 lors de la création du certificat SSL.
- Correction du pilote Azure NetApp Files pour permettre la duplication des noms de ressources et limiter les opérations à un seul emplacement.
- Correction du pilote Azure NetApp Files pour permettre la duplication des noms de ressources et limiter les opérations à un seul emplacement.

## Améliorations

- Améliorations de Kubernetes :
  - Prise en charge ajoutée de Kubernetes 1.23.
  - Ajoutez des options de planification pour les pods Trident lorsqu'ils sont installés via l'opérateur Trident ou Helm. ("[Problème GitHub n° 651](#)")
- Autorisation des volumes inter-régions dans le pilote GCP ("[Problème GitHub n° 633](#)")
- Ajout de la prise en charge de l'option 'unixPermissionss' aux volumes Azure NetApp Files. ("[Problème GitHub n° 666](#)")

## Déclarations

L'interface REST de Trident peut écouter et servir uniquement aux adresses 127.0.0.1 ou [::1]

## Changements en 21.10.1



La version v21.10.0 présente un problème qui peut placer le contrôleur Trident dans un état CrashLoopBackOff lorsqu'un nœud est supprimé, puis réintégré au cluster Kubernetes. Ce problème a été résolu dans la version 1.210.1 (édition GitHub 669).

## Correctifs

- Condition de race potentielle fixe lors de l'importation d'un volume sur un back-end Cloud CVS GCP, entraînant l'échec de l'importation.
- Résolution d'un problème de mise en service du contrôleur Trident dans un état CrashLoopBackOff lorsqu'un nœud est retiré, puis réintégré au cluster Kubernetes (problème GitHub 669).
- Problème résolu : les SVM n'ont plus été découverts si aucun nom de SVM n'a été spécifié (problème GitHub 612).

## Changements en 21.10.0

## Correctifs

- Problème résolu : les clones de volumes XFS n'ont pas pu être montés sur le même nœud que le volume source (problème GitHub 514).
- Résolution du problème pendant lequel Astra Trident a enregistré une erreur fatale lors de l'arrêt (problème GitHub 597).
- Correctifs liés à Kubernetes :
  - Renvoie l'espace utilisé d'un volume comme taille de restauration minimale lors de la création de snapshots avec des `ontap-nas` pilotes et `ontap-nas-flexgroup` (problème GitHub 645).
  - Résolution du problème d' `Failed to expand filesystem` enregistrement de l'erreur après le redimensionnement du volume (problème GitHub 560).
  - Résolution du problème de blocage d'un pod à `Terminating` l'état (problème GitHub 572).
  - Résolution du problème : un `ontap-san-economy` FlexVol peut être saturé de LUN de snapshot (problème GitHub 533).
  - Résolution du problème d'installation YAML personnalisé avec une image différente (problème GitHub 613).
  - Calcul de la taille de snapshot fixe (problème GitHub 611).
  - Problème résolu : tous les installateurs Trident d'Astra pouvaient identifier Kubernetes ordinaire comme OpenShift (problème GitHub 639).
  - A corrigé l'opérateur Trident pour arrêter la réconciliation si le serveur d'API Kubernetes est inaccessible (problème GitHub 599).

## Améliorations

- Ajout de la prise en charge des options pour `unixPermissions` les volumes de performance GCP-CVS.
- Ajout de la prise en charge des volumes CVS optimisés pour l'évolutivité dans GCP dans la plage de 600

Gio à 1 Tio.

- Améliorations liées à Kubernetes :

- Prise en charge ajoutée de Kubernetes 1.22.
- Compatibilité de l'opérateur Trident et du tableau Helm avec Kubernetes 1.22 (problème GitHub 628).
- Ajout de l'image de l'opérateur à la `tridentctl` commande `images` (GitHub problème 570).

## Améliorations expérimentales

- Ajout de la prise en charge de la réPLICATION de volume dans le `ontap-san` pilote.
- Ajout de la prise en charge REST de **TECH Preview** pour les `ontap-nas-flexgroup` pilotes , `ontap-san` et `ontap-nas-economy` .

## Problèmes connus

Les problèmes connus identifient les problèmes susceptibles de vous empêcher d'utiliser le produit avec succès.

- Lors de la mise à niveau d'un cluster Kubernetes de la version 1.24 vers la version 1.25 ou ultérieure sur lequel Astra Trident est installé, vous devez mettre à jour `Values.yaml` pour définir `excludePodSecurityPolicy` sur `true` ou ajouter la `--set excludePodSecurityPolicy=true` `helm upgrade` commande avant de pouvoir mettre à niveau le cluster.
- ASTRA Trident applique désormais un espace vide `fsType` (`fsType=""`) pour les volumes qui n'ont pas `fsType` spécifié dans leur classe de stockage. Avec Kubernetes 1.17 ou version ultérieure, Trident prend en charge la fourniture d'un espace vide `fsType` pour les volumes NFS. Pour les volumes iSCSI, vous devez définir le `fsType` sur votre classe de stockage lors de l'application d'un à l'aide d'un `fsGroup` contexte de sécurité.
- Lors de l'utilisation d'un système back-end sur plusieurs instances Astra Trident, chaque fichier de configuration back-end doit avoir `storagePrefix` une valeur différente pour les systèmes ONTAP back-end ou utiliser un système back-end différent `TenantName` pour les systèmes SolidFire back-end. Astra Trident ne peut pas détecter les volumes que d'autres instances d'Astra Trident ont créés. Tentative de création d'un volume existant sur un système back-end ONTAP ou SolidFire réussie, Astra Trident traite la création de volume comme une opération identique. Si `storagePrefix` ou `TenantName` ne diffèrent pas, il peut y avoir des collisions de nom pour les volumes créés sur le même backend.
- Lors de l'installation d'Astra Trident (à l'aide de `tridentctl` ou de l'opérateur Trident) et de l'utilisation de `tridentctl` pour gérer Astra Trident, vous devez vous assurer que la `KUBECONFIG` variable d'environnement est définie. Ceci est nécessaire pour indiquer le cluster Kubernetes sur lequel `tridentctl` doit fonctionner. Lorsque vous travaillez avec plusieurs environnements Kubernetes, vous devez vous assurer que le `KUBECONFIG` fichier provient correctement.
- Pour réclamer de l'espace en ligne pour des volumes persistants iSCSI, le système d'exploitation sous-jacent du nœud worker peut nécessiter le passage des options de montage vers le volume. Ceci est vrai pour les instances RHEL/RedHat CoreOS, qui nécessitent le [option de montage](#); assurez-vous que la mise au rebut de `mountOption` est incluse dans votre `[StorageClass^]` pour prendre en charge la suppression de bloc en ligne.
- Si vous possédez plusieurs instances d'Astra Trident par cluster Kubernetes, Astra Trident ne peut pas communiquer avec d'autres instances et ne peut pas détecter les autres volumes qu'ils ont créés, ce qui entraîne un comportement inattendu et incorrect si plusieurs instances s'exécutent dans un cluster. Il ne devrait y avoir qu'une seule instance d'Astra Trident par cluster Kubernetes.
- Si des objets basés sur Astra Trident `StorageClass` sont supprimés de Kubernetes alors qu'Astra Trident

est hors ligne, Astra Trident ne supprime pas les classes de stockage correspondantes de sa base de données lorsqu'elle est de nouveau en ligne. Vous devez supprimer ces classes de stockage à l'aide de `tridentctl` ou de l'API REST.

- Si un utilisateur supprime un volume persistant provisionné par Astra Trident avant de supprimer le volume persistant correspondant, Astra Trident ne supprime pas automatiquement le volume de sauvegarde. Vous devez supprimer le volume via `tridentctl` ou l'API REST.
- ONTAP ne peut pas provisionner simultanément plusieurs FlexGroup, sauf si l'ensemble d'agrégats est unique pour chaque demande de provisionnement.
- Lorsque vous utilisez Astra Trident sur IPv6, vous devez spécifier `managementLIF` et `dataLIF` dans la définition du back-end entre crochets. Par exemple `[fd20:8b1e:b258:2000:f816:3eff:feec:0]`, ..



Vous ne pouvez pas spécifier `dataLIF` sur un système SAN backend ONTAP. Astra Trident détecte toutes les LIF iSCSI disponibles et les utilise pour établir la session multivoie.

- Si vous utilisez le `solidfire-san` pilote avec OpenShift 4.5, assurez-vous que les nœuds worker sous-jacents utilisent MD5 comme algorithme d'authentification CHAP. Les algorithmes CHAP sécurisés conformes à la norme FIPS SHA1, SHA-256 et SHA3-256 sont disponibles avec Element 12.7.

## Trouvez plus d'informations

- ["Astra Trident GitHub"](#)
- ["Blogs Trident d'Astra"](#)

## Versions antérieures de la documentation

Si vous n'exécutez pas Astra Trident 24.06, la documentation relative aux versions précédentes est disponible sur la base du ["Cycle de vie de prise en charge d'Astra Trident"](#).

- ["ASTRA Trident 24.02"](#)
- ["ASTRA Trident 23.10"](#)
- ["ASTRA Trident 23.07"](#)
- ["ASTRA Trident 23.04"](#)
- ["ASTRA Trident 23.01"](#)
- ["ASTRA Trident 22.10"](#)
- ["ASTRA Trident 22.07"](#)
- ["ASTRA Trident 22.04"](#)

# Commencez

## Découvrez Astra Trident

### Découvrez Astra Trident

ASTRA Trident est un projet open source entièrement pris en charge et géré par NetApp dans le cadre du "[Gamme de produits Astra](#)". Il a été conçu pour vous aider à répondre aux exigences de persistance de vos applications conteneurisées en utilisant des interfaces standard telles que l'interface CSI (Container Storage interface).

#### Qu'est-ce qu'Astra ?

Astra facilite la gestion, la protection et le déplacement de leurs workloads riches en données qui s'exécutent sur Kubernetes, dans les clouds publics et sur site.

ASTRA provisionne et fournit un stockage persistant de conteneur basé sur Astra Trident. Il offre également des fonctionnalités avancées de gestion des données compatibles avec les applications, telles que les copies Snapshot, la sauvegarde et la restauration, les journaux d'activité et le clonage actif pour la protection des données, la reprise d'activité et les données, l'audit des données et la migration pour les workloads Kubernetes.

En savoir plus sur "[ASTRA ou inscrivez-vous pour un essai gratuit](#)".

#### Qu'est-ce qu'Astra Trident ?

ASTRA Trident permet la consommation et la gestion des ressources de stockage sur toutes les plateformes de stockage NetApp populaires, dans le cloud public ou sur site, y compris ONTAP (AFF, FAS, Select, Cloud, Amazon FSX pour NetApp ONTAP), Element (NetApp HCI, SolidFire), Azure NetApp Files service et Cloud Volumes Service sur Google Cloud.

ASTRA Trident est un orchestrateur de stockage dynamique conforme à CSI (Container Storage interface) qui s'intègre de manière native à "[Kubernetes](#)". ASTRA Trident s'exécute en tant que pod unique de contrôleur et comme pod de nœud sur chaque nœud worker dans le cluster. Voir "[Architecture d'Astra Trident](#)" pour plus de détails.

ASTRA Trident assure également une intégration directe avec l'écosystème Docker pour les plateformes de stockage NetApp. Le plug-in de volume Docker (nDVP) de NetApp prend en charge le provisionnement et la gestion des ressources de stockage depuis la plateforme de stockage jusqu'aux hôtes Docker. Voir "[Déployez Astra Trident pour Docker](#)" pour plus de détails.



Si vous utilisez Kubernetes pour la première fois, familiarisez-vous avec le "[Concepts et outils Kubernetes](#)".

### Testez Astra Trident

Pour tester un disque, demandez l'accès au « déploiement et clonage simplifiés du stockage persistant pour les workloads conteneurisés » "[Test Drive NetApp](#)" à l'aide d'une image de laboratoire prête à l'emploi. Le test Drive fournit un environnement sandbox avec un cluster Kubernetes à trois nœuds et Astra Trident installé et configuré. C'est un excellent moyen de vous familiariser avec Astra Trident et d'explorer ses fonctionnalités.

La solution est également "[Guide d'installation de kubeadm](#)" fournie par Kubernetes.



N'utilisez pas un cluster Kubernetes que vous créez en utilisant ces instructions dans un environnement de production. Utilisez les guides de déploiement de production fournis par votre distributeur pour les clusters prêts à la production.

## Intégration de Kubernetes avec les produits NetApp

Le portefeuille de produits de stockage NetApp s'intègre à de nombreux aspects des clusters Kubernetes avec des fonctionnalités avancées de gestion des données qui améliorent la fonctionnalité, la capacité, les performances et la disponibilité du déploiement Kubernetes.

### Amazon FSX pour NetApp ONTAP

["Amazon FSX pour NetApp ONTAP"](#) Est un service AWS entièrement géré qui vous permet de lancer et d'exécuter des systèmes de fichiers optimisés par le système d'exploitation du stockage NetApp ONTAP.

### Azure NetApp Files

["Azure NetApp Files"](#) Est un service de partage de fichiers Azure haute performance, optimisé par NetApp. Vous pouvez exécuter les workloads basés sur des fichiers les plus exigeants dans Azure de façon native, avec les performances et les fonctionnalités avancées de gestion des données que vous attendez de NetApp.

### Cloud Volumes ONTAP

["Cloud Volumes ONTAP"](#) Est une appliance de stockage exclusivement logicielle qui exécute le logiciel de gestion des données ONTAP dans le cloud.

### Cloud Volumes Service pour Google Cloud

["NetApp Cloud Volumes Service pour Google Cloud"](#) Est un service de fichiers natif du cloud qui fournit des volumes NAS sur NFS et SMB avec des performances 100 % Flash.

### Logiciel Element

["Elément"](#) permet à l'administrateur du stockage de consolider les charges de travail en garantissant la performance et en simplifiant et en rationalisant l'empreinte du stockage.

### NetApp HCI

["NetApp HCI"](#) simplifie la gestion et l'évolutivité du data center en automatisant les tâches de routine et en permettant aux administrateurs d'infrastructure de donner la priorité aux fonctions plus importantes.

ASTRA Trident peut provisionner et gérer des dispositifs de stockage pour des applications conteneurisées directement à partir de la plateforme de stockage NetApp HCI sous-jacente.

## NetApp ONTAP

["NetApp ONTAP"](#) Il s'agit du système d'exploitation de stockage unifié multiprotocole NetApp qui offre des fonctionnalités avancées de gestion des données pour toutes les applications.

Les systèmes ONTAP sont dotés de configurations 100 % Flash, hybrides ou 100 % HDD et proposent différents modèles de déploiement, notamment du matériel spécialisé (FAS et AFF), de l'infrastructure générique (ONTAP Select) et du cloud uniquement (Cloud Volumes ONTAP). ASTRA Trident prend en charge ces modèles de déploiement ONTAP.

### Pour en savoir plus

- ["Gamme NetApp Astra"](#)
- ["Documentation relative au service après-vente Astra Control"](#)
- ["Documentation Astra Control Center"](#)
- ["Documentation de l'API Astra"](#)

## Architecture d'Astra Trident

ASTRA Trident s'exécute en tant que pod unique de contrôleur et comme pod de nœud sur chaque nœud worker dans le cluster. Le pod de nœuds doit être exécuté sur n'importe quel hôte sur lequel vous souhaitez potentiellement monter un volume Astra Trident.

### Présentation des pods de contrôleur et des nœuds

ASTRA Trident se déploie comme une seule [Pod du contrôleur Trident](#) et même entité ou plus [Pods de nœuds Trident](#) dans le cluster Kubernetes et utilise des conteneurs Sidecar Kubernetes standard [CSI](#) pour simplifier le déploiement des plug-ins CSI. ["Conteneurs Sidecar Kubernetes CSI"](#) Sont gérés par la communauté Kubernetes Storage.

Kubernetes ["sélecteurs de nœuds"](#) et ["tolérances et rejets"](#) sont utilisés pour contraindre un pod à s'exécuter sur un nœud spécifique ou préféré. Vous pouvez configurer des sélecteurs de nœuds et des tolérances pour les pods de contrôleur et de nœud lors de l'installation d'Astra Trident.

- Le plug-in du contrôleur gère le provisionnement et la gestion des volumes, tels que les snapshots et le redimensionnement.
- Le plug-in du nœud permet d'attacher le stockage au nœud.

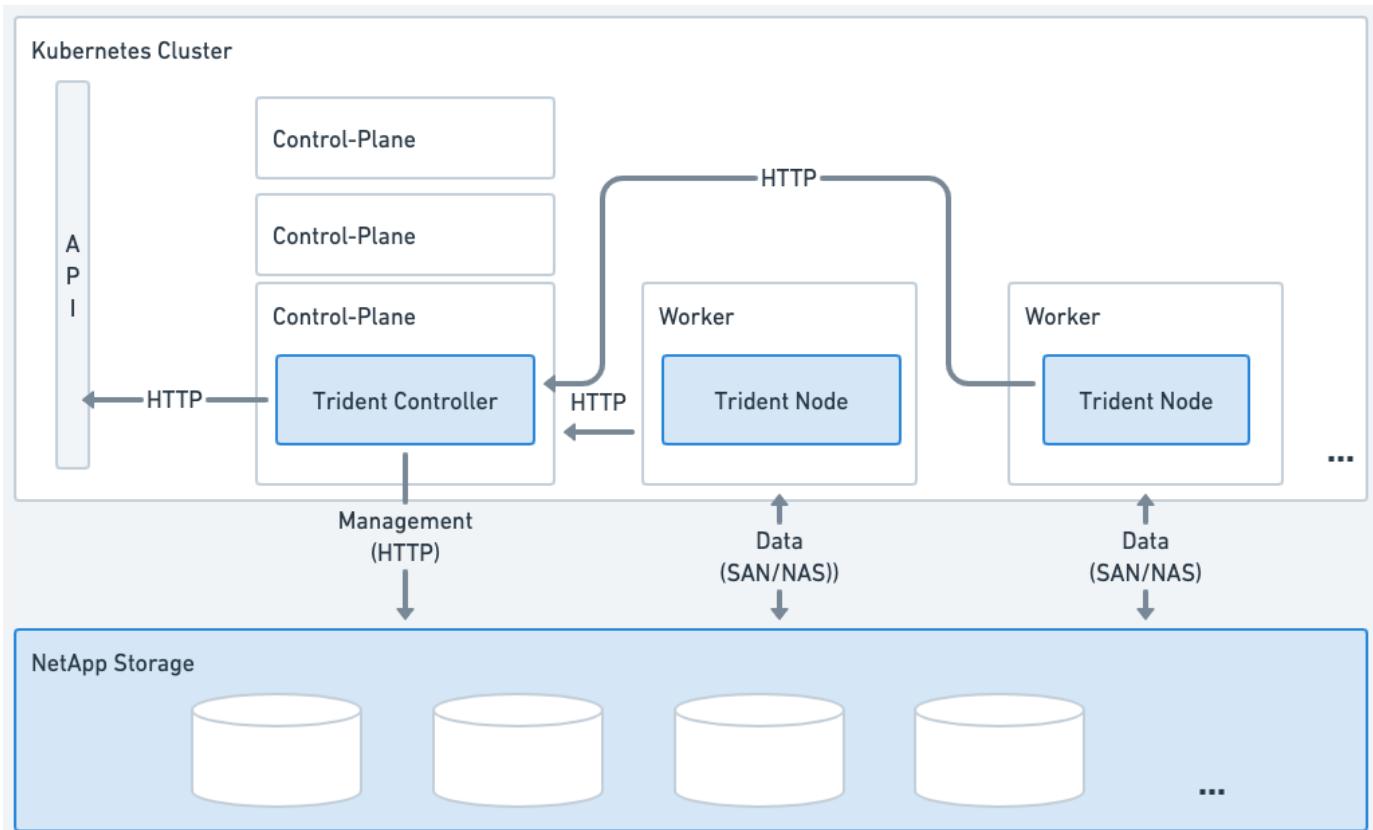


Figure 1. ASTRA Trident a été déployé sur le cluster Kubernetes

#### Pod du contrôleur Trident

Le pod du contrôleur Trident est un pod unique exécutant le plug-in du contrôleur CSI.

- Responsable du provisionnement et de la gestion des volumes dans le stockage NetApp
- Géré par un déploiement Kubernetes
- Peut s'exécuter sur le plan de contrôle ou les nœuds workers, selon les paramètres d'installation.

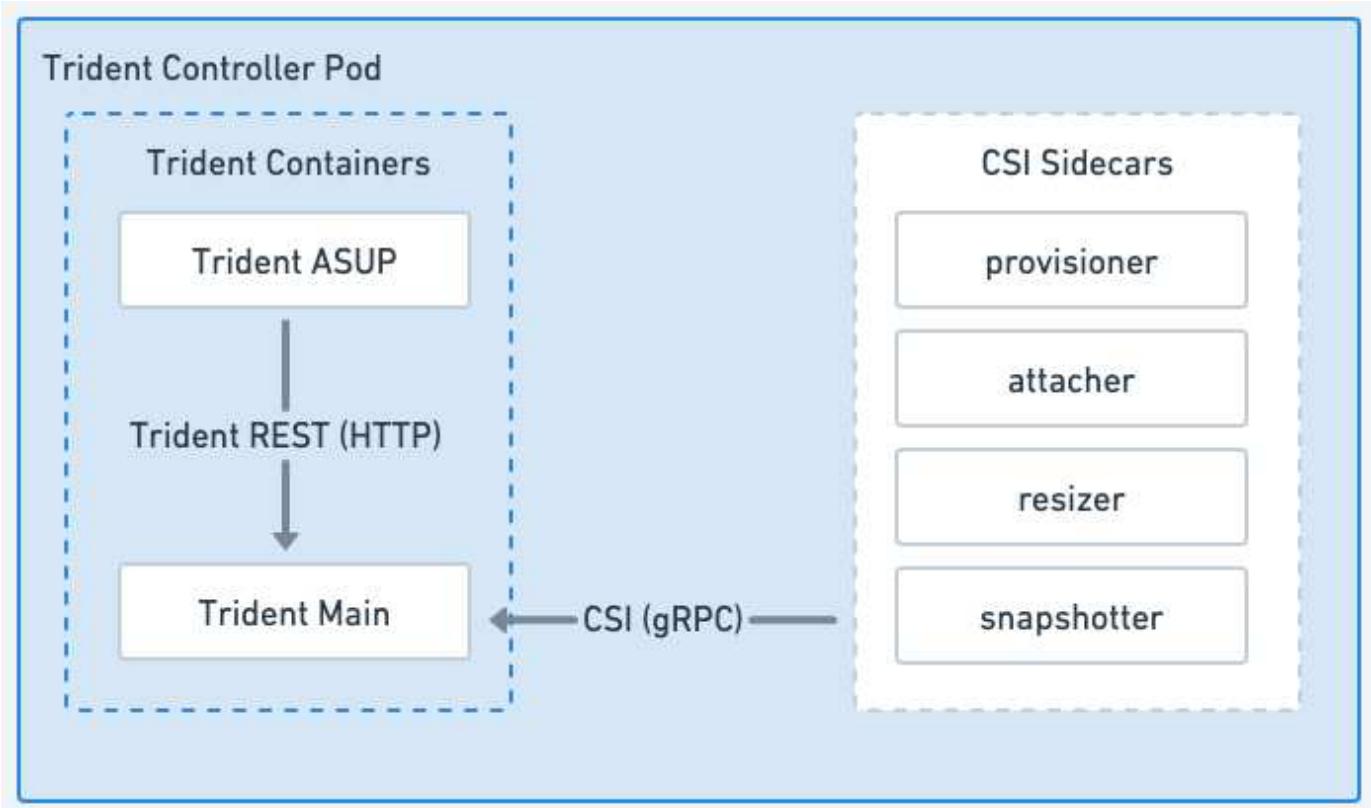


Figure 2. Diagramme du module de contrôleur Trident

#### Pods de nœuds Trident

Les pods de nœud Trident sont des pods privilégiés exécutant le plug-in **CSI Node**.

- Responsable du montage et du démontage du stockage des pods qui s'exécutent sur l'hôte
- Géré par un jeu de démonstration Kubernetes
- Doit s'exécuter sur n'importe quel nœud qui montera le stockage NetApp

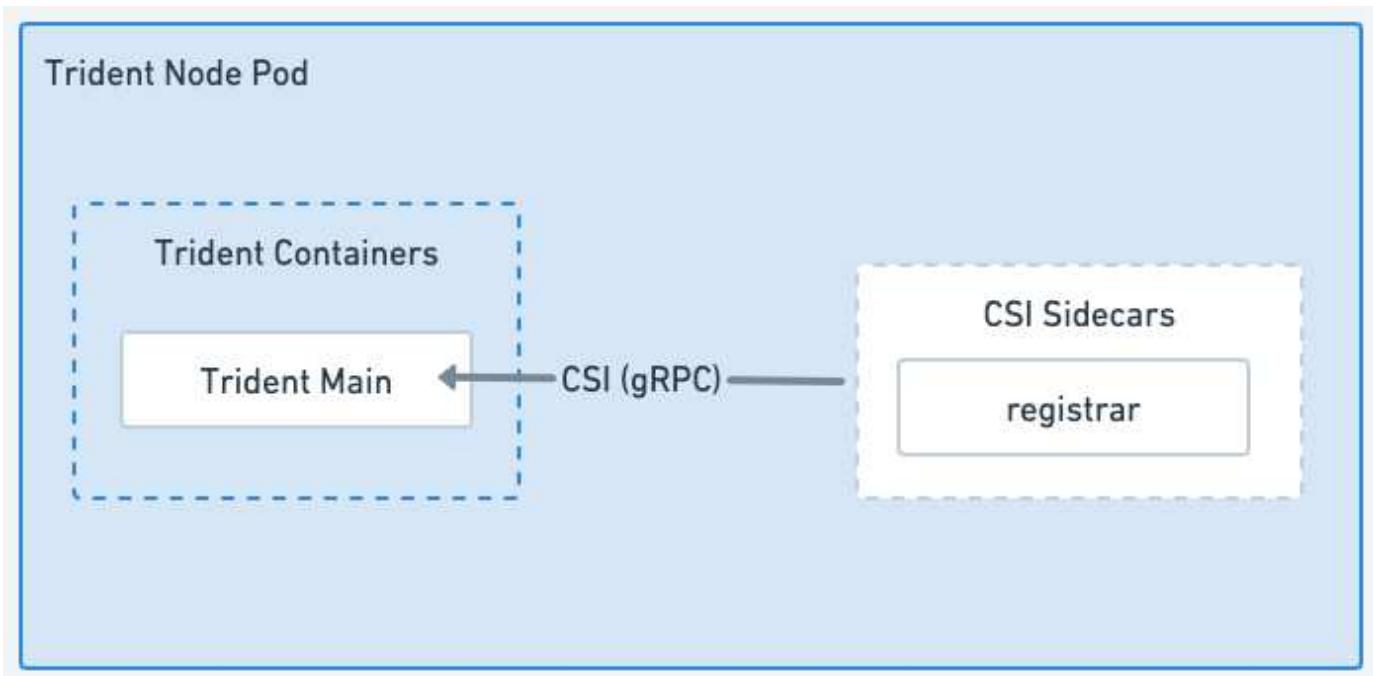


Figure 3. Diagramme Trident Node Pod

### Architectures de cluster Kubernetes prises en charge

Astra Trident est pris en charge avec les architectures Kubernetes suivantes :

Architectures en cluster Kubernetes	Pris en charge	Installation par défaut
Maître unique, calcul	Oui	Oui
Plusieurs maîtres, calcul	Oui	Oui
Maître, etcd, calcul	Oui	Oui
Maîtrise, infrastructure, calcul	Oui	Oui

## Concepts

### Provisionnement

Le provisionnement avec Astra Trident a deux phases principales. La première phase associe une classe de stockage à l'ensemble des pools de stockage back-end appropriés et effectue la préparation nécessaire avant le provisionnement. La deuxième phase inclut la création du volume et nécessite le choix d'un pool de stockage parmi ceux associés à la classe de stockage du volume en attente.

### Association de classe de stockage

L'association de pools de stockage back-end à une classe de stockage dépend à la fois des attributs demandés de la classe de stockage et des `storagePools` , `additionalStoragePools` et `excludeStoragePools` . Lorsque vous créez une classe de stockage, Trident compare les attributs et les

pools proposés par chacun de ses systèmes back-end à ceux requis par la classe de stockage. Si les attributs et le nom d'un pool de stockage correspondent à tous les attributs et noms de pool demandés, Astra Trident ajoute ce pool de stockage à l'ensemble des pools de stockage appropriés pour cette classe de stockage. En outre, Astra Trident ajoute à cet ensemble tous les pools de stockage répertoriés dans `additionalStoragePools` la liste, même si leurs attributs ne remplissent pas la totalité ou l'un des attributs demandés par la classe de stockage. Vous devez utiliser cette `excludeStoragePools` liste pour remplacer et supprimer les pools de stockage qui ne sont pas utilisés pour une classe de stockage. La solution Astra Trident effectue un processus similaire chaque fois que vous ajoutez un nouveau système back-end, en vérifiant si ses pools de stockage correspondent à ceux des classes de stockage existantes et en supprimant ceux qui ont été marqués comme exclus.

## Création du volume

Astra Trident utilise ensuite les associations entre les classes de stockage et les pools de stockage pour déterminer où provisionner les volumes. Lorsque vous créez un volume, Astra Trident commence par obtenir l'ensemble des pools de stockage correspondant à la classe de stockage du volume. De plus, si vous spécifiez un protocole pour le volume, Astra Trident supprime les pools de stockage qui ne peuvent pas fournir le protocole demandé (par exemple, un back-end NetApp HCI/SolidFire ne peut pas fournir un volume basé sur les fichiers, tandis qu'un back-end ONTAP NAS ne peut pas fournir un volume basé sur les blocs). Astra Trident répartit de manière aléatoire l'ordre de ce jeu, afin de faciliter une distribution homogène des volumes, puis l'itérate via lui pour tenter de provisionner le volume sur chaque pool de stockage. S'il réussit sur un, il retourne avec succès, en enregistrant les échecs rencontrés dans le processus. Astra Trident renvoie une défaillance **uniquement si** il ne parvient pas à approvisionner **tous** les pools de stockage disponibles pour la classe et le protocole de stockage demandés.

## Snapshots de volume

Découvrez comment Astra Trident gère la création de copies Snapshot de volume pour ses pilotes.

### En savoir plus sur la création de snapshots de volume

- Pour les `ontap-nas` pilotes, `ontap-san`, `gcp-cvs` et `azure-netapp-files`, chaque volume persistant est mappé sur un FlexVol. Par conséquent, des snapshots de volume sont créés sous forme de snapshots NetApp. La technologie Snapshot de NetApp offre davantage de stabilité, d'évolutivité, de capacité de restauration et de performances que les technologies Snapshot concurrentes. Ces copies Snapshot sont extrêmement efficaces, aussi bien en termes de temps de création que d'espace de stockage.
- Pour le `ontap-nas-flexgroup` pilote, chaque volume persistant est mappé sur un FlexGroup. Par conséquent, des snapshots de volume sont créés sous forme de snapshots NetApp FlexGroup. La technologie Snapshot de NetApp offre davantage de stabilité, d'évolutivité, de capacité de restauration et de performances que les technologies Snapshot concurrentes. Ces copies Snapshot sont extrêmement efficaces, aussi bien en termes de temps de création que d'espace de stockage.
- Pour le `ontap-san-economy` pilote, les volumes persistants sont mappés sur les LUN créées sur les volumes FlexVol partagés. Les copies FlexClone de la LUN associée permettent d'obtenir les copies Snapshot VolumeSnapshot de la LUN associée. Grâce à la technologie FlexClone de ONTAP, il est possible de créer quasi instantanément des copies des jeux de données les plus volumineux, même les plus volumineux. Les copies partagent les blocs de données avec leurs parents. Aucun stockage n'est nécessaire, sauf pour les métadonnées.
- Pour le `solidfire-san` pilote, chaque volume persistant est mappé sur une LUN créée sur le cluster NetApp Element logiciel/NetApp HCI. Les copies Snapshot VolumeCas sont représentées par des copies Snapshot Element de la LUN sous-jacente. Ces snapshots sont des copies à un point dans le temps et ne

prennent en charge qu'une petite quantité de ressources et d'espace système.

- Lorsque vous travaillez avec les `ontap-nas` pilotes et `ontap-san`, les snapshots ONTAP sont des copies instantanées de la FlexVol et consomment de l'espace sur la FlexVol elle-même. Cela peut entraîner la quantité d'espace inscriptible dans le volume pour une réduction du temps lors de la création ou de la planification des snapshots. L'une des façons simples de résoudre ce problème est d'augmenter le volume en le redimensionnant via Kubernetes. Une autre option consiste à supprimer les snapshots qui ne sont plus nécessaires. Lors de la suppression d'un Snapshot VolumeCas créé via Kubernetes, Astra Trident supprime le snapshot ONTAP associé. Les snapshots ONTAP qui n'ont pas été créés par Kubernetes peuvent également être supprimés.

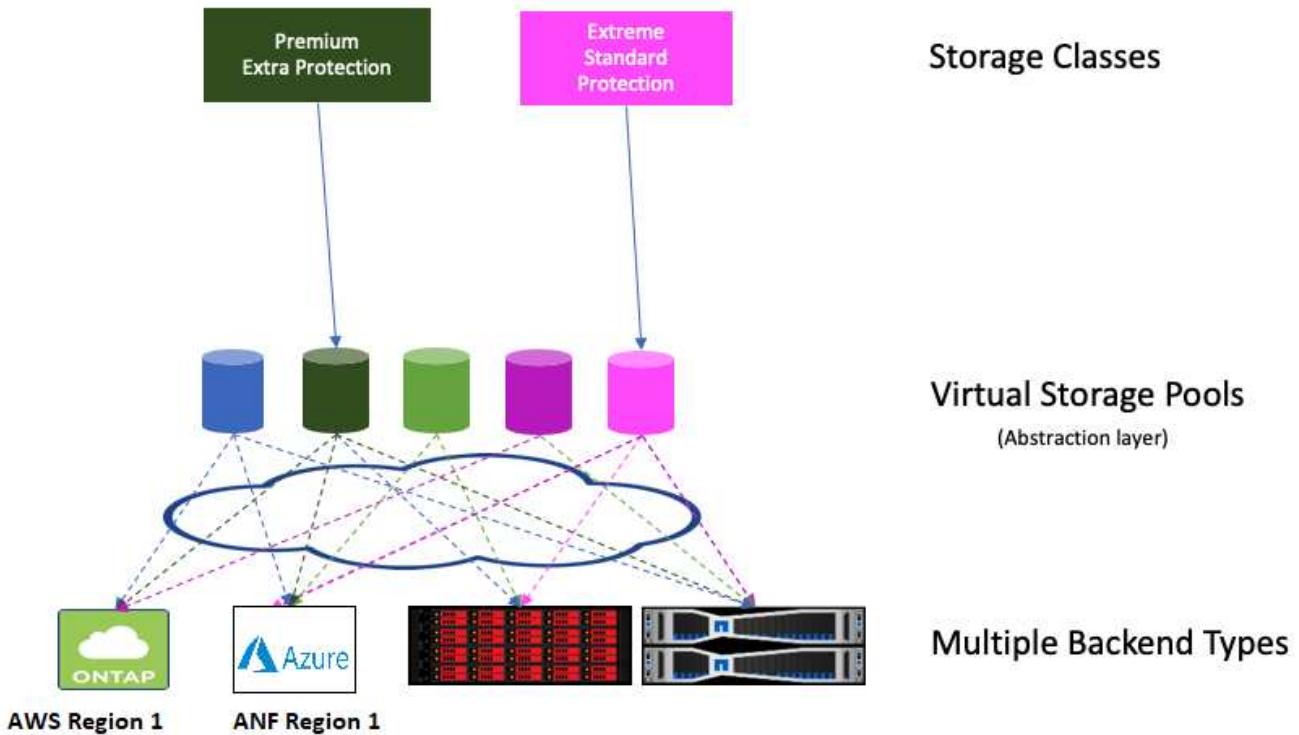
Avec Astra Trident, vous pouvez utiliser Volumesnapshots pour créer de nouveaux volumes persistants à partir d'entre eux. La création de volumes persistants est effectuée à partir de ces copies Snapshot à l'aide de la technologie FlexClone pour les systèmes back-end ONTAP et CVS pris en charge. Lors de la création d'un volume persistant à partir d'un snapshot, le volume de sauvegarde est un volume FlexClone du volume parent du snapshot. Le `solidfire-san` pilote utilise des clones de volume du logiciel Element pour créer des volumes persistants à partir de snapshots. Ici, cela crée un clone à partir du snapshot Element.

## Pools virtuels

Les pools virtuels fournissent une couche d'abstraction entre les systèmes back-end de stockage Astra Trident et Kubernetes StorageClasses. Ils permettent à un administrateur de définir des aspects, tels que l'emplacement, les performances et la protection de chaque back-end de manière commune et indépendante du back-end, sans StorageClass spécifier le backend physique, le pool back-end ou le type de back-end à utiliser pour répondre aux critères souhaités.

### En savoir plus sur les pools virtuels

L'administrateur du stockage peut définir des pools virtuels sur n'importe quel système back-end Trident Astra dans un fichier de définition JSON ou YAML.



Tout aspect spécifié en dehors de la liste des pools virtuels est global au back-end et s'appliquera à tous les pools virtuels, tandis que chaque pool virtuel peut spécifier un ou plusieurs aspects individuellement (remplaçant les aspects backend-global).

- Lors de la définition de pools virtuels, n'essayez pas de réorganiser l'ordre des pools virtuels existants dans une définition backend.
- Nous vous conseillons de modifier les attributs d'un pool virtuel existant. Vous devez définir un nouveau pool virtuel pour apporter des modifications.

La plupart des aspects sont spécifiés dans des termes spécifiques au système back-end. Il est important de noter que les valeurs d'aspect ne sont pas exposées en dehors du pilote du back-end et ne sont pas disponibles pour la correspondance dans. L' `StorageClasses` administrateur définit plutôt un ou plusieurs libellés pour chaque pool virtuel. Chaque étiquette est une paire clé:valeur et les étiquettes sont souvent répandues sur différents systèmes back-end. Tout comme les aspects, les étiquettes peuvent être spécifiées par pool ou globales au back-end. Contrairement aux aspects, qui ont des noms et des valeurs prédéfinis, l'administrateur dispose d'une entière discréption pour définir les clés et les valeurs de libellé selon les besoins. Pour plus de commodité, les administrateurs du stockage peuvent définir des étiquettes par pool virtuel et les volumes de groupe par étiquette.

Un `StorageClass` identifie le pool virtuel à utiliser en référençant les étiquettes dans un paramètre de sélecteur. Les sélecteurs de pool virtuel prennent en charge les opérateurs suivants :

Opérateur	Exemple	La valeur d'étiquette d'un pool doit :
=	<code>performance=premium</code>	Correspondance
!=	<code>performance !=extrême</code>	Ne correspond pas

Opérateur	Exemple	La valeur d'étiquette d'un pool doit :
in	emplacement à (est, ouest)	Être dans l'ensemble de valeurs
notin	performances notin (argent, bronze)	Ne pas être dans l'ensemble de valeurs
<key>	la protection	Existe avec n'importe quelle valeur
!<key>	!protection	N'existe pas

## Groupes d'accès de volume

En savoir plus sur la façon dont Astra Trident utilise "[groupes d'accès de volume](#)".



Ignorez cette section si vous utilisez CHAP, qui est recommandé pour simplifier la gestion et éviter la limite de mise à l'échelle décrite ci-dessous. De plus, si vous utilisez Astra Trident en mode CSI, vous pouvez ignorer cette section. Astra Trident utilise CHAP lorsqu'il est installé en tant que mécanisme de provisionnement CSI amélioré.

### En savoir plus sur les groupes d'accès aux volumes

Astra Trident peut utiliser des groupes d'accès de volume pour contrôler l'accès aux volumes qu'il provisionne. Si CHAP est désactivé, il s'attend à trouver un groupe d'accès appelé `trident`, sauf si vous spécifiez un ou plusieurs ID de groupe d'accès dans la configuration.

ASTRA Trident associe de nouveaux volumes aux groupes d'accès configurés, mais il ne crée pas et ne gère pas les groupes d'accès eux-mêmes. Les groupes d'accès doivent exister avant l'ajout du système back-end de stockage à Astra Trident et doivent contenir les IQN iSCSI de chaque nœud du cluster Kubernetes pouvant potentiellement monter les volumes provisionnés par ce back-end. Dans la plupart des installations, cela inclut tous les nœuds workers dans le cluster.

Pour les clusters Kubernetes de plus de 64 nœuds, vous devez utiliser plusieurs groupes d'accès. Chaque groupe d'accès peut contenir jusqu'à 64 IQN et chaque volume peut appartenir à quatre groupes d'accès. Avec quatre groupes d'accès configurés au maximum, n'importe quel nœud d'un cluster de 256 nœuds maximum pourra accéder à n'importe quel volume. Pour connaître les dernières limites des groupes d'accès aux volumes, reportez-vous "[ici](#)" à la section .

Si vous modifiez la configuration d'un groupe qui utilise le groupe d'accès par défaut `trident` à un autre, incluez l'ID du `trident` groupe d'accès dans la liste.

## Démarrage rapide d'Astra Trident

Vous pouvez installer Astra Trident et commencer à gérer les ressources de stockage en quelques étapes. Avant de commencer, consultez "[Exigences d'Astra Trident](#)".



Pour Docker, reportez-vous "[Astra Trident pour Docker](#)" à la .



### 1 Installer Astra Trident

ASTRA Trident offre plusieurs méthodes et modes d'installation optimisés pour un large éventail d'environnements et d'entreprises.

"Installer Astra Trident"

2

## Préparez le nœud worker

Tous les nœuds workers du cluster Kubernetes doivent pouvoir monter les volumes provisionnés pour vos pods.

["Préparez le nœud de travail"](#)

3

## Créer un backend

Un système back-end définit la relation entre Astra Trident et un système de stockage. Il explique à Astra Trident comment communiquer avec ce système de stockage et comment Astra Trident doit provisionner des volumes à partir de celui-ci.

["Configurer un back-end"](#) de votre système de stockage

4

## Créez une classe de stockage Kubernetes

L'objet StorageClass Kubernetes spécifie Astra Trident en tant que mécanisme de provisionnement et permet de créer une classe de stockage pour provisionner des volumes avec des attributs personnalisables. Astra Trident crée une classe de stockage correspondante pour les objets Kubernetes pour spécifier le mécanisme de provisionnement Astra Trident.

["Créer une classe de stockage"](#)

5

## Provisionner un volume

Un *PersistentVolume* (PV) est une ressource de stockage physique provisionnée par l'administrateur du cluster sur un cluster Kubernetes. La demande de volume persistant *PersistentVolumeClaim* (PVC) est une demande d'accès au volume persistant sur le cluster.

Créez un volume persistant et une demande de volume persistant qui utilisent la classe de stockage Kubernetes configurée pour demander l'accès au volume persistant. Vous pouvez ensuite monter le volume persistant sur un pod.

["Provisionner un volume"](#)

## Et la suite ?

Vous pouvez à présent ajouter des systèmes back-end supplémentaires, gérer les classes de stockage, gérer les systèmes back-end et effectuer des opérations de volume.

## De formation

Avant d'installer Astra Trident, il est recommandé de vérifier ces exigences système générales. Il se peut que les systèmes back-end spécifiques présentent des exigences supplémentaires.

## Informations stratégiques sur Astra Trident

Vous devez lire les renseignements essentiels suivants sur Astra Trident.

### <strong> informations pratiques sur le Tridécouvrez Astra </strong>

- Kubernetes 1.30 est désormais pris en charge dans Astra Trident. Mettez à niveau Astra Trident avant de mettre à niveau Kubernetes.
- ASTRA Trident applique strictement l'utilisation de la configuration de chemins d'accès multiples dans les environnements SAN, avec la valeur recommandée de `find_multipaths: no` dans le fichier multipathing.conf.

L'utilisation d'une configuration sans chemins d'accès multiples ou l'utilisation d'`find_multipaths: yes` une valeur ou `find_multipaths: smart` dans un fichier multipath.conf entraînera des échecs de montage. ASTRA Trident recommande l'utilisation de `find_multipaths: no` depuis la version 21.07.

## Systèmes front-end (orchestrateurs) pris en charge

Astra Trident prend en charge plusieurs moteurs et orchestrateurs de conteneur, notamment :

- Anthos sur site (VMware) et Anthos sur bare Metal 1.16
- Kubernetes 1.24 - 1.30
- OpenShift 4.10 - 4.16

L'opérateur de Trident est pris en charge par ces versions :

- Anthos sur site (VMware) et Anthos sur bare Metal 1.16
- Kubernetes 1.24 - 01.30
- OpenShift 4.10 - 4.16

ASTRA Trident fonctionne également avec de nombreuses autres offres Kubernetes entièrement gérées et autogérées, notamment Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Services (EKS), Azure Kubernetes Service (AKS), Mirantis Kubernetes Engine (MKE), Rancher et le portefeuille VMware Tanzu.

ASTRA Trident et ONTAP peuvent être utilisés comme fournisseur de stockage pour ["KubeVirt"](#).

 Avant de mettre à niveau un cluster Kubernetes de la version 1.24 vers la version 1.25 ou ultérieure sur ["Mettre à niveau une installation Helm"](#) lequel Astra Trident est installé, reportez-vous à la section .

## Systèmes back-end pris en charge (stockage)

Pour utiliser Astra Trident, vous avez besoin d'un ou de plusieurs des systèmes back-end pris en charge :

- Amazon FSX pour NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP

- Cloud Volumes Service pour GCP
- FAS/AFF>Select 9.5 ou version ultérieure
- Baie SAN 100 % Flash (ASA) de NetApp
- Logiciel NetApp HCI/Element 11 ou version ultérieure

## Configuration requise

Le tableau ci-dessous résume les fonctionnalités disponibles dans cette version d'Astra Trident et les versions de Kubernetes qu'il prend en charge.

Fonction	Version Kubernetes	Portes-fonctions requises ?
Astra Trident	1,24 - 1,30	Non
Snapshots de volume	1,24 - 1,30	Non
Volume persistant à partir des copies Snapshot des volumes	1,24 - 1,30	Non
Redimensionnement PV iSCSI	1,24 - 1,30	Non
Chap bidirectionnel ONTAP	1,24 - 1,30	Non
Règles d'exportation dynamiques	1,24 - 1,30	Non
Opérateur Trident	1,24 - 1,30	Non
Topologie CSI	1,24 - 1,30	Non

## Systèmes d'exploitation hôtes testés

Bien que l'Astra Trident ne prenne pas officiellement en charge des systèmes d'exploitation spécifiques, il s'agit des éléments suivants qui fonctionnent :

- Versions de Red Hat CoreOS (RHCOS) prises en charge par OpenShift Container Platform (AMD64 et ARM64)
- RHEL 8+ (AMD64 ET ARM64)



NVMe/TCP requiert RHEL 9 ou version ultérieure.

- Ubuntu 22.04 ou version ultérieure (AMD64 et ARM64)
- Windows Server 2022

Par défaut, Astra Trident s'exécute dans un conteneur et s'exécute donc sur un utilisateur Linux. Cependant, ces employés doivent pouvoir monter les volumes qu'Astra Trident utilise le client NFS standard ou l'initiateur iSCSI, en fonction du système back-end utilisé.

L' `tridentctl` utilitaire s'exécute également sur n'importe laquelle de ces distributions de Linux.

## Configuration de l'hôte

Tous les nœuds workers du cluster Kubernetes doivent pouvoir monter les volumes provisionnés pour vos pods. Pour préparer les nœuds worker, vous devez installer les outils NFS, iSCSI ou NVMe en fonction de votre sélection de pilotes.

["Préparez le nœud de travail"](#)

## Configuration du système de stockage

Il est possible qu'Astra Trident modifie le système de stockage avant qu'une configuration back-end ne puisse l'utiliser.

["Configuration des systèmes back-end"](#)

## Ports Trident d'Astra

L'Astra Trident doit accéder à des ports spécifiques pour la communication.

["Ports Trident d'Astra"](#)

## Images de conteneur et versions Kubernetes correspondantes

Pour les installations utilisant des systèmes à air comprimé, la liste suivante est une référence des images de conteneur nécessaires à l'installation d'Astra Trident. Utiliser `tridentctl images` la commande pour vérifier la liste des images de conteneur nécessaires.

Versions de Kubernetes	Image de conteneur
v1.24.0, v1.25.0, v1.26.0, v1.27.0, v1.28.0, v1.29.0, v1.30.0	<ul style="list-style-type: none"><li>• docker.io/netapp/trident : 24.06.0</li><li>• docker.io/netapp/trident-autosupport:24.06</li><li>• registry.k8s.io/sig-storage/csi-provisionneur:v4.0.1</li><li>• registry.k8s.io/sig-storage/csi-attacher:v4.6.0</li><li>• registry.k8s.io/sig-storage/csi-resizer:v1.11.0</li><li>• registry.k8s.io/sig-storage/csi-snapshotter:v7.0.2</li><li>• registry.k8s.io/sig-storage/csi-node-driver-registratr:v2.10.0</li><li>• docker.io/netapp/trident-operator:24.06.0 (en option)</li></ul>

# **Installer Astra Trident**

**Installer à l'aide de l'opérateur Trident**

**Installation à l'aide de tridentctl**

# Avec Astra Trident

## Préparez le nœud de travail

Tous les nœuds workers du cluster Kubernetes doivent pouvoir monter les volumes provisionnés pour vos pods. Pour préparer les nœuds worker, vous devez installer les outils NFS, iSCSI ou NVMe/TCP en fonction de votre sélection de pilotes.

### Choisir les bons outils

Si vous utilisez une combinaison de pilotes, vous devez installer tous les outils requis pour vos pilotes. Les versions récentes de RedHat CoreOS ont les outils installés par défaut.

#### Outils NFS

["Installez les outils NFS"](#) si vous utilisez : ontap-nas, , ontap-nas-economy, ontap-nas-flexgroup, azure-netapp-files gcp-cvs .

#### Outils iSCSI

["Installez les outils iSCSI"](#) si vous utilisez : ontap-san, , ontap-san-economy solidfire-san .

#### Outils NVMe

["Installez les outils NVMe"](#) Si vous utilisez ontap-san pour le protocole NVMe (Nonvolatile Memory Express) over TCP (NVMe/TCP).



ONTAP 9.12 ou version ultérieure est recommandé pour NVMe/TCP.

## Détection des services de nœud

Astra Trident tente de détecter automatiquement si le nœud peut exécuter des services iSCSI ou NFS.



La découverte de services de nœuds identifie les services détectés, mais ne garantit pas que les services sont correctement configurés. Inversement, l'absence d'un service découvert ne garantit pas l'échec du montage du volume.

### Révision des événements

Astra Trident crée des événements pour le nœud afin d'identifier les services découverts. Pour passer en revue ces événements, exécutez :

```
kubectl get event -A --field-selector involvedObject.name=<Kubernetes node name>
```

### Examiner les services découverts

Astra Trident identifie les services activés pour chaque nœud du nœud Trident CR. Pour afficher les services découverts, exécutez :

```
tridentctl get node -o wide -n <Trident namespace>
```

## Volumes NFS

Installez les outils NFS à l'aide des commandes de votre système d'exploitation. Assurez-vous que le service NFS est démarré pendant le démarrage.

### RHEL 8+

```
sudo yum install -y nfs-utils
```

### Ubuntu

```
sudo apt-get install -y nfs-common
```



Redémarrez les nœuds workers après l'installation des outils NFS afin d'éviter toute défaillance lors de la connexion des volumes aux conteneurs.

## Volumes iSCSI

Astra Trident peut établir automatiquement une session iSCSI, analyser les LUN et détecter les périphériques à chemins d'accès multiples, les formater et les monter sur un pod.

### Fonctionnalités d'auto-rétablissement de l'iSCSI

Pour les systèmes ONTAP, Astra Trident exécute l'auto-rétablissement iSCSI toutes les cinq minutes pour :

1. **Identifier** l'état de session iSCSI souhaité et l'état de session iSCSI en cours.
2. **Comparer** l'état souhaité à l'état actuel pour identifier les réparations nécessaires. Astra Trident détermine les priorités de réparation et le moment auquel les réparations doivent être effectuées.
3. **Effectuez les réparations** requises pour rétablir l'état de session iSCSI actuel à l'état de session iSCSI souhaité.



Les journaux d'activité d'auto-rétablissement se trouvent dans `trident-main` le conteneur sur le pod Demeset respectif. Pour afficher les journaux, vous devez avoir défini `debug` sur « `true` » lors de l'installation d'Astra Trident.

Avec les fonctionnalités d'autorétablissement iSCSI d'Astra Trident,

- Sessions iSCSI obsolètes ou non saines pouvant survenir après un problème de connectivité réseau. Dans le cas d'une session obsolète, Astra Trident attend sept minutes avant de se déconnecter pour rétablir la connexion avec un portail.



Par exemple, si les secrets CHAP ont tourné sur le contrôleur de stockage et que le réseau perd la connectivité, les anciens secrets CHAP (*obsolète*) pourraient persister. L'auto-rétablissement peut reconnaître ceci et rétablir automatiquement la session pour appliquer les secrets CHAP mis à jour.

- Sessions iSCSI manquantes
- LUN manquantes

## Points à prendre en compte avant de mettre à niveau Trident

- Si seuls les igroups par nœud (introduits dans 23.04+) sont utilisés, l'auto-rétablissement iSCSI lance des renumérisations SCSI pour tous les périphériques du bus SCSI.
- Si seuls les igroups dont le périmètre est back-end (*obsolète* à partir de la version 23.04) sont utilisés, l'auto-rétablissement iSCSI lance des renumérisations SCSI pour obtenir les ID de LUN exacts dans le bus SCSI.
- Si une combinaison d'igroups par nœud et d'igroups scoped back-end est utilisée, l'autorétablissement iSCSI lance des renumérisations SCSI pour obtenir des ID de LUN exacts sur le bus SCSI.

## Installez les outils iSCSI

Installez les outils iSCSI à l'aide des commandes de votre système d'exploitation.

### Avant de commencer

- Chaque nœud du cluster Kubernetes doit avoir un IQN unique. **C'est une condition préalable nécessaire.**
- Si vous utilisez RHCOS version 4.5 ou ultérieure, ou toute autre distribution Linux compatible avec RHEL, avec le `solidfire-san` pilote et Element OS 12.5 ou version antérieure, assurez-vous que l'algorithme d'authentification CHAP est défini sur MD5 dans les `/etc/iscsi/iscsid.conf` algorithmes CHAP sécurisés conformes à la norme FIPS SHA1, SHA-256 et SHA3-256 sont disponibles avec Element 12.7.

```
sudo sed -i 's/^(\node.session.auth.chap_algs\).*/\1 = MD5/'  
/etc/iscsi/iscsid.conf
```

- Lors de l'utilisation de nœuds worker exécutant RHEL/RedHat CoreOS avec iSCSI PVS, spécifiez la `discard` `mountOption` dans la classe de stockage pour effectuer la récupération d'espace en ligne. Reportez-vous à la "[Documentation Red Hat](#)".

## RHEL 8+

1. Installez les packages système suivants :

```
sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils device-mapper-multipath
```

2. Vérifiez que la version iscsi-initiator-utils est 6.2.0.874-2.el7 ou ultérieure :

```
rpm -q iscsi-initiator-utils
```

3. Définir la numérisation sur manuelle :

```
sudo sed -i 's/^\\(node.session.scan\\) .*\\1 = manual/' /etc/iscsi/iscsid.conf
```

4. Activer les chemins d'accès multiples :

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```



Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de defaults.

5. Assurez-vous que `iscsid` et `multipathd` sont en cours d'exécution :

```
sudo systemctl enable --now iscsid multipathd
```

6. Activer et démarrer `iscsi`:

```
sudo systemctl enable --now iscsi
```

## Ubuntu

1. Installez les packages système suivants :

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools scsitools
```

2. Vérifiez que la version Open-iscsi est 2.0.874-5ubuntu2.10 ou ultérieure (pour bionic) ou 2.0.874-7.1ubuntu6.1 ou ultérieure (pour focal) :

```
dpkg -l open-iscsi
```

### 3. Définir la numérisation sur manuelle :

```
sudo sed -i 's/^\\(node.session.scan\\).*/\\1 = manual/'  
/etc/iscsi/iscsid.conf
```

### 4. Activer les chemins d'accès multiples :

```
sudo tee /etc/multipath.conf <<-'EOF'  
defaults {  
    user_friendly_names yes  
    find_multipaths no  
}  
EOF  
sudo systemctl enable --now multipath-tools.service  
sudo service multipath-tools restart
```



Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

### 5. Assurez-vous que `open-iscsi` et `multipath-tools` sont activés et en cours d'exécution :

```
sudo systemctl status multipath-tools  
sudo systemctl enable --now open-iscsi.service  
sudo systemctl status open-iscsi
```



Pour Ubuntu 18.04, vous devez détecter les ports cibles avec `iscsiadm` avant de démarrer `open-iscsi` pour que le démon iSCSI démarre. Vous pouvez également modifier le `iscsi` service pour qu'il démarre `iscsid` automatiquement.

## Configurez ou désactivez l'auto-rétablissement iSCSI

Vous pouvez configurer les paramètres d'autorétablissement iSCSI d'Astra Trident suivants pour corriger les sessions obsolètes :

- **Intervalle d'auto-rétablissement iSCSI** : détermine la fréquence à laquelle l'auto-rétablissement iSCSI est appelé (par défaut : 5 minutes). Vous pouvez le configurer pour qu'il s'exécute plus fréquemment en définissant un nombre plus petit ou moins fréquemment en définissant un nombre plus grand.

 La définition de l'intervalle d'auto-rétablissement iSCSI sur 0 arrête complètement l'auto-rétablissement iSCSI. Nous ne recommandons pas de désactiver l'auto-rétablissement iSCSI. Il ne doit être désactivé que dans certains cas lorsque l'auto-rétablissement iSCSI ne fonctionne pas comme prévu ou à des fins de débogage.

- **Délai d'attente d'auto-rétablissement iSCSI** : détermine la durée d'attente de l'auto-rétablissement iSCSI avant de se déconnecter d'une session défectueuse et de tenter de se reconnecter (par défaut : 7 minutes). Vous pouvez le configurer sur un nombre plus grand de sorte que les sessions identifiées comme non saines doivent attendre plus longtemps avant d'être déconnectées, puis une tentative de connexion est faite, ou un nombre plus petit pour se déconnecter et se connecter plus tôt.

## Gouvernail

Pour configurer ou modifier les paramètres d'autorétablissement iSCSI, passez les `iscsiSelfHealingInterval` paramètres et `iscsiSelfHealingWaitTime` lors de l'installation de Helm ou de la mise à jour Helm.

L'exemple suivant définit l'intervalle d'auto-rétablissement iSCSI sur 3 minutes et le temps d'attente d'auto-rétablissement sur 6 minutes :

```
helm install trident trident-operator-100.2406.0.tgz --set
iscsiSelfHealingInterval=3m0s --set iscsiSelfHealingWaitTime=6m0s -n
trident
```

## tridentctl

Pour configurer ou modifier les paramètres d'auto-rétablissement iSCSI, passez les `iscsi-self-healing-interval` paramètres et `iscsi-self-healing-wait-time` lors de l'installation ou de la mise à jour de tridentctl.

L'exemple suivant définit l'intervalle d'auto-rétablissement iSCSI sur 3 minutes et le temps d'attente d'auto-rétablissement sur 6 minutes :

```
tridentctl install --iscsi-self-healing-interval=3m0s --iscsi-self-
-healing-wait-time=6m0s -n trident
```

## Volumes NVMe/TCP

Installez les outils NVMe à l'aide des commandes correspondant à votre système d'exploitation.

- 
- NVMe requiert RHEL 9 ou version ultérieure.
  - Si la version du noyau de votre nœud Kubernetes est trop ancienne ou si le package NVMe n'est pas disponible pour votre version du noyau, vous devrez peut-être mettre à jour la version du noyau de votre nœud avec le package NVMe.

## RHEL 9

```
sudo yum install nvme-cli
sudo yum install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

## Ubuntu

```
sudo apt install nvme-cli
sudo apt -y install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

## Vérifiez l'installation

Après l'installation, vérifiez que chaque nœud du cluster Kubernetes dispose d'un NQN unique via la commande :

```
cat /etc/nvme/hostnqn
```



ASTRA Trident modifie la `ctrl_device_tmo` valeur pour s'assurer que NVMe ne renonce pas au chemin s'il tombe en panne. Ne modifiez pas ce paramètre.

# Configuration et gestion des systèmes back-end

## Configuration des systèmes back-end

Un système back-end définit la relation entre Astra Trident et un système de stockage. Il explique à Astra Trident comment communiquer avec ce système de stockage et comment Astra Trident doit provisionner des volumes à partir de celui-ci.

Astra Trident propose automatiquement des pools de stockage back-end correspondant aux exigences définies par une classe de stockage. Découvrez comment configurer le système back-end pour votre système de stockage.

- ["Configurer un back-end Azure NetApp Files"](#)
- ["Configurer un système back-end Cloud Volumes Service pour Google Cloud Platform"](#)
- ["Configurer un système NetApp HCI ou SolidFire backend"](#)
- ["Configurer un système back-end avec des pilotes NAS ONTAP ou Cloud Volumes ONTAP"](#)
- ["Configurer un système back-end avec des pilotes SAN ONTAP ou Cloud Volumes ONTAP"](#)
- ["Utilisez Astra Trident avec Amazon FSX pour NetApp ONTAP"](#)

## Azure NetApp Files

### Configurer un back-end Azure NetApp Files

Vous pouvez configurer Azure NetApp Files en tant que back-end pour Astra Trident. Vous pouvez relier des volumes NFS et SMB à l'aide d'un back-end Azure NetApp Files. ASTRA Trident prend également en charge la gestion des identifiants à l'aide d'identités gérées pour les clusters Azure Kubernetes Services (AKS).

#### Détails du pilote Azure NetApp Files

ASTRA Trident fournit les pilotes de stockage Azure NetApp Files suivants pour communiquer avec le cluster. Les modes d'accès pris en charge sont : *ReadWriteOnce* (RWO), *ReadOnlyMey* (ROX), *ReadWriteMaly* (RWX), *ReadWriteOncePod* (RWOP).

Conducteur	Protocole	Mode Volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
azure-netapp-files	NFS SMB	Système de fichiers	RWO, ROX, RWX, RWOP	nfs, smb

### Considérations

- Le service Azure NetApp Files ne prend pas en charge des volumes de moins de 100 Go. ASTRA Trident crée automatiquement des volumes de 100 Gio si un volume plus petit est demandé.
- Astra Trident prend en charge les volumes SMB montés sur des pods qui s'exécutent uniquement sur des nœuds Windows.

### Identités gérées pour AKS

ASTRA Trident prend en charge "[identités gérées](#)" les clusters Azure Kubernetes Services. Pour tirer parti de la gestion rationalisée des informations d'identification offerte par les identités gérées, vous devez disposer des éléments suivants :

- Cluster Kubernetes déployé à l'aide d'AKS
- Identités gérées configurées sur le cluster AKS kubernetes
- ASTRA Trident installé qui inclut le `cloudProvider` à spécifier "Azure".

## Opérateur Trident

Pour installer Astra Trident à l'aide de l'opérateur Trident, modifiez `tridentorchestrator_cr.yaml` pour définir sur `cloudProvider "Azure"`. Par exemple :

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
```

## Gouvernail

L'exemple suivant installe les ensembles Astra Trident `cloudProvider` sur Azure à l'aide de la variable d'environnement `$CP` :

```
helm install trident trident-operator-100.2406.0.tgz --create
-namespace --namespace <trident-namespace> --set cloudProvider=$CP
```

**<code> </code>**

L'exemple suivant installe Astra Trident et définit le `cloudProvider` drapeau sur Azure:

```
tridentctl install --cloud-provider="Azure" -n trident
```

## Identité cloud pour AKS

L'identité cloud permet aux pods Kubernetes d'accéder aux ressources Azure en s'authentifiant comme identité de workload au lieu de fournir des informations d'identification Azure explicites.

Pour tirer parti de l'identité cloud dans Azure, vous devez disposer des éléments suivants :

- Cluster Kubernetes déployé à l'aide d'AKS
- Identité de la charge de travail et émetteur oidc configurés sur le cluster AKS Kubernetes
- ASTRA Trident installé, qui inclut le système `cloudProvider` à spécifier "Azure" et `cloudIdentity` spécifier l'identité de workload

## Opérateur Trident

Pour installer Astra Trident à l'aide de l'opérateur Trident, modifiez `tridentoperator_cr.yaml` pour définir sur `cloudProvider "Azure"` et définir `cloudIdentity` sur `azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx`.

Par exemple :

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullPolicy: IfNotPresent
  cloudProvider: "Azure"
  *cloudIdentity: 'azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx'*
```

## Gouvernail

Définissez les valeurs des indicateurs **cloud-Provider (CP)** et **cloud-Identity (ci)** à l'aide des variables d'environnement suivantes :

```
export CP="Azure"
export CI="azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx"
```

L'exemple suivant installe Astra Trident et le définit `cloudProvider` sur Azure à l'aide de la variable d'environnement `$CP` et définit le `cloudIdentity` à l'aide de la variable d'environnement `$CI` :

```
helm install trident trident-operator-100.2406.0.tgz --set
cloudProvider=$CP --set cloudIdentity=$CI
```

**<code> </code>**

Définissez les valeurs des indicateurs **cloud Provider** et **cloud Identity** à l'aide des variables d'environnement suivantes :

```
export CP="Azure"
export CI="azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx"
```

L'exemple suivant installe Astra Trident et définit le `cloud-provider` drapeau sur `$CP`, et `cloud-identity` sur `$CI`:

```
tridentctl install --cloud-provider=$CP --cloud-identity="$CI" -n  
trident
```

## Préparez la configuration d'un back-end Azure NetApp Files

Avant de pouvoir configurer le système back-end Azure NetApp Files, vous devez vous assurer que les exigences suivantes sont respectées.

### Prérequis pour les volumes NFS et SMB

Si vous utilisez Azure NetApp Files pour la première fois ou dans un nouvel emplacement, une configuration initiale est requise pour configurer Azure NetApp Files et créer un volume NFS. Reportez-vous à la ["Azure : configurez Azure NetApp Files et créez un volume NFS"](#).

Pour configurer et utiliser un ["Azure NetApp Files"](#) back-end, vous avez besoin des éléments suivants :

- subscriptionID, tenantID clientID , , location Et clientSecret sont facultatifs lorsque vous utilisez des identités gérées sur un cluster AKS.
  - tenantID, clientID Et clientSecret sont facultatifs lors de l'utilisation d'une identité de cloud sur un cluster AKS.
- Un pool de capacité. Reportez-vous à la ["Microsoft : créez un pool de capacité pour Azure NetApp Files"](#).
- Sous-réseau délégué à Azure NetApp Files. Reportez-vous à la ["Microsoft : déléguer un sous-réseau à Azure NetApp Files"](#).
- subscriptionID Depuis un abonnement Azure avec Azure NetApp Files activé.
- tenantID, clientID Et clientSecret à partir d'un ["Enregistrement d'applications"](#) dans Azure Active Directory avec les autorisations suffisantes pour le service Azure NetApp Files. L'enregistrement de l'application doit utiliser l'une des options suivantes :
  - Le rôle propriétaire ou contributeur ["Prédéfinie par Azure"](#).
  - A ["Rôle de contributeur personnalisé"](#) au niveau de l'abonnement (assignableScopes) avec les autorisations suivantes qui sont limitées à ce qu'Astra Trident exige. Après avoir créé le rôle personnalisé, ["Attribuez le rôle à l'aide du portail Azure"](#).

## Rôle de contributeur personnalisé

```
{
  "id": "/subscriptions/<subscription-id>/providers/Microsoft.Authorization/roleDefinitions/<role-definition-id>",
  "properties": {
    "roleName": "custom-role-with-limited-perms",
    "description": "custom role providing limited permissions",
    "assignableScopes": [
      "/subscriptions/<subscription-id>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.NetApp/netAppAccounts/capacityPools/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/read",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/write",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/snapshots/delete",
          "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/MountTargets/read",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/subnets/read",
          "Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/read",
          "Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/write"
        ]
      }
    ]
  }
}
```

```

    "Microsoft.Features/featureProviders/subscriptionFeatureRegistrations/delete",
        "Microsoft.Features/features/read",
        "Microsoft.Features/operations/read",
        "Microsoft.Features/providers/features/read",

    "Microsoft.Features/providers/features/register/action",

    "Microsoft.Features/providers/features/unregister/action",

    "Microsoft.Features/subscriptionFeatureRegistrations/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
    }
]
}
}

```

- L'Azure location qui contient au moins un "[sous-réseau délégué](#)". À partir de Trident 22.01, le location paramètre est un champ obligatoire au niveau supérieur du fichier de configuration back-end. Les valeurs d'emplacement spécifiées dans les pools virtuels sont ignorées.
- Pour utiliser Cloud Identity, obtenez le client ID à partir d'un "[identité gérée attribuée par l'utilisateur](#)" et spécifiez cet ID dans azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.

#### Exigences supplémentaires pour les volumes SMB

Pour créer un volume SMB, vous devez disposer des éléments suivants :

- Active Directory configuré et connecté à Azure NetApp Files. Reportez-vous à la "[Microsoft : création et gestion des connexions Active Directory pour Azure NetApp Files](#)".
- Cluster Kubernetes avec un nœud de contrôleur Linux et au moins un nœud worker Windows exécutant Windows Server 2022. Astra Trident prend en charge les volumes SMB montés sur des pods qui s'exécutent uniquement sur des nœuds Windows.
- Au moins un secret Astra Trident contenant vos informations d'identification Active Directory pour que Azure NetApp Files puisse s'authentifier auprès d'Active Directory. Pour générer un secret smbcreds:

```

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

```

- Un proxy CSI configuré en tant que service Windows. Pour configurer un `csi-proxy`, reportez-vous

"GitHub : proxy CSI" à la section ou "GitHub : proxy CSI pour Windows" pour les nœuds Kubernetes s'exécutant sous Windows.

## Exemples et options de configuration du back-end Azure NetApp Files

Découvrez les options de configuration NFS et SMB backend pour Azure NetApp Files et passez en revue les exemples de configuration.

### Options de configuration du back-end

ASTRA Trident utilise votre configuration back-end (sous-réseau, réseau virtuel, niveau de service et emplacement) pour créer des volumes Azure NetApp Files sur des pools de capacité disponibles à l'emplacement demandé et qui correspondent au niveau de service et au sous-réseau requis.



Astra Trident ne prend pas en charge les pools de capacité manuels de QoS.

Les systèmes Azure NetApp Files back-end proposent ces options de configuration.

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	« azure-netapp-files »
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + caractères aléatoires
subscriptionID	L'ID d'abonnement de votre abonnement Azure Facultatif lorsque les identités gérées sont activées sur un cluster AKS.	
tenantID	L'ID de locataire d'un enregistrement d'application facultatif lorsque des identités gérées ou une identité cloud sont utilisées sur un cluster AKS.	
clientID	L'ID client d'un enregistrement d'application facultatif lorsque des identités gérées ou une identité cloud sont utilisées sur un cluster AKS.	
clientSecret	Le secret client d'une application Registration Facultatif lorsque des identités gérées ou une identité cloud sont utilisées sur un cluster AKS.	
serviceLevel	Un de Standard, , Premium ou Ultra	« » (aléatoire)

Paramètre	Description	Valeur par défaut
location	Nom de l'emplacement Azure où les nouveaux volumes seront créés Facultatif lorsque les identités gérées sont activées sur un cluster AKS.	
resourceGroups	Liste des groupes de ressources pour le filtrage des ressources découvertes	«[]» (sans filtre)
netappAccounts	Liste des comptes NetApp permettant de filtrer les ressources découvertes	«[]» (sans filtre)
capacityPools	Liste des pools de capacité pour le filtrage des ressources découvertes	«[]» (sans filtre, aléatoire)
virtualNetwork	Nom d'un réseau virtuel avec un sous-réseau délégué	«»
subnet	Nom d'un sous-réseau délégué à Microsoft.Netapp/volumes	«»
networkFeatures	Ensemble de fonctions vNet pour un volume, peut être Basic ou Standard. Les fonctions réseau ne sont pas disponibles dans toutes les régions et peuvent être activées dans un abonnement. Si vous spécifiez networkFeatures lorsque la fonctionnalité n'est pas activée, le provisionnement des volumes échoue.	«»
nfsMountOptions	Contrôle précis des options de montage NFS. Ignoré pour les volumes SMB. Pour monter des volumes avec NFS version 4.1, incluez nfsvers=4 dans la liste des options de montage délimitées par des virgules pour choisir NFS v4.1. Les options de montage définies dans une définition de classe de stockage remplacent les options de montage définies dans la configuration backend.	«nfsvers=3»
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur	«» (non appliqué par défaut)

Paramètre	Description	Valeur par défaut
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, <code>\{"api": false, "method": true, "discovery": true}</code> . Ne l'utilisez pas à moins que vous ne soyez en mesure de résoudre les problèmes et que vous ayez besoin d'un viddage détaillé des journaux.	nul
nasType	Configurez la création de volumes NFS ou SMB. Les options sont nfs, smb ou NULL. La valeur null par défaut sur les volumes NFS.	nfs
supportedTopologies	Représente une liste de régions et de zones prises en charge par ce back-end. Pour plus d'informations, reportez-vous <a href="#">"Utiliser la topologie CSI"</a> à .	



Pour plus d'informations sur les fonctionnalités réseau, reportez-vous ["Configurer les fonctions réseau d'un volume Azure NetApp Files"](#) à la section .

## Autorisations et ressources requises

Si vous recevez une erreur « aucun pool de capacité trouvé » lors de la création d'une demande de volume persistant, il est probable que votre enregistrement d'application ne dispose pas des autorisations et des ressources requises (sous-réseau, réseau virtuel, pool de capacité). Si le débogage est activé, Astra Trident consigne les ressources Azure découvertes lors de la création du back-end. Vérifiez que vous utilisez un rôle approprié.

Les valeurs de `resourceGroups`, `netappAccounts`, `capacityPools`, `virtualNetwork` et `subnet` peuvent être spécifiées à l'aide de noms courts ou complets. Les noms complets sont recommandés dans la plupart des cas, car les noms abrégés peuvent faire correspondre plusieurs ressources avec le même nom.

Les `resourceGroups` valeurs , , `netappAccounts` et `capacityPools` sont des filtres qui limitent l'ensemble des ressources découvertes à celles disponibles pour ce back-end de stockage et peuvent être spécifiées dans n'importe quelle combinaison. Les noms complets suivent le format suivant :

Type	Format
Groupe de ressources	<code>&lt;groupe de ressources&gt;</code>
Compte NetApp	<code>&lt;groupe de ressources&gt;/&lt;compte netapp&gt;</code>
Pool de capacité	<code>&lt;groupe de ressources&gt;/&lt;compte netapp&gt;/&lt;pool de capacité&gt;</code>
Réseau virtuel	<code>&lt;groupe de ressources&gt;/&lt;région virtuel&gt;</code>
Sous-réseau	<code>&lt;groupe de ressources&gt;/&lt;région virtuel&gt;/&lt;sous-réseau&gt;</code>

## Provisionnement de volume

Vous pouvez contrôler le provisionnement de volume par défaut en spécifiant les options suivantes dans une section spéciale du fichier de configuration. Voir [Exemples de configurations](#) pour plus de détails.

Paramètre	Description	Valeur par défaut
exportRule	Règles d'exportation pour les nouveaux volumes. exportRule Doit être une liste séparée par des virgules de toute combinaison d'adresses IPv4 ou de sous-réseaux IPv4 en notation CIDR. Ignoré pour les volumes SMB.	« 0.0.0.0/0 »
snapshotDir	Contrôle la visibilité du répertoire .snapshot	« faux »
size	Taille par défaut des nouveaux volumes	« 100 G »
unixPermissions	Les autorisations unix des nouveaux volumes (4 chiffres octaux). Ignoré pour les volumes SMB.	« » (fonction d'aperçu, liste blanche requise dans l'abonnement)

## Exemples de configurations

Les exemples suivants montrent des configurations de base qui laissent la plupart des paramètres par défaut. C'est la façon la plus simple de définir un back-end.

## Configuration minimale

Il s'agit de la configuration back-end minimale absolue. Avec cette configuration, Astra Trident détecte tous vos comptes NetApp, pools de capacité et sous-réseaux délégués à Azure NetApp Files à l'emplacement configuré, et place de nouveaux volumes dans l'un de ces pools et sous-réseaux de manière aléatoire. Comme `nasType` est omis, la `nfs` valeur par défaut s'applique et le back-end provisionne les volumes NFS.

Cette configuration est idéale lorsque vous commencez à utiliser Azure NetApp Files et que vous essayez d'autres fonctionnalités, mais dans la pratique, vous voudrez ajouter de l'étendue aux volumes que vous provisionnez.

```
---
```

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
  tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
  clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
  clientSecret: SECRET
  location: eastus
```

## Identités gérées pour AKS

Cette configuration backend omet `subscriptionID` `tenantID` `clientID` , , , et `clientSecret`, qui sont facultatifs lors de l'utilisation d'identités gérées.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools: ["ultra-pool"]
  resourceGroups: ["aks-ami-eastus-rg"]
  netappAccounts: ["smb-na"]
  virtualNetwork: eastus-prod-vnet
  subnet: eastus-anf-subnet
```

## Identité cloud pour AKS

Cette configuration backend omet `tenantID` `clientID` , et `clientSecret`, qui sont facultatifs lors de l'utilisation d'une identité de nuage.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf-1
  namespace: trident
spec:
  version: 1
  storageDriverName: azure-netapp-files
  capacityPools: ["ultra-pool"]
  resourceGroups: ["aks-ami-eastus-rg"]
  netappAccounts: ["smb-na"]
  virtualNetwork: eastus-prod-vnet
  subnet: eastus-anf-subnet
  location: eastus
  subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
```

## Configuration de niveau de service spécifique avec filtres de pool de capacité

Cette configuration back-end place les volumes dans l'emplacement d'Azure `eastus` dans un `Ultra` pool de capacité. ASTRA Trident détecte automatiquement tous les sous-réseaux délégués à Azure NetApp Files à cet emplacement et place un nouveau volume sur l'un d'entre eux de manière aléatoire.

```
---  
version: 1  
storageDriverName: azure-netapp-files  
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451  
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf  
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa  
clientSecret: SECRET  
location: eastus  
serviceLevel: Ultra  
capacityPools:  
- application-group-1/account-1/ultra-1  
- application-group-1/account-1/ultra-2
```

## Configuration avancée

Cette configuration back-end réduit davantage l'étendue du placement des volumes sur un seul sous-réseau et modifie également certains paramètres par défaut du provisionnement des volumes.

```
---
```

```
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
serviceLevel: Ultra
capacityPools:
- application-group-1/account-1/ultra-1
- application-group-1/account-1/ultra-2
virtualNetwork: my-virtual-network
subnet: my-subnet
networkFeatures: Standard
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 500Gi
defaults:
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  snapshotDir: 'true'
  size: 200Gi
  unixPermissions: '0777'
```

## Configuration de pool virtuel

Cette configuration back-end définit plusieurs pools de stockage dans un seul fichier. Cette fonction est utile lorsque plusieurs pools de capacité prennent en charge différents niveaux de service, et que vous souhaitez créer des classes de stockage dans Kubernetes qui les représentent. Des étiquettes de pool virtuel ont été utilisées pour différencier les pools en fonction de performance .

```
---
version: 1
storageDriverName: azure-netapp-files
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa
clientSecret: SECRET
location: eastus
resourceGroups:
- application-group-1
networkFeatures: Basic
nfsMountOptions: vers=3,proto=tcp,timeo=600
labels:
  cloud: azure
storage:
- labels:
    performance: gold
    serviceLevel: Ultra
    capacityPools:
    - ultra-1
    - ultra-2
    networkFeatures: Standard
- labels:
    performance: silver
    serviceLevel: Premium
    capacityPools:
    - premium-1
- labels:
    performance: bronze
    serviceLevel: Standard
    capacityPools:
    - standard-1
    - standard-2
```

## Configuration des topologies prises en charge

ASTRA Trident facilite le provisionnement de volumes pour les workloads en fonction des régions et des zones de disponibilité. Le `supportedTopologies` bloc de cette configuration back-end est utilisé pour fournir une liste de régions et de zones par back-end. Les valeurs de région et de zone spécifiées ici doivent correspondre aux valeurs de région et de zone indiquées sur les étiquettes de chaque nœud de cluster Kubernetes. Ces régions et zones représentent la liste des valeurs autorisées pouvant être fournies dans une classe de stockage. Pour les classes de stockage qui contiennent un sous-ensemble des régions et zones fournies dans un back-end, Astra Trident crée des volumes dans la région et la zone mentionnées. Pour plus d'informations, reportez-vous "[Utiliser la topologie CSI](#)" à .

```
---  
version: 1  
storageDriverName: azure-netapp-files  
subscriptionID: 9f87c765-4774-fake-ae98-a721add45451  
tenantID: 68e4f836-edc1-fake-bff9-b2d865ee56cf  
clientID: dd043f63-bf8e-fake-8076-8de91e5713aa  
clientSecret: SECRET  
location: eastus  
serviceLevel: Ultra  
capacityPools:  
- application-group-1/account-1/ultra-1  
- application-group-1/account-1/ultra-2  
supportedTopologies:  
- topology.kubernetes.io/region: eastus  
  topology.kubernetes.io/zone: eastus-1  
- topology.kubernetes.io/region: eastus  
  topology.kubernetes.io/zone: eastus-2
```

## Définitions des classes de stockage

Les définitions suivantes `StorageClass` font référence aux pools de stockage ci-dessus.

### Exemples de définitions utilisant le parameter.selector champ

A l'aide de `parameter.selector`, vous pouvez spécifier pour chaque `StorageClass` pool virtuel utilisé pour héberger un volume. Les aspects définis dans le pool sélectionné seront définis pour le volume.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: bronze
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze"
allowVolumeExpansion: true

```

## Exemples de définitions pour les volumes SMB

A l'aide de `nasType`, `node-stage-secret-name`, et `node-stage-secret-namespace`, vous pouvez spécifier un volume SMB et fournir les informations d'identification Active Directory requises.

## Configuration de base sur l'espace de noms par défaut

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## Utilisation de secrets différents par espace de noms

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

## Utilisation de secrets différents par volume

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-smb
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: ${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```



nasType: smb Filtres pour les pools qui prennent en charge les volumes SMB. nasType: nfs Ou nasType: null des filtres pour les pools NFS.

### Créer le backend

Après avoir créé le fichier de configuration backend, exécutez la commande suivante :

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

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

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

## Google Cloud NetApp volumes

### Configurez un système back-end Google Cloud NetApp volumes

Vous pouvez désormais configurer Google Cloud NetApp volumes en tant que back-end pour Astra Trident. Vous pouvez relier des volumes NFS à l'aide d'un système back-end Google Cloud NetApp volumes.

Google Cloud NetApp Volumes is a tech preview feature in Astra Trident 24.06.

### Détails du pilote Google Cloud NetApp volumes

ASTRA Trident fournit le `google-cloud-netapp-volumes` pilote pour communiquer avec le cluster. Les modes d'accès pris en charge sont : `ReadWriteOnce` (RWO), `ReadOnlyMey` (ROX), `ReadWriteMaly` (RWX), `ReadWriteOncePod` (RWOP).

Conducteur	Protocole	Mode Volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
google-cloud-netapp-volumes	NFS	Système de fichiers	RWO, ROX, RWX, RWOP	nfs

### Préparez la configuration d'un système back-end Google Cloud NetApp volumes

Avant de pouvoir configurer votre système back-end Google Cloud NetApp volumes, vous devez vous assurer que les exigences suivantes sont respectées.

## Prérequis pour les volumes NFS

Si vous utilisez Google Cloud NetApp volumes pour la première fois ou dans un nouvel emplacement, une configuration initiale est requise pour configurer Google Cloud NetApp volumes et créer un volume NFS. Reportez-vous à la ["Avant de commencer"](#).

Vérifiez les points suivants avant de configurer le système back-end Google Cloud NetApp volumes :

- Compte Google Cloud configuré avec le service Google Cloud NetApp volumes. Reportez-vous à la ["Google Cloud NetApp volumes"](#).
- Numéro de projet de votre compte Google Cloud. Reportez-vous à la ["Identification des projets"](#).
- Un compte de service Google Cloud avec le rôle d'administrateur NetApp volumes (netappcloudvolumes.admin). Reportez-vous à la ["Rôles et autorisations de gestion des identités et des accès"](#).
- Fichier de clé API pour votre compte GCNV. Reportez-vous à ["Authentifiez-vous à l'aide de clés API"](#).
- Un pool de stockage. Reportez-vous à la ["Présentation des pools de stockage"](#).

Pour plus d'informations sur la configuration de l'accès à Google Cloud NetApp volumes, consultez ["Configurez l'accès à Google Cloud NetApp volumes"](#).

## Options et exemples de configuration back-end de Google Cloud NetApp volumes

Découvrez les options de configuration NFS backend pour Google Cloud NetApp volumes et examinez des exemples de configuration.

### Options de configuration du back-end

Chaque back-end provisionne les volumes dans une seule région Google Cloud. Pour créer des volumes dans d'autres régions, vous pouvez définir des systèmes back-end supplémentaires.

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	La valeur de storageDriverName doit être indiquée comme « google-cloud-netapp-volumes ».
backendName	(Facultatif) Nom personnalisé du système back-end de stockage	Nom du pilote + " " + partie de la clé API
storagePools	Paramètre facultatif utilisé pour spécifier les pools de stockage pour la création du volume.	
projectNumber	Numéro de projet de compte Google Cloud. La valeur est disponible sur la page d'accueil du portail Google Cloud.	

Paramètre	Description	Valeur par défaut
location	Emplacement Google Cloud où Astra Trident crée des volumes GCNV. Lors de la création de clusters Kubernetes répartis entre régions, les volumes créés dans un <code>location</code> peuvent être utilisés dans des workloads planifiés sur des nœuds répartis sur plusieurs régions Google Cloud. Le trafic entre les régions coûte plus cher.	
apiKey	Clé d'API pour le compte de service Google Cloud avec le <code>netappcloudvolumes.admin</code> rôle. Il inclut le contenu au format JSON du fichier de clé privée d'un compte de service Google Cloud (copié en compte dans le fichier de configuration back-end). Le <code>apiKey</code> doit inclure des paires clé-valeur pour les clés suivantes : <code>type</code> <code>project_id</code> , <code>client_email</code> , <code>client_id</code> , <code>auth_uri</code> <code>token_uri</code> <code>auth_provider_x509_cert_url</code> , et <code>client_x509_cert_url</code> .	
nfsMountOptions	Contrôle précis des options de montage NFS.	« <code>nfsvers=3</code> »
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur.	« » (non appliqué par défaut)
serviceLevel	Niveau de service d'un pool de stockage et de ses volumes. Les valeurs sont <code>flex</code> , <code>standard</code> , <code>premium</code> ou <code>extreme</code> .	
network	Réseau Google Cloud utilisé pour les volumes GCNV.	
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, <code>{"api":false, "method":true}</code> . Ne l'utilisez pas à moins que vous ne soyez en mesure de résoudre les problèmes et que vous ayez besoin d'un vidage détaillé des journaux.	nul
supportedTopologies	Représente une liste de régions et de zones prises en charge par ce back-end. Pour plus d'informations, reportez-vous <a href="#">"Utiliser la topologie CSI"</a> à . Par exemple : <code>supportedTopologies:</code> - <code>topology.kubernetes.io/region: europe-west6</code> <code>topology.kubernetes.io/zone: europe-west6-b</code>	

#### Options de provisionnement de volumes

Vous pouvez contrôler le provisionnement du volume par défaut dans la `defaults` section du fichier de configuration.

Paramètre	Description	Valeur par défaut
exportRule	Règles d'exportation pour les nouveaux volumes. Doit être une liste séparée par des virgules de toute combinaison d'adresses IPv4.	« 0.0.0.0/0 »
snapshotDir	Accès au .snapshot répertoire	« faux »
snapshotReserve	Pourcentage de volume réservé pour les snapshots	« » (accepter la valeur par défaut de 0)
unixPermissions	Les autorisations unix des nouveaux volumes (4 chiffres octaux).	« »

### Exemples de configurations

Les exemples suivants montrent des configurations de base qui laissent la plupart des paramètres par défaut. C'est la façon la plus simple de définir un back-end.

## Configuration minimale

Il s'agit de la configuration back-end minimale absolue. Avec cette configuration, Astra Trident détecte tous vos pools de stockage délégués à Google Cloud NetApp volumes à l'emplacement configuré, et place de nouveaux volumes dans l'un de ces pools de manière aléatoire. Comme `nasType` est omis, la `nfs` valeur par défaut s'applique et le back-end provisionne les volumes NFS.

Cette configuration est idéale lorsque vous n'utilisez que Google Cloud NetApp volumes et que vous essayez d'effectuer des opérations. Dans la pratique, vous devrez probablement fournir une étendue supplémentaire pour les volumes que vous provisionnez.

— — —

```
XsYg6gyxy4zq70lwWgLwGa==  
-----END PRIVATE KEY-----
```

----

```
apiVersion: trident.netapp.io/v1  
kind: TridentBackendConfig  
metadata:  
  name: backend-tbc-gcnv  
spec:  
  version: 1  
  storageDriverName: google-cloud-netapp-volumes  
  projectNumber: '123455380079'  
  location: europe-west6  
  serviceLevel: premium  
  apiKey:  
    type: service_account  
    project_id: my-gcnv-project  
    client_email: myproject-prod@my-gcnv-  
project.iam.gserviceaccount.com  
    client_id: '103346282737811234567'  
    auth_uri: https://accounts.google.com/o/oauth2/auth  
    token_uri: https://oauth2.googleapis.com/token  
    auth_provider_x509_cert_url:  
      https://www.googleapis.com/oauth2/v1/certs  
      client_x509_cert_url:  
        https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-  
gcnv-project.iam.gserviceaccount.com  
  credentials:  
    name: backend-tbc-gcnv-secret
```

## Configuration avec filtre StoragePools

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-gcnv-secret
type: Opaque
stringData:
  private_key_id: 'f2cb6ed6d7cc10c453f7d3406fc700c5df0ab9ec'
  private_key: |
    -----BEGIN PRIVATE KEY-----
    znHczZsrrtHisIsAbOguSaPIKeyAZNchRAGzlzZE4jK3b1/qp8B4Kws8zX5ojY9m
    XsYg6gyxy4zq7OlwWgLwGa==
    -----END PRIVATE KEY-----
    ---

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
```

```
version: 1
storageDriverName: google-cloud-netapp-volumes
projectNumber: '123455380079'
location: europe-west6
serviceLevel: premium
storagePools:
- premium-pool1-europe-west6
- premium-pool2-europe-west6
apiKey:
  type: service_account
  project_id: my-gcnv-project
  client_email: myproject-prod@my-gcnv-
project.iam.gserviceaccount.com
  client_id: '103346282737811234567'
  auth_uri: https://accounts.google.com/o/oauth2/auth
  token_uri: https://oauth2.googleapis.com/token
  auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
credentials:
  name: backend-tbc-gcnv-secret
```

## Configuration de pool virtuel

Cette configuration back-end définit plusieurs pools virtuels dans un seul fichier. Les pools virtuels sont définis dans la `storage` section. Ces fonctionnalités sont utiles lorsque plusieurs pools de stockage prennent en charge différents niveaux de services et que vous souhaitez créer dans Kubernetes des classes de stockage qui les représentent. Les étiquettes de pool virtuel sont utilisées pour différencier les pools. Par exemple, dans l'exemple ci-dessous `performance`, le libellé et `serviceLevel` le type sont utilisés pour différencier les pools virtuels.

Vous pouvez également définir des valeurs par défaut applicables à tous les pools virtuels et remplacer les valeurs par défaut des pools virtuels individuels. Dans l'exemple suivant, `snapshotReserve` et `exportRule` servent de valeurs par défaut pour tous les pools virtuels.

Pour plus d'informations, reportez-vous "[Pools virtuels](#)" à .

```

znHczzsrrtHisIsAbOguSaPIKeyAZNchRAGzlzzE4jK3b1/qp8B4Kws8zX5ojY9m
znHczzsrrtHisIsAbOguSaPIKeyAZNchRAGzlzzE4jK3b1/qp8B4Kws8zX5ojY9m
znHczzsrrtHisIsAbOguSaPIKeyAZNchRAGzlzzE4jK3b1/qp8B4Kws8zX5ojY9m
XsYg6gyxy4zq70lwWgLwGa==
-----END PRIVATE KEY-----

---

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: '123455380079'
  location: europe-west6
  apiKey:
    type: service_account
    project_id: my-gcnv-project
    client_email: myproject-prod@my-gcnv-
project.iam.gserviceaccount.com
    client_id: '103346282737811234567'
    auth_uri: https://accounts.google.com/o/oauth2/auth
    token_uri: https://oauth2.googleapis.com/token
    auth_provider_x509_cert_url:
      https://www.googleapis.com/oauth2/v1/certs
    client_x509_cert_url:
      https://www.googleapis.com/robot/v1/metadata/x509/myproject-prod%40my-
gcnv-project.iam.gserviceaccount.com
  credentials:
    name: backend-tbc-gcnv-secret
  defaults:
    snapshotReserve: '10'
    exportRule: 10.0.0.0/24
  storage:
    - labels:
        performance: extreme
        serviceLevel: extreme
        defaults:
          snapshotReserve: '5'
          exportRule: 0.0.0.0/0
    - labels:
        performance: premium
        serviceLevel: premium
    - labels:

```

```
  performance: standard
  serviceLevel: standard
```

## Et la suite ?

Après avoir créé le fichier de configuration backend, exécutez la commande suivante :

```
kubectl create -f <backend-file>
```

Pour vérifier que le back-end est correctement créé, exécutez la commande suivante :

```
kubectl get tridentbackendconfig
```

NAME	BACKEND NAME	BACKEND UUID
PHASE STATUS		
backend-tbc-gcnav	backend-tbc-gcnav	b2fd1ff9-b234-477e-88fd-713913294f65
Bound Success		

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez décrire le back-end à l'aide de la `kubectl get tridentbackendconfig <backend-name>` commande ou afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

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

## Plus d'exemples

### Exemples de définition de classe de stockage

Voici une définition de base `StorageClass` qui fait référence au back-end ci-dessus.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnav-nfs-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
```

### Exemples de définitions utilisant le `parameter.selector` champ :

A l'aide de `parameter.selector`, vous pouvez spécifier pour chaque `StorageClass` système "pool virtuel" utilisé pour héberger un volume. Les aspects définis dans le pool sélectionné seront définis pour le volume.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: extreme-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=extreme"
  backendType: "google-cloud-netapp-volumes"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: premium-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium"
  backendType: "google-cloud-netapp-volumes"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: standard-sc
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=standard"
  backendType: "google-cloud-netapp-volumes"
```

Pour plus de détails sur les classes de stockage, reportez-vous "[Créer une classe de stockage](#)" à la section .

### **Exemple de définition de PVC**

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: gcnv-nfs-pvc
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 100Gi
  storageClassName: gcnv-nfs-sc

```

Pour vérifier si la demande de volume persistant est liée, exécutez la commande suivante :

```
kubectl get pvc gcnv-nfs-pvc
```

NAME	STATUS	VOLUME	CAPACITY
ACCESS MODES	STORAGECLASS	AGE	
gcnv-nfs-pvc	Bound	pvc-b00f2414-e229-40e6-9b16-ee03eb79a213	100Gi
RWX	gcnv-nfs-sc	1m	

## Configurer un système Cloud Volumes Service pour Google Cloud backend

Découvrez comment configurer NetApp Cloud Volumes Service pour Google Cloud en tant que backend pour votre installation d'Astra Trident à l'aide des exemples de configuration fournis.

### Détails du pilote Google Cloud

ASTRA Trident fournit le `gcp-cvs` pilote pour communiquer avec le cluster. Les modes d'accès pris en charge sont : `ReadWriteOnce` (RWO), `ReadOnlyMany` (ROX), `ReadWriteMany` (RWX), `ReadWriteOncePod` (RWOP).

Conducteur	Protocole	Mode Volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
<code>gcp-cvs</code>	NFS	Système de fichiers	RWO, ROX, RWX, RWOP	<code>nfs</code>

### En savoir plus sur la prise en charge d'Astra Trident pour Cloud Volumes Service pour Google Cloud

ASTRA Trident peut créer des volumes Cloud Volumes Service dans l'une des deux "[types de service](#)" :

- **CVS-Performance** : le type de service Astra Trident par défaut. Ce type de service aux performances optimisées est parfaitement adapté aux charges de travail de production qui exigent des performances élevées. Le type de service CVS-Performance est une option matérielle prenant en charge les volumes d'une taille minimale de 100 Gio. Vous pouvez choisir l'une des "[trois niveaux de service](#)" options suivantes

:

- standard
- premium
- extreme

- **CVS:** Le type de service CVS fournit une haute disponibilité zonale avec des niveaux de performance limités à modérés. Le type de service CVS est une option logicielle utilisant des pools de stockage pour prendre en charge des volumes de 1 Gio. Le pool de stockage peut contenir jusqu'à 50 volumes dans lesquels tous les volumes partagent la capacité et les performances du pool. Vous pouvez choisir l'une des "deux niveaux de service" options suivantes :

- standardsw
- zoneredundantstandardsw

### Ce dont vous avez besoin

Pour configurer et utiliser le "[Cloud Volumes Service pour Google Cloud](#)" back-end, vous avez besoin des éléments suivants :

- Un compte Google Cloud configuré avec NetApp Cloud Volumes Service
- Numéro de projet de votre compte Google Cloud
- Compte de service Google Cloud avec le `netappcloudvolumes.admin` rôle
- Fichier de clé API pour votre compte Cloud Volumes Service

### Options de configuration du back-end

Chaque back-end provisionne les volumes dans une seule région Google Cloud. Pour créer des volumes dans d'autres régions, vous pouvez définir des systèmes back-end supplémentaires.

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	« gcp-cvs »
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + " " + partie de la clé API
storageClass	Paramètre facultatif utilisé pour spécifier le type de service CVS. Utilisez <code>software</code> pour sélectionner le type de service CVS. Sinon, Astra Trident suppose le type de service CVS-Performance (hardware).	
storagePools	Type de service CVS uniquement. Paramètre facultatif utilisé pour spécifier les pools de stockage pour la création du volume.	
projectNumber	Numéro de projet de compte Google Cloud. La valeur est disponible sur la page d'accueil du portail Google Cloud.	
hostProjectNumber	Requis si l'utilisation d'un réseau VPC partagé. Dans ce scénario, <code>projectNumber</code> est le projet de service, et <code>hostProjectNumber</code> est le projet hôte.	

Paramètre	Description	Valeur par défaut
apiRegion	Région Google Cloud dans laquelle Astra Trident crée des volumes Cloud Volumes Service. Lors de la création de clusters Kubernetes répartis entre régions, les volumes créés dans un <code>apiRegion</code> peuvent être utilisés dans des workloads planifiés sur des nœuds répartis sur plusieurs régions Google Cloud. Le trafic entre les régions coûte plus cher.	
apiKey	Clé d'API pour le compte de service Google Cloud avec le <code>netappcloudvolumes.admin</code> rôle. Il inclut le contenu au format JSON du fichier de clé privée d'un compte de service Google Cloud (copié en compte dans le fichier de configuration back-end).	
proxyURL	URL proxy si le serveur proxy doit se connecter au compte CVS. Le serveur proxy peut être un proxy HTTP ou HTTPS. Pour un proxy HTTPS, la validation du certificat est ignorée pour permettre l'utilisation de certificats auto-signés dans le serveur proxy. Les serveurs proxy avec authentification activée ne sont pas pris en charge.	
nfsMountOptions	Contrôle précis des options de montage NFS.	« <code>nfsvers=3</code> »
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur.	« » (non appliqué par défaut)
serviceLevel	Niveau de service CVS-Performance ou CVS pour les nouveaux volumes. Les valeurs de performances CVS sont <code>standard</code> , <code>premium</code> ou <code>extreme</code> . Les valeurs CVS sont <code>standardsw</code> ou <code>zoneredundantstandardsw</code> .	CVS-Performance par défaut est « <code>standard</code> ». CVS default est "standardsw".
network	Réseau Google Cloud utilisé pour les volumes Cloud Volumes Service.	« par défaut »
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, <code>\{ "api":false, "method":true \}</code> . Ne l'utilisez pas à moins que vous ne soyez en mesure de résoudre les problèmes et que vous ayez besoin d'un vidage détaillé des journaux.	nul
allowedTopologies	Pour activer l'accès interrégional, votre définition de classe de stockage pour <code>allowedTopologies</code> doit inclure toutes les régions. Par exemple : <ul style="list-style-type: none"> <li>- <code>key: topology.kubernetes.io/region</code></li> <li><code>values:</code></li> <li>- <code>us-east1</code></li> <li>- <code>europe-west1</code></li> </ul>	

## Options de provisionnement de volumes

Vous pouvez contrôler le provisionnement du volume par défaut dans la `defaults` section du fichier de configuration.

Paramètre	Description	Valeur par défaut
exportRule	Règles d'exportation pour les nouveaux volumes. Doit être une liste séparée par des virgules d'une combinaison d'adresses IPv4 ou de sous-réseaux IPv4 en notation CIDR.	« 0.0.0.0/0 »
snapshotDir	Accès au .snapshot répertoire	« faux »
snapshotReserve	Pourcentage de volume réservé pour les snapshots	« » (Accepter CVS par défaut de 0)
size	La taille des nouveaux volumes. CVS-Performance minimum est de 100 Gio. CVS est au minimum de 1 Gio.	Le type de service CVS-Performance utilise par défaut « 100 Gio ». Le type de service CVS n'est pas défini par défaut mais nécessite au moins 1 Gio.

### Exemples de type de service CVS-Performance

Les exemples suivants fournissent des exemples de configuration pour le type de service CVS-Performance.

## Exemple 1 : configuration minimale

Il s'agit de la configuration back-end minimale avec le type de service CVS-Performance par défaut et le niveau de service « standard » par défaut.

```
---  
version: 1  
storageDriverName: gcp-cvs  
projectNumber: '012345678901'  
apiRegion: us-west2  
apiKey:  
  type: service_account  
  project_id: my-gcp-project  
  private_key_id: "<id_value>"  
  private_key: |  
    -----BEGIN PRIVATE KEY-----  
    <key_value>  
    -----END PRIVATE KEY-----  
  client_email: cloudvolumes-admin-sa@my-gcp-  
project.iam.gserviceaccount.com  
  client_id: '123456789012345678901'  
  auth_uri: https://accounts.google.com/o/oauth2/auth  
  token_uri: https://oauth2.googleapis.com/token  
  auth_provider_x509_cert_url:  
    https://www.googleapis.com/oauth2/v1/certs  
  client_x509_cert_url:  
    https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-  
sa%40my-gcp-project.iam.gserviceaccount.com
```

## Exemple 2 : configuration du niveau de service

Dans cet exemple, nous présentons les options de configuration du back-end, y compris les niveaux de service et les valeurs par défaut des volumes.

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
apiRegion: us-west2
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
client_id: '123456789012345678901'
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
  https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
    https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
    sa%40my-gcp-project.iam.gserviceaccount.com
proxyURL: http://proxy-server-hostname/
nfsMountOptions: vers=3,proto=tcp,timeo=600
limitVolumeSize: 10Ti
serviceLevel: premium
defaults:
  snapshotDir: 'true'
  snapshotReserve: '5'
  exportRule: 10.0.0.0/24,10.0.1.0/24,10.0.2.100
  size: 5Ti
```

### Exemple 3 : configuration de pool virtuel

Cet exemple utilise `storage` pour configurer les pools virtuels et le `StorageClasses` qui les renvoie. Reportez-vous [Définitions des classes de stockage](#) à la pour savoir comment les classes de stockage ont été définies.

Ici, des valeurs par défaut spécifiques sont définies pour tous les pools virtuels, qui définissent le `snapshotReserve` à 5 % et le `exportRule` à 0.0.0.0/0. Les pools virtuels sont définis dans la `storage` section. Chaque pool virtuel individuel définit son propre pool `serviceLevel` et certains pools remplacent les valeurs par défaut. Des étiquettes de pool virtuel ont été utilisées pour différencier les pools en fonction de `performance` et `'protection'` de .

```
---
version: 1
storageDriverName: gcp-cvs
projectNumber: '012345678901'
apiRegion: us-west2
apiKey:
  type: service_account
  project_id: my-gcp-project
  private_key_id: "<id_value>"
  private_key: |
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
client_email: cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com
client_id: '123456789012345678901'
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
  https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
  https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com
nfsMountOptions: vers=3,proto=tcp,timeo=600
defaults:
  snapshotReserve: '5'
  exportRule: 0.0.0.0/0
labels:
  cloud: gcp
region: us-west2
storage:
- labels:
    performance: extreme
    protection: extra
    serviceLevel: extreme
```

```
defaults:
  snapshotDir: 'true'
  snapshotReserve: '10'
  exportRule: 10.0.0.0/24
- labels:
  performance: extreme
  protection: standard
  serviceLevel: extreme
- labels:
  performance: premium
  protection: extra
  serviceLevel: premium
defaults:
  snapshotDir: 'true'
  snapshotReserve: '10'
- labels:
  performance: premium
  protection: standard
  serviceLevel: premium
- labels:
  performance: standard
  serviceLevel: standard
```

## Définitions des classes de stockage

Les définitions de classe de stockage suivantes s'appliquent à l'exemple de configuration de pool virtuel. A l'aide de `parameters.selector`, vous pouvez spécifier pour chaque classe de stockage le pool virtuel utilisé pour héberger un volume. Les aspects définis dans le pool sélectionné seront définis pour le volume.

## Exemple de classe de stockage

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=extreme; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-standard-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium-extra-protection
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-standard
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=standard"
allowVolumeExpansion: true
```

```
---  
apiVersion: storage.k8s.io/v1  
kind: StorageClass  
metadata:  
  name: cvs-extra-protection  
provisioner: csi.trident.netapp.io  
parameters:  
  selector: "protection=extra"  
allowVolumeExpansion: true
```

- La première classe de stockage (`cvs-extreme-extra-protection`) est mappée sur le premier pool virtuel. Il s'agit du seul pool offrant des performances extrêmes avec une réserve Snapshot de 10 %.
- La dernière classe de stockage (`cvs-extra-protection`) fait appel à n'importe quel pool de stockage qui fournit une réserve de snapshots de 10 %. Astra Trident décide du pool virtuel sélectionné et s'assure que les exigences de la réserve de snapshots sont respectées.

### Exemples de type de service CVS

Les exemples suivants fournissent des exemples de configuration pour le type de service CVS.

## Exemple 1 : configuration minimale

Il s'agit de la configuration dorsale minimale qui utilise `storageClass` pour spécifier le type de service CVS et le niveau de service par défaut `standardsw`.

```
---  
version: 1  
storageDriverName: gcp-cvs  
projectNumber: '012345678901'  
storageClass: software  
apiRegion: us-east4  
apiKey:  
  type: service_account  
  project_id: my-gcp-project  
  private_key_id: "<id_value>"  
  private_key: |  
    -----BEGIN PRIVATE KEY-----  
    <key_value>  
    -----END PRIVATE KEY-----  
  client_email: cloudvolumes-admin-sa@my-gcp-  
project.iam.gserviceaccount.com  
  client_id: '123456789012345678901'  
  auth_uri: https://accounts.google.com/o/oauth2/auth  
  token_uri: https://oauth2.googleapis.com/token  
  auth_provider_x509_cert_url:  
    https://www.googleapis.com/oauth2/v1/certs  
  client_x509_cert_url:  
    https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-  
    sa%40my-gcp-project.iam.gserviceaccount.com  
  serviceLevel: standardsw
```

## Exemple 2 : configuration du pool de stockage

Cet exemple de configuration back-end utilise `storagePools` pour configurer un pool de stockage.

```
---
version: 1
storageDriverName: gcp-cvs
backendName: gcp-std-so-with-pool
projectNumber: '531265380079'
apiRegion: europe-west1
apiKey:
  type: service_account
  project_id: cloud-native-data
  private_key_id: "<id_value>"
  private_key: |-
    -----BEGIN PRIVATE KEY-----
    <key_value>
    -----END PRIVATE KEY-----
client_email: cloudvolumes-admin-sa@cloud-native-
data.iam.gserviceaccount.com
client_id: '107071413297115343396'
auth_uri: https://accounts.google.com/o/oauth2/auth
token_uri: https://oauth2.googleapis.com/token
auth_provider_x509_cert_url:
https://www.googleapis.com/oauth2/v1/certs
  client_x509_cert_url:
https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40cloud-native-data.iam.gserviceaccount.com
storageClass: software
zone: europe-west1-b
network: default
storagePools:
- 1bc7f380-3314-6005-45e9-c7dc8c2d7509
serviceLevel: Standardsw
```

## Et la suite ?

Après avoir créé le fichier de configuration backend, exécutez la commande suivante :

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

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

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

## Configurer un système NetApp HCI ou SolidFire backend

Découvrez comment créer et utiliser un back-end Element avec votre installation Astra Trident.

### Détails du pilote d'élément

ASTRA Trident fournit le `solidfire-san` pilote de stockage pour communiquer avec le cluster. Les modes d'accès pris en charge sont : `ReadWriteOnce` (RWO), `ReadOnlyMey` (ROX), `ReadWriteMaly` (RWX), `ReadWriteOncePod` (RWOP).

Le `solidfire-san` pilote de stockage prend en charge les modes `file` et `block` volume. Pour le `Filesystem volumeMode`, Astra Trident crée un volume et un système de fichiers. Le type de système de fichiers est spécifié par la classe de stockage.

Conducteur	Protocole	Mode Volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
solidfire-san	ISCSI	Bloc	RWO, ROX, RWX, RWOP	Aucun système de fichiers. Périphérique de bloc brut.
solidfire-san	ISCSI	Système de fichiers	RWO, RWOP	xfs, ext3 ext4

### Avant de commencer

Vous aurez besoin des éléments suivants avant de créer un back-end d'élément.

- Système de stockage pris en charge exécutant le logiciel Element.
- Identifiants de locataire ou administrateur de cluster NetApp HCI/SolidFire pouvant gérer les volumes
- Tous vos nœuds workers Kubernetes doivent avoir installé les outils iSCSI appropriés. Reportez-vous à la "[informations de préparation du nœud de travail](#)".

### Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	Toujours « solidfire-san ».

Paramètre	Description	Valeur par défaut
backendName	Nom personnalisé ou système back-end de stockage	“SolidFire_” + adresse IP de stockage (iSCSI)
Endpoint	MVIP pour le cluster SolidFire avec les identifiants de locataire	
SVIP	Port et adresse IP de stockage (iSCSI)	
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes.	« »
TenantName	Nom du locataire à utiliser (créé si introuvable)	
InitiatorIFace	Limitez le trafic iSCSI à une interface hôte spécifique	« par défaut »
UseCHAP	Utilisez CHAP pour authentifier iSCSI. ASTRA Trident utilise le protocole CHAP.	vrai
AccessGroups	Liste des ID de groupes d'accès à utiliser	Recherche l'ID d'un groupe d'accès nommé « trident »
Types	Spécifications de QoS	
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur	« » (non appliqué par défaut)
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, {"api":false, "méthode":true}	nul



Ne pas utiliser debugTraceFlags sauf si vous effectuez un dépannage et que vous avez besoin d'un vidage de journal détaillé.

### Exemple 1 : configuration back-end pour un solidfire-san pilote avec trois types de volume

Cet exemple montre un fichier back-end utilisant l'authentification CHAP et la modélisation de trois types de volumes avec des garanties de QoS spécifiques. Il est probable que vous définissiez ensuite les classes de stockage pour les consommer à l'aide du IOPS paramètre de classe de stockage.

```
---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
SVIP: "<svip>:3260"
TenantName: "<tenant>"
labels:
  k8scluster: dev1
  backend: dev1-element-cluster
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
```

## Exemple 2 : configuration du back-end et des classes de stockage pour le solidfire-san pilote avec pools virtuels

Cet exemple représente le fichier de définition du back-end configuré avec des pools virtuels ainsi que des classes de stockage qui les renvoient.

Astra Trident copie les étiquettes présentes sur un pool de stockage vers le LUN de stockage back-end lors du provisionnement. Pour plus de commodité, les administrateurs du stockage peuvent définir des étiquettes par pool virtuel et les volumes de groupe par étiquette.

Dans l'exemple de fichier de définition back-end illustré ci-dessous, des valeurs par défaut spécifiques sont définies pour tous les pools de stockage, qui définissent le `type` sur `Silver`. Les pools virtuels sont définis dans la `storage` section. Dans cet exemple, certains pools de stockage définissent leur propre `type` et certains d'entre eux remplacent les valeurs par défaut définies ci-dessus.

```
---
version: 1
storageDriverName: solidfire-san
Endpoint: https://<user>:<password>@<mvip>/json-rpc/8.0
```

```

SVIP: "<svip>:3260"
TenantName: "<tenant>"
UseCHAP: true
Types:
- Type: Bronze
  Qos:
    minIOPS: 1000
    maxIOPS: 2000
    burstIOPS: 4000
- Type: Silver
  Qos:
    minIOPS: 4000
    maxIOPS: 6000
    burstIOPS: 8000
- Type: Gold
  Qos:
    minIOPS: 6000
    maxIOPS: 8000
    burstIOPS: 10000
type: Silver
labels:
  store: solidfire
  k8scluster: dev-1-cluster
region: us-east-1
storage:
- labels:
    performance: gold
    cost: '4'
    zone: us-east-1a
    type: Gold
- labels:
    performance: silver
    cost: '3'
    zone: us-east-1b
    type: Silver
- labels:
    performance: bronze
    cost: '2'
    zone: us-east-1c
    type: Bronze
- labels:
    performance: silver
    cost: '1'
    zone: us-east-1d

```

Les définitions de classe de stockage suivantes font référence aux pools virtuels ci-dessus. En utilisant ce

parameters.selector champ, chaque classe de stockage indique quel(s) pool(s) virtuel(s) peut(NT) être utilisé(s) pour héberger un volume. Les aspects définis dans le pool virtuel sélectionné seront définis pour le volume.

La première classe de stockage (**solidfire-gold-four**) est mappée sur le premier pool virtuel. Il s'agit de la seule piscine offrant des performances or avec un Volume Type QoS de Gold. La dernière classe de stockage (**solidfire-silver**) fait référence à n'importe quel pool de stockage offrant des performances Silver. Astra Trident va décider du pool virtuel sélectionné et s'assurer que les besoins en stockage sont satisfaits.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-gold-four
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold; cost=4"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-three
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=3"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-bronze-two
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze; cost=2"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-one
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=1"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
  fsType: "ext4"
```

## Trouvez plus d'informations

- "Groupes d'accès de volume"

## Pilotes SAN de ONTAP

### Présentation du pilote SAN ONTAP

Découvrez comment configurer un back-end ONTAP avec les pilotes ONTAP et SAN Cloud Volumes ONTAP.

### Détails du pilote SAN ONTAP

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



Si vous utilisez Astra Control pour la protection, la restauration et la mobilité, lisez [Compatibilité du pilote Astra Control](#) .

Conducteur	Protocole	Mode Volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
ontap-san	ISCSI	Bloc	RWO, ROX, RWX, RWOP	Pas de système de fichiers, périphérique de bloc brut
ontap-san	ISCSI	Système de fichiers	RWO, RWOP ROX et RWX ne sont pas disponibles en mode de volume du système de fichiers.	xfs, ext3 ext4
ontap-san	NVMe/TCP  Reportez-vous à la <a href="#">Autres considérations relatives au NVMe/TCP</a> .	Bloc	RWO, ROX, RWX, RWOP	Pas de système de fichiers, périphérique de bloc brut

Conducteur	Protocole	Mode Volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
ontap-san	NVMe/TCP  Reportez-vous à la <a href="#">Autres considérations relatives au NVMe/TCP</a> .	Système de fichiers	RWO, RWOP  ROX et RWX ne sont pas disponibles en mode de volume du système de fichiers.	xfs, ext3 ext4
ontap-san-economy	ISCSI	Bloc	RWO, ROX, RWX, RWOP	Pas de système de fichiers, périphérique de bloc brut
ontap-san-economy	ISCSI	Système de fichiers	RWO, RWOP  ROX et RWX ne sont pas disponibles en mode de volume du système de fichiers.	xfs, ext3 ext4

## Compatibilité du pilote Astra Control

ASTRA Control offre une protection transparente, une reprise d'activité et une mobilité (déplacement de volumes entre les clusters Kubernetes) pour les volumes créés avec les `ontap-nas` pilotes, `ontap-nas-flexgroup` et `ontap-san`. Voir "[Conditions préalables à la réplication d'Astra Control](#)" pour plus de détails.

- À utiliser `ontap-san-economy` uniquement si le nombre d'utilisations de volume persistant doit être supérieur à "[Limites de volume ONTAP prises en charge](#)".
- À utiliser `ontap-nas-economy` uniquement si le nombre d'utilisations de volume persistant doit être supérieur à et si "[Limites de volume ONTAP prises en charge](#)" le `ontap-san-economy` pilote ne peut pas être utilisé.
- N'utilisez pas cette option `ontap-nas-economy` si vous prévoyez d'avoir besoin de protection des données, de reprise après incident ou de mobilité.

## Autorisations utilisateur

ASTRA Trident attend d'être exécuté en tant qu'administrateur ONTAP ou SVM, généralement avec l'`admin` utilisateur du cluster ou un utilisateur SVM, ou un utilisateur avec un `vsadmin` nom différent qui a le même rôle. Pour les déploiements Amazon FSX pour NetApp ONTAP, Astra Trident prévoit d'être exécutée en tant qu'administrateur ONTAP ou SVM, en utilisant l'utilisateur du cluster ou un utilisateur SVM, ou en tant qu'`fsxadmin` utilisateur `vsadmin` avec un nom différent et ayant le même rôle. `fsxadmin` L'utilisateur est un remplaçant limité pour l'utilisateur admin du cluster.



Si vous utilisez le `limitAggregateUsage` paramètre, les autorisations d'administration du cluster sont requises. Lors de l'utilisation d'Amazon FSX pour NetApp ONTAP avec Astra Trident, le `limitAggregateUsage` paramètre ne fonctionnera pas avec les `vsadmin` comptes d'utilisateur et `fsxadmin`. L'opération de configuration échoue si vous spécifiez ce paramètre.

S'il est possible de créer au sein de ONTAP un rôle plus restrictif qu'un pilote Trident peut utiliser, nous ne le recommandons pas. La plupart des nouvelles versions de Trident appellent des API supplémentaires qui devront être prises en compte, ce qui complique les mises à niveau et risque d'erreurs.

#### Autres considérations relatives au NVMe/TCP

ASTRA Trident prend en charge le protocole NVMe (non-volatile Memory Express) à l'aide du `ontap-san` pilote, notamment :

- IPv6
- Copies Snapshot et clones de volumes NVMe
- Redimensionnement d'un volume NVMe
- Importation d'un volume NVMe créé en dehors d'Astra Trident afin que son cycle de vie puisse être géré par Astra Trident
- Chemins d'accès multiples natifs NVMe
- Arrêt normal ou sans gracieuse des nœuds K8s (24.06)

ASTRA Trident ne prend pas en charge :

- DH-HMAC-CHAP pris en charge par NVMe de manière native
- Chemins d'accès multiples du mappeur de périphériques (DM)
- Cryptage LUKS

### Préparez la configuration du système back-end avec les pilotes SAN ONTAP

Découvrez les exigences et les options d'authentification pour la configuration d'un back-end ONTAP avec des pilotes SAN ONTAP.

#### De formation

Pour tous les systèmes back-end ONTAP, Astra Trident requiert au moins un agrégat affecté à la SVM.

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 celui-ci `ontap-san-economy`.

Tous vos nœuds workers Kubernetes doivent avoir installé les outils iSCSI appropriés. Voir "["Préparez le nœud de travail"](#)" pour plus de détails.

#### Authentifiez le back-end ONTAP

Astra Trident propose deux modes d'authentification d'un système back-end ONTAP.

- Basé sur les informations d'identification : nom d'utilisateur et mot de passe pour 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 de ONTAP.

- Basé sur des certificats : Astra Trident peut également communiquer avec un cluster ONTAP à l'aide d'un certificat installé sur le système back-end. Dans ce cas, la définition `backend` doit contenir des valeurs encodées Base64 du certificat client, de la clé et du certificat d'autorité de certification de confiance, le cas échéant (recommandé).

Vous pouvez mettre à jour les systèmes back-end existants pour passer d'une méthode basée sur les identifiants à une méthode basée sur les certificats. Toutefois, une seule méthode d'authentification est prise en charge à la fois. Pour passer à une méthode d'authentification différente, vous devez supprimer la méthode existante de la configuration `backend`.



Si vous tentez de fournir **les deux identifiants et les certificats**, la création du back-end échoue 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 informations d'identification

Astra Trident nécessite les identifiants d'un administrateur SVM-scoped/cluster-scoped pour communiquer avec le ONTAP back-end. Il est recommandé d'utiliser des rôles standard prédéfinis tels que `admin` ou `vsadmin`. Il est ainsi possible d'assurer une compatibilité avec les futures versions d'ONTAP et d'exposer les API de fonctionnalités à utiliser avec les futures versions d'Astra Trident. Un rôle de connexion de sécurité personnalisé peut être créé et utilisé avec Astra Trident, mais il n'est pas recommandé.

Voici un exemple de définition du back-end :

## 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"
}
```

Gardez à l'esprit que la définition du back-end est le seul endroit où les informations d'identification sont stockées en texte brut. Une fois le système backend créé, les noms d'utilisateur/mots de passe sont codés avec Base64 et stockés sous forme de secrets Kubernetes. La création ou la mise à jour d'un back-end est la seule étape qui nécessite la connaissance des informations d'identification. Il s'agit donc d'une opération uniquement administrative, qui doit être effectuée par l'administrateur Kubernetes/du stockage.

### Activer l'authentification basée sur certificat

Les systèmes back-end, nouveaux et existants, peuvent utiliser un certificat et communiquer avec le système back-end ONTAP. Trois paramètres sont requis dans la définition du back-end.

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

Un flux de travail type comprend 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 pour qu'il s'authentifie.

```
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. Il se peut déjà que l'administrateur de stockage gère cet espace. Ignorer si aucune autorité de certification approuvée 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 (à partir de l'étape 1) sur le cluster ONTAP.

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

4. Vérifiez que le rôle de connexion de sécurité ONTAP prend en charge cert 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 d'un certificat généré. Remplacer <ONTAP Management LIF> et <vserver name> par Management LIF IP et SVM name.

```
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 CA 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 back-end à l'aide des valeurs obtenues à partir de l'étape précédente.

```
cat cert-backend.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkeeee...Vaaallluuuueeee",
  "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 |           |
+-----+-----+
+-----+-----+
```

### Mettre à jour les méthodes d'authentification ou faire pivoter les informations d'identification

Vous pouvez mettre à jour un back-end existant pour utiliser une méthode d'authentification différente ou pour faire pivoter leurs informations d'identification. Cela fonctionne de deux manières : les systèmes back-end qui utilisent le nom d'utilisateur/mot de passe peuvent être mis à jour pour utiliser des certificats ; les systèmes back-end qui utilisent des certificats peuvent être mis à jour en fonction du nom d'utilisateur/mot de passe. Pour ce faire, vous devez supprimer la méthode d'authentification existante et ajouter la nouvelle méthode d'authentification. Utilisez ensuite le fichier backend.json mis à jour contenant les paramètres requis pour exécuter `tridentctl 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 | 
+-----+-----+-----+
+-----+-----+

```

**i** Lors de la rotation des mots de passe, l'administrateur du stockage doit d'abord mettre à jour le mot de passe de l'utilisateur sur ONTAP. Cette opération est suivie d'une mise à jour du back-end. Lors de la rotation de certificats, plusieurs certificats peuvent être ajoutés à l'utilisateur. Le back-end est ensuite mis à jour pour utiliser le nouveau certificat, en suivant lequel l'ancien certificat peut être supprimé du cluster ONTAP.

La mise à jour d'un back-end n'interrompt pas l'accès aux volumes qui ont déjà été créés, et n'a aucun impact sur les connexions de volume effectuées après. Une mise à jour réussie indique qu'Astra Trident peut communiquer avec le système back-end ONTAP et gérer les opérations de volumes à venir.

#### Authentifier les connexions avec le protocole CHAP bidirectionnel

ASTRA Trident peut authentifier les sessions iSCSI avec le protocole CHAP bidirectionnel pour les ontap-san pilotes et ontap-san-economy. Pour ce faire, vous devez activer useCHAP l'option dans votre définition de back-end. Lorsque cette option est définie sur true, Astra Trident configure la sécurité initiateur par défaut du SVM sur CHAP bidirectionnel et définit le nom d'utilisateur et les secrets à partir du fichier back-end. NetApp recommande d'utiliser le protocole CHAP bidirectionnel pour l'authentification des 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: c19qxIm36DKyawxy
chapTargetInitiatorSecret: rqxigXgkesIpwxyz
chapTargetUsername: iJF4heBRT0TCwxyz
chapUsername: uh2aNCLSd6cNwxyz
```

 Le `useCHAP` paramètre est une option booléenne qui ne peut être configurée qu'une seule fois. Elle est définie sur `FALSE` par défaut. Une fois la valeur `true` définie, vous ne pouvez pas la définir sur `false`.

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

## Comment cela fonctionne

En définissant la `useCHAP` valeur sur `true`, l'administrateur du stockage commande à Astra Trident de configurer le protocole CHAP sur le back-end de stockage. Ceci inclut les éléments suivants :

- Configuration du protocole CHAP sur le SVM :
  - Si le type de sécurité initiateur par défaut du SVM est `None` (défini par défaut) et il n'y a pas de LUN préexistantes déjà présentes dans le volume, Astra Trident définit le type de sécurité par défaut sur CHAP et passe à la configuration de l'initiateur CHAP et du nom d'utilisateur et des secrets de la cible.
  - Si le SVM contient des LUN, Astra Trident n'active pas le protocole CHAP sur le SVM. Cela garantit que l'accès aux LUNs déjà présentes sur le SVM n'est pas restreint.
- Configuration de l'initiateur CHAP et du nom d'utilisateur cible et des secrets ; ces options doivent être spécifiées dans la configuration backend (comme indiqué ci-dessus).

Une fois le back-end créé, Astra Trident crée un CRD correspondant `tridentbackend` et stocke les secrets CHAP et les noms d'utilisateur comme des secrets Kubernetes. Tous les volumes persistants créés par Astra Trident sur ce back-end seront montés et rattachés au protocole CHAP.

## Rotation des identifiants et mise à jour des systèmes back-end

Vous pouvez mettre à jour les informations d'identification CHAP en mettant à jour les paramètres CHAP dans `backend.json` le fichier. Ceci nécessitera la mise à jour des secrets CHAP et l'utilisation de la `tridentctl update` commande pour refléter 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 identifiants du cluster de stockage via l'interface de ligne de commande/ONTAP car Astra Trident ne pourra pas détecter 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": "c19qxUpDaTeD",
    "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 ne seront pas affectées. Elles restent actives si les identifiants sont mis à jour par Astra Trident sur le SVM. Les nouvelles connexions utiliseront les informations d'identification mises à jour et les connexions existantes continuent de rester actives. La déconnexion et la reconnexion des anciens volumes persistants se traduiront par l'utilisation des identifiants mis à jour.

### Options et exemples de configuration du SAN ONTAP

Découvrez comment créer et utiliser les pilotes SAN ONTAP avec votre installation Astra Trident. Cette section fournit des exemples de configuration back-end et des détails sur le mappage des systèmes back-end aux classes de stockage.

## Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDrive rName	Nom du pilote de stockage	ontap-nas ontap-nas- economy, ontap-nas- flexgroup, , ontap-san ontap-san-economy
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + dataLIF
managementLIF	Adresse IP d'un cluster ou d'une LIF de management du SVM. Un nom de domaine complet (FQDN) peut être spécifié. Peut être défini pour utiliser des adresses IPv6 si Astra Trident a été installé à l'aide de l'indicateur IPv6. Les adresses IPv6 doivent être définies entre crochets, par exemple [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Pour un basculement MetroCluster transparent, consultez le <a href="#">[mcc-best]</a> .	« 10.0.0.1 », « [2001:1234:abcd::fefe] »
dataLIF	Adresse IP de la LIF de protocole. <b>Ne spécifiez pas pour iSCSI.</b> ASTRA Trident utilise " <a href="#">Mappage de LUN sélectif ONTAP</a> " pour découvrir les LIF iSCSI nécessaires pour établir une session à chemins multiples. Un avertissement est généré si dataLIF est explicitement défini. <b>Omettre pour MetroCluster.</b> Voir la <a href="#">[mcc-best]</a> .	Dérivé par la SVM
svm	Machine virtuelle de stockage à utiliser <b>omet pour MetroCluster.</b> Voir la <a href="#">[mcc-best]</a> .	Dérivé si un SVM managementLIF est spécifié
useCHAP	Utilisez CHAP pour authentifier iSCSI pour les pilotes SAN ONTAP [Boolean]. Défini sur true pour Astra Trident afin de configurer et d'utiliser le protocole CHAP bidirectionnel comme authentification par défaut pour le SVM donné dans le back-end. Voir " <a href="#">"Préparez la configuration du système back-end avec les pilotes SAN ONTAP"</a> " pour plus de détails.	false
chapInitiatorSecret	Secret de l'initiateur CHAP. Requis si useCHAP=true	« »
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	« »
chapTargetInitiatorSecret	Secret de l'initiateur cible CHAP. Requis si useCHAP=true	« »
chapUsername	Nom d'utilisateur entrant. Requis si useCHAP=true	« »
chapTargetUsername	Nom d'utilisateur cible. Requis si useCHAP=true	« »

Paramètre	Description	Valeur par défaut
clientCertificate	Valeur encodée en Base64 du certificat client. Utilisé pour l'authentification par certificat	« »
clientPrivateKey	Valeur encodée en Base64 de la clé privée du client. Utilisé pour l'authentification par certificat	« »
trustedCACertificate	Valeur encodée en Base64 du certificat CA de confiance. Facultatif. Utilisé pour l'authentification basée sur des certificats.	« »
username	Le nom d'utilisateur devait communiquer avec le cluster ONTAP. Utilisé pour l'authentification basée sur les identifiants.	« »
password	Mot de passe requis pour communiquer avec le cluster ONTAP. Utilisé pour l'authentification basée sur les identifiants.	« »
svm	Serveur virtuel de stockage à utiliser	Dérivé si un SVM managementLIF est spécifié
storagePrefix	Préfixe utilisé pour le provisionnement des nouveaux volumes dans la SVM. Ne peut pas être modifié ultérieurement. Pour mettre à jour ce paramètre, vous devez créer un nouveau backend.	trident
limitAggregateUsage	Echec du provisionnement si l'utilisation est supérieure à ce pourcentage. Si vous utilisez un backend Amazon FSX for NetApp ONTAP, ne spécifiez pas limitAggregateUsage. Les fournies fsxadmin et vsadmin ne contiennent pas les autorisations requises pour récupérer l'utilisation des agrégats et les limiter à l'aide d'Astra Trident.	« » (non appliqué par défaut)
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur. Restreint également la taille maximale des volumes qu'il gère pour les qtrees et les LUN.	« » (non appliqué par défaut)
lunsPerFlexvol	Nombre maximal de LUN par FlexVol, doit être compris dans la plage [50, 200]	100
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, {"api":false, "method":true} n'utilisez que si vous effectuez un dépannage et que vous avez besoin d'un vidage de journal détaillé.	null

Paramètre	Description	Valeur par défaut
useREST	<p>Paramètre booléen pour utiliser les API REST de ONTAP.</p> <p>useREST Lorsqu'il est défini sur <code>true</code>, Astra Trident utilisera les API REST ONTAP pour communiquer avec le back-end. Lorsqu'il est défini sur <code>false</code>, Astra Trident utilisera les appels ZAPI ONTAP pour communiquer avec le back-end. Cette fonctionnalité requiert ONTAP 9.11.1 et versions ultérieures. En outre, le rôle de connexion ONTAP utilisé doit avoir accès à l' <code>ontap</code> application. Ceci est satisfait par les rôles et prédéfinis <code>vsadmin</code> <code>cluster-admin</code>.</p> <p>Depuis la version Astra Trident 24.06 et ONTAP 9.15.1 ou version ultérieure,</p> <p>useREST est défini sur <code>true</code> par défaut. Passez useREST à <code>false</code> pour utiliser les appels ZAPI ONTAP.</p> <p>useREST Est pleinement qualifié pour NVMe/TCP.</p>	true Pour ONTAP 9.15.1 ou version ultérieure, sinon <code>false</code> .
sanType	Utilisez pour sélectionner <code>iscsi</code> pour iSCSI ou <code>nvme</code> pour NVMe/TCP.	<code>iscsi</code> si vide

#### Options de configuration back-end pour les volumes de provisionnement

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

Paramètre	Description	Valeur par défaut
spaceAllocation	Allocation d'espace pour les LUN	« vrai »
spaceReserve	Mode de réservation d'espace ; « aucun » (fin) ou « volume » (épais)	« aucun »
snapshotPolicy	Règle Snapshot à utiliser	« aucun »
qosPolicy	QoS policy group à affecter pour les volumes créés. Choisissez une de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> par pool de stockage/back-end. Avec Astra Trident, les groupes de règles de QoS doivent être utilisés avec ONTAP 9.8 ou version ultérieure. Nous recommandons l'utilisation d'un groupe de règles de qualité de service non partagé et nous assurer que le groupe de règles est appliqué à chaque composant individuellement. Un groupe de règles de QoS partagé appliquera le plafond du débit total de toutes les charges de travail.	« »
adaptiveQosPolicy	Groupe de règles de QoS adaptative à attribuer aux volumes créés. Choisissez une de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> par pool de stockage/back-end	« »

Paramètre	Description	Valeur par défaut
snapshotReserve	Pourcentage de volume réservé pour les snapshots	« 0 » si <code>snapshotPolicy</code> est « aucun », sinon « »
splitOnClone	Séparer un clone de son parent lors de sa création	« faux »
encryption	Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume. La valeur par défaut est <code>false</code> . Pour utiliser cette option, NVE doit être sous licence et activé sur le cluster. Si NAE est activé sur le back-end, tous les volumes provisionnés dans Astra Trident seront activés par NAE. Pour plus d'informations, reportez-vous à la section : <a href="#">"Fonctionnement d'Astra Trident avec NVE et NAE"</a> .	« faux »
luksEncryption	Activez le cryptage LUKS. Reportez-vous à la <a href="#">"Utiliser la configuration de clé unifiée Linux (LUKS)"</a> . Le cryptage LUKS n'est pas pris en charge pour NVMe/TCP.	« »
securityStyle	Style de sécurité pour les nouveaux volumes	unix
tieringPolicy	Règle de hiérarchisation à utiliser « aucun »	« Snapshot uniquement » pour la configuration SVM-DR antérieure à ONTAP 9.5
nameTemplate	Modèle pour créer des noms de volume personnalisés.	« »
limitVolumePoolSize	Taille maximale des FlexVol pouvant être demandées lors de l'utilisation de LUN dans le back-end ONTAP-san Economy.	« » (non appliqué par défaut)

## 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 `ontap-san` du pilote, Astra Trident ajoute une capacité supplémentaire de 10 % au FlexVol pour prendre en charge les métadonnées de LUN. La LUN sera provisionnée avec la taille exacte que l'utilisateur demande dans la demande de volume persistant. Astra Trident ajoute 10 % au système FlexVol (dont la taille disponible dans ONTAP). Les utilisateurs obtiennent à présent la capacité utilisable requise. Cette modification empêche également que les LUN ne soient en lecture seule, à moins que l'espace disponible soit pleinement utilisé. Cela ne s'applique pas à l'économie d'`ontap-san`.

Pour les systèmes back-end définis par `snapshotReserve`, Astra Trident calcule la taille des volumes comme suit :

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

Le modèle 1.1 est le modèle 10 % d'Astra Trident supplémentaire qui s'ajoute à la baie FlexVol pour prendre en charge les métadonnées de la LUN. Pour `snapshotReserve = 5 %` et `demande de volume persistant = 5 Gio`, la taille totale du volume est de 5,79 Gio et la taille disponible est de 5,5 Gio. `volume show` La commande doit 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_134adb8e6d		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 minimaux

Les exemples suivants montrent des configurations de base qui laissent la plupart des paramètres par défaut. C'est la façon la plus simple de définir un back-end.



Si vous utilisez Amazon FSX sur NetApp ONTAP avec Astra Trident, nous vous recommandons de spécifier des noms DNS pour les LIF au lieu d'adresses IP.

#### Exemple de SAN ONTAP

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

```
---
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 d'économie SAN ONTAP

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

#### 1. exemple

Vous pouvez configurer le back-end pour éviter de devoir mettre à jour manuellement la définition du back-end après le basculement et le rétablissement pendant "[RéPLICATION ET RESTAURATION DES SVM](#)".

Pour un basculement et un rétablissement transparents, préciser le SVM en utilisant `managementLIF` et omettre les `dataLIF` paramètres et `svm`. Par exemple :

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

### Exemple d'authentification basée sur un certificat

Dans cet exemple de configuration de base `clientCertificate`, `clientPrivateKey`, et `trustedCACertificate` (facultatif, si vous utilisez une autorité de certification approuvée) sont renseignés `backend.json` et prennent respectivement les valeurs codées en base64 du certificat client, de la clé privée et du certificat de l'autorité de certification approuvée.

```
---  
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: ZXROZXJwYXB...ICMgJ3BhcGVyc2  
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX  
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz
```

## Exemples CHAP bidirectionnels

Ces exemples créent un back-end avec `useCHAP` défini sur `true`.

### Exemple CHAP de SAN ONTAP

```
---  
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: rxqigXgkesIpwxyz  
chapTargetUsername: iJF4heBRT0TCwxyz  
chapUsername: uh2aNCLSd6cNwxyz  
username: vsadmin  
password: <password>
```

### Exemple CHAP d'économie SAN ONTAP

```
---  
version: 1  
storageDriverName: ontap-san-economy  
managementLIF: 10.0.0.1  
svm: svm_iscsi_eco  
useCHAP: true  
chapInitiatorSecret: cl9qxIm36DKyawxy  
chapTargetInitiatorSecret: rxqigXgkesIpwxyz  
chapTargetUsername: iJF4heBRT0TCwxyz  
chapUsername: uh2aNCLSd6cNwxyz  
username: vsadmin  
password: <password>
```

## Exemple NVMe/TCP

Un SVM doit être configuré avec NVMe sur votre back-end ONTAP. Il s'agit d'une configuration back-end 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 configuration back-end avec nomTemplate

```
---  
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}}_{{.volume.R  
equestName}}"  
},  
"labels": {"cluster": "ClusterA", "PVC":  
"{{.volume.Namespace}}_{{.volume.RequestName}}"}  
}
```

## Exemples de systèmes back-end avec pools virtuels

Dans ces exemples de fichiers de définition back-end, des valeurs par défaut spécifiques sont définies pour tous les pools de stockage, comme spaceReserve aucun, spaceAllocation faux et encryption faux. Les pools virtuels sont définis dans la section stockage.

ASTRA Trident définit les étiquettes de provisionnement dans le champ « Commentaires ». Les commentaires sont définis sur le FlexVol. Astra Trident copie toutes les étiquettes présentes sur un pool virtuel vers le volume de stockage lors du provisionnement. Pour plus de commodité, les administrateurs du stockage peuvent définir des étiquettes par pool virtuel et les volumes de groupe par étiquette.

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

## Exemple de 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'
```

## Mappage des systèmes back-end aux classes de stockage

Les définitions de classe de stockage suivantes font référence à la [Exemples de systèmes back-end avec pools virtuels](#). En utilisant ce `parameters.selector` champ, chaque classe de stockage indique quels pools virtuels peuvent être utilisés pour héberger un volume. Les aspects définis dans le pool virtuel sélectionné seront définis pour le volume.

- La `protection-gold` classe de stockage est mappée sur le premier pool virtuel du `ontap-san` back-end. Il s'agit du seul pool offrant une protection de niveau Gold.

```

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

```

- La `protection-not-gold` classe de stockage sera mappée sur le deuxième et le troisième pool virtuel du `ontap-san` back-end. 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"

```

- La `app-mysqldb` classe de stockage sera mappée sur le troisième pool virtuel du `ontap-san-economy` back-end. Il s'agit du seul pool offrant la configuration du 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=mysqldb"
  fsType: "ext4"

```

- La `protection-silver-creditpoints-20k` classe de stockage sera mappée sur le second pool virtuel du `ontap-san` back-end. Il s'agit de la seule piscine 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"

```

- La `creditpoints-5k` classe de stockage est mappée sur le troisième pool virtuel du `ontap-san` back-end et le quatrième pool virtuel du `ontap-san-economy` back-end. Il s'agit des seules offres de pool avec 5000 points de crédit.

```

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

```

- La `my-test-app-sc` classe de stockage est mappée sur le `testAPP` pool virtuel du `ontap-san` pilote avec `sanType: nvme`. C'est la seule offre de piscine `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"

```

Astra Trident va décider du pool virtuel sélectionné et s'assurer que les besoins en stockage sont satisfaits.

## Pilotes NAS de ONTAP

### Présentation du pilote NAS ONTAP

Découvrez comment configurer un back-end ONTAP avec les pilotes ONTAP et NAS Cloud Volumes ONTAP.

## Détails du pilote NAS ONTAP

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



Si vous utilisez Astra Control pour la protection, la restauration et la mobilité, lisez [Compatibilité du pilote Astra Control](#) .

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

## Compatibilité du pilote Astra Control

ASTRA Control offre une protection transparente, une reprise d'activité et une mobilité (déplacement de volumes entre les clusters Kubernetes) pour les volumes créés avec les `ontap-nas` pilotes , `ontap-nas-flexgroup` et `ontap-san`. Voir "[Conditions préalables à la réPLICATION d'Astra Control](#)" pour plus de détails.



- À utiliser `ontap-san-economy` uniquement si le nombre d'utilisations de volume persistant doit être supérieur à "[Limites de volume ONTAP prises en charge](#)".
- À utiliser `ontap-nas-economy` uniquement si le nombre d'utilisations de volume persistant doit être supérieur à et si "[Limites de volume ONTAP prises en charge](#)" le `ontap-san-economy` pilote ne peut pas être utilisé.
- N'utilisez pas cette option `ontap-nas-economy` si vous prévoyez d'avoir besoin de protection des données, de reprise après incident ou de mobilité.

## Autorisations utilisateur

ASTRA Trident attend d'être exécuté en tant qu'administrateur ONTAP ou SVM, généralement avec l' `admin` `utilisateur du cluster ou un utilisateur SVM, ou un utilisateur avec un `vsadmin` nom différent qui a le même rôle.

Pour les déploiements Amazon FSX pour NetApp ONTAP, Astra Trident prévoit d'être exécutée en tant qu'administrateur ONTAP ou SVM, en utilisant l'utilisateur du cluster ou un utilisateur SVM, ou en tant qu' `fsxadmin` `utilisateur `vsadmin` avec un nom différent et ayant le même rôle. `fsxadmin` L'utilisateur est un remplaçant limité pour l'utilisateur `admin` du cluster.



Si vous utilisez le `limitAggregateUsage` paramètre, les autorisations d'administration du cluster sont requises. Lors de l'utilisation d'Amazon FSX pour NetApp ONTAP avec Astra Trident, le `limitAggregateUsage` paramètre ne fonctionnera pas avec les `vsadmin` comptes d'utilisateur et `fsxadmin`. L'opération de configuration échoue si vous spécifiez ce paramètre.

S'il est possible de créer au sein de ONTAP un rôle plus restrictif qu'un pilote Trident peut utiliser, nous ne le recommandons pas. La plupart des nouvelles versions de Trident appellent des API supplémentaires qui devront être prises en compte, ce qui complique les mises à niveau et risque d'erreurs.

## Préparez la configuration d'un système back-end avec les pilotes NAS ONTAP

Découvrez les exigences, les options d'authentification et les règles d'exportation pour la configuration d'un back-end ONTAP avec des pilotes NAS ONTAP.

### De formation

- Pour tous les systèmes back-end ONTAP, Astra Trident requiert au moins un agrégat affecté à la SVM.
- Vous pouvez exécuter plusieurs pilotes et créer des classes de stockage qui pointent vers l'un ou l'autre. Par exemple, vous pouvez configurer une classe Gold qui utilise le `ontap-nas` pilote et une classe Bronze qui utilise celui-ci `ontap-nas-economy`.
- Tous vos nœuds workers Kubernetes doivent avoir installé les outils NFS appropriés. Voir "[Ici](#)" pour plus de détails.
- Astra Trident prend en charge les volumes SMB montés sur des pods qui s'exécutent uniquement sur des nœuds Windows. Voir [Préparez-vous au provisionnement des volumes SMB](#) pour plus de détails.

### Authentifiez le back-end ONTAP

Astra Trident propose deux modes d'authentification d'un système back-end ONTAP.

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

Vous pouvez mettre à jour les systèmes back-end existants pour passer d'une méthode basée sur les identifiants à une méthode basée sur les certificats. Toutefois, une seule méthode d'authentification est prise en charge à la fois. Pour passer à une méthode d'authentification différente, vous devez supprimer la méthode existante de la configuration `backend`.

 Si vous tentez de fournir **les deux identifiants et les certificats**, la création du back-end échoue 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 informations d'identification

Astra Trident nécessite les identifiants d'un administrateur SVM-scoped/cluster-scoped pour communiquer avec le ONTAP backend. Il est recommandé d'utiliser des rôles standard prédéfinis tels que `admin` ou `vsadmin`. Il est ainsi possible d'assurer une compatibilité avec les futures versions d'ONTAP et d'exposer les API de fonctionnalités à utiliser avec les futures versions d'Astra Trident. Un rôle de connexion de sécurité personnalisé peut être créé et utilisé avec Astra Trident, mais il n'est pas recommandé.

Voici un exemple de définition du back-end :

## YAML

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

## JSON

```
{  
  "version": 1,  
  "backendName": "ExampleBackend",  
  "storageDriverName": "ontap-nas",  
  "managementLIF": "10.0.0.1",  
  "dataLIF": "10.0.0.2",  
  "svm": "svm_nfs",  
  "username": "vsadmin",  
  "password": "password"  
}
```

Gardez à l'esprit que la définition du back-end est le seul endroit où les informations d'identification sont stockées en texte brut. Une fois le système backend créé, les noms d'utilisateur/mots de passe sont codés avec Base64 et stockés sous forme de secrets Kubernetes. La création/la conversion d'un back-end est la seule étape qui nécessite la connaissance des informations d'identification. Il s'agit donc d'une opération uniquement administrative, qui doit être effectuée par l'administrateur Kubernetes/du stockage.

### Activez l'authentification basée sur les certificats

Les systèmes back-end, nouveaux et existants, peuvent utiliser un certificat et communiquer avec le système back-end ONTAP. Trois paramètres sont requis dans la définition du back-end.

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

Un flux de travail type comprend 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 pour qu'il s'authentifie.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=vsadmin"
```

2. Ajoutez un certificat d'autorité de certification de confiance au cluster ONTAP. Il se peut déjà que l'administrateur de stockage gère cet espace. Ignorer si aucune autorité de certification approuvée 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 (à partir de l'étape 1) sur le cluster ONTAP.

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

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

```
security login create -user-or-group-name vsadmin -application ontapi  
-authentication-method cert -vserver <vserver-name>  
security login create -user-or-group-name vsadmin -application http  
-authentication-method cert -vserver <vserver-name>
```

5. Testez l'authentification à l'aide d'un certificat généré. Remplacer <ONTAP Management LIF> et <vserver name> par Management LIF IP et SVM name. Vous devez vous assurer que la stratégie de service de la LIF est définie sur default-data-management.

```
curl -X POST -Lk https://<ONTAP-Management-LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key  
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp  
xmlns="http://www.netapp.com/filer/admin" version="1.21"  
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Encodez le certificat, la clé et le certificat CA 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 back-end à l'aide des valeurs obtenues à partir de l'étape précédente.

```
cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkeeee...Vaaallluuuueeee",
  "clientPrivateKey": "LS0tFAKE...0VaLuES0tLS0K",
  "storagePrefix": "myPrefix_"
}

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

## Mettre à jour les méthodes d'authentification ou faire pivoter les informations d'identification

Vous pouvez mettre à jour un back-end existant pour utiliser une méthode d'authentification différente ou pour faire pivoter leurs informations d'identification. Cela fonctionne de deux manières : les systèmes back-end qui utilisent le nom d'utilisateur/mot de passe peuvent être mis à jour pour utiliser des certificats ; les systèmes back-end qui utilisent des certificats peuvent être mis à jour en fonction du nom d'utilisateur/mot de passe. Pour ce faire, vous devez supprimer la méthode d'authentification existante et ajouter la nouvelle méthode d'authentification. Utilisez ensuite le fichier backend.json mis à jour contenant les paramètres requis pour exécuter `tridentctl update backend`.

```

cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "password",
  "storagePrefix": "myPrefix_"
}

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

```

**i** Lors de la rotation des mots de passe, l'administrateur du stockage doit d'abord mettre à jour le mot de passe de l'utilisateur sur ONTAP. Cette opération est suivie d'une mise à jour du back-end. Lors de la rotation de certificats, plusieurs certificats peuvent être ajoutés à l'utilisateur. Le back-end est ensuite mis à jour pour utiliser le nouveau certificat, en suivant lequel l'ancien certificat peut être supprimé du cluster ONTAP.

La mise à jour d'un back-end n'interrompt pas l'accès aux volumes qui ont déjà été créés, et n'a aucun impact sur les connexions de volume effectuées après. Une mise à jour réussie indique qu'Astra Trident peut communiquer avec le système back-end ONTAP et gérer les opérations de volumes à venir.

### Gestion des règles d'exportation NFS

Astra Trident utilise les règles d'exportation NFS pour contrôler l'accès aux volumes qu'il provisionne.

Astra Trident propose deux options pour l'utilisation des règles d'exportation :

- Astra Trident peut gérer la règle d'exportation de manière dynamique. Dans ce mode de fonctionnement, l'administrateur du stockage spécifie une liste de blocs CIDR qui représentent les adresses IP admissibles. Astra Trident ajoute automatiquement des adresses IP de nœud qui font partie de ces plages à la règle d'exportation. En outre, lorsqu'aucun CIDRS n'est spécifié, toute adresse IP unicast globale trouvée sur les nœuds est ajoutée à la règle d'exportation.

- Les administrateurs du stockage peuvent créer une export-policy et ajouter des règles manuellement. Astra Trident utilise la export policy par défaut, sauf si un nom différent de export policy est spécifié dans la configuration.

## Gérez les règles d'exportation de manière dynamique

ASTRA Trident permet de gérer dynamiquement les règles d'exportation pour les systèmes ONTAP back-end. Cela permet à l'administrateur du stockage de spécifier un espace d'adresse autorisé pour les adresses IP du nœud de travail, au lieu de définir manuellement des règles explicites. Il simplifie considérablement la gestion des export policy ; les modifications apportées à l'export policy ne nécessitent plus d'intervention manuelle sur le cluster de stockage. De plus, cela permet de limiter l'accès au cluster de stockage uniquement aux nœuds workers dont les adresses IP sont comprises dans la plage spécifiée, ce qui prend en charge une gestion automatisée et précise.

 N'utilisez pas NAT (Network Address Translation) lorsque vous utilisez des stratégies d'exportation dynamiques. Avec NAT, le contrôleur de stockage voit l'adresse NAT front-end et non l'adresse IP réelle de l'hôte. L'accès sera donc refusé lorsqu'aucune correspondance n'est trouvée dans les règles d'exportation.

### Exemple

Deux options de configuration doivent être utilisées. Voici un exemple de définition de back-end :

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

 Lorsque vous utilisez cette fonctionnalité, vous devez vous assurer que la jonction root dans votre SVM possède une export policy précédemment créée avec une règle d'exportation qui autorise le bloc CIDR (comme la export policy par défaut) du nœud. Suivez toujours les bonnes pratiques recommandées par NetApp pour dédier un SVM à Astra Trident.

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

- `autoExportPolicy` est défini sur `true`. Cela indique qu'Astra Trident créera une export policy pour le `svm1` SVM et gérera l'ajout et la suppression de règles utilisant des `autoExportCIDRs` blocs d'adresses. Par exemple, un back-end avec UUID `403b5326-8482-40db-96d0-d83fb3f4daec` et `autoExportPolicy` set to `true` crée une export policy nommée `trident-403b5326-8482-40db-96d0-d83fb3f4daec` sur le SVM.
- `autoExportCIDRs` contient une liste de blocs d'adresses. Ce champ est facultatif et il prend par défaut la valeur `["0.0.0.0/", ":/0"]`. S'il n'est pas défini, Astra Trident ajoute toutes les adresses de diffusion

individuelle à périmètre global présentes sur les nœuds du worker.

Dans cet exemple, l' 192.168.0.0/24` espace d'adresse est fourni. Cela indique que les adresses IP des nœuds Kubernetes qui appartiennent à cette plage d'adresse seront ajoutées à la règle d'exportation créée par Astra Trident. Lorsque Astra Trident enregistre un nœud sur lequel il s'exécute, il récupère les adresses IP du nœud et les compare aux blocs d'adresse fournis dans `autoExportCIDRs. après le filtrage des adresses IP, Astra Trident crée des règles d'export pour les adresses IP du client qu'il découvre, avec une règle pour chaque nœud qu'il identifie.

Vous pouvez mettre à jour autoExportPolicy et autoExportCIDRs pour les systèmes back-end une fois que vous les avez créés. Vous pouvez ajouter de nouveaux rapports CIDR pour un back-end qui est géré automatiquement ou supprimé des rapports CIDR existants. Faites preuve de prudence lors de la suppression des CIDR pour vous assurer que les connexions existantes ne sont pas tombées. Vous pouvez également choisir de désactiver autoExportPolicy pour un backend et de revenir à une export policy créée manuellement. Pour cela, vous devrez définir le exportPolicy paramètre dans votre configuration back-end.

Une fois qu'Astra Trident a créé ou mis à jour un back-end, vous pouvez vérifier le back-end à l'aide de tridentctl ou du CRD correspondant tridentbackend :

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

Lorsque des nœuds sont ajoutés à un cluster Kubernetes et enregistrés avec le contrôleur Astra Trident, les politiques d'exportation des systèmes back-end existants sont mises à jour (à condition qu'elles relèvent de la plage d'adresses spécifiée dans autoExportCIDRs pour le système back-end).

Lorsqu'un nœud est retiré, Astra Trident vérifie tous les systèmes back-end en ligne afin de supprimer la règle d'accès du nœud. En supprimant cette IP de nœud des règles d'exportation des systèmes back-end gérés, Astra Trident empêche les montages erratiques, à moins que cette adresse IP soit réutilisée par un nouveau nœud du cluster.

Pour les systèmes back-end antérieurs, la mise à jour du back-end avec `tridentctl update backend` garantit qu'Astra Trident gère automatiquement les règles d'exportation. Cela créera une nouvelle export policy nommée après que l'UUID du back-end et les volumes présents sur le back-end utiliseront la nouvelle export policy créée lorsqu'ils sont à nouveau montés.

 La suppression d'un back-end avec des règles d'exportation gérées automatiquement supprimera l'export policy créée de manière dynamique. Si le back-end est recréé, il est traité comme un nouveau backend et entraîne la création d'une nouvelle export policy.

Si l'adresse IP d'un nœud actif est mise à jour, vous devez redémarrer le pod Astra Trident sur le nœud. Astra Trident va ensuite mettre à jour la règle d'exportation pour les systèmes back-end qu'il gère pour tenir compte de ce changement d'IP.

#### Préparez-vous au provisionnement des volumes SMB

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

 Vous devez configurer les protocoles NFS et SMB/CIFS au SVM pour créer un `ontap-nas-economy` volume SMB pour ONTAP sur site. La configuration de l'un de ces protocoles entraîne l'échec de la création du volume SMB.

#### Avant de commencer

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

- Cluster Kubernetes avec un nœud de contrôleur Linux et au moins un nœud worker Windows exécutant Windows Server 2022. Astra Trident prend en charge les volumes SMB montés sur des pods qui s'exécutent uniquement sur des nœuds Windows.
- Au moins un secret Astra Trident contenant vos identifiants Active Directory. Pour générer un secret `smbcreds`:

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

- Un proxy CSI configuré en tant que service Windows. Pour configurer un `csi-proxy`, reportez-vous "[GitHub : proxy CSI](#)" à la section ou "[GitHub : proxy CSI pour Windows](#)" pour les nœuds Kubernetes s'exécutant sous Windows.

#### Étapes

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



Les partages SMB sont requis pour Amazon FSX pour ONTAP.

Vous pouvez créer les partages d'administration SMB de deux manières, soit à l'aide du "[Console de gestion Microsoft](#)" composant logiciel enfichable dossiers partagés, soit à l'aide de l'interface de ligne de commande ONTAP. Pour créer les partages SMB à l'aide de l'interface de ligne de commandes ONTAP :

- a. Si nécessaire, créez la structure du chemin d'accès au répertoire pour le partage.

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

- b. Créer un partage SMB associé au SVM spécifié :

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

- c. Vérifiez que le partage a été créé :

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



Reportez-vous "[Créez un partage SMB](#)" à pour plus de détails.

2. Lors de la création du back-end, vous devez configurer le suivant pour spécifier les volumes SMB. Pour toutes les options de configuration du back-end FSX for ONTAP, reportez-vous à "["Exemples et options de configuration de FSX pour ONTAP"](#)" la section .

Paramètre	Description	Exemple
smbShare	Vous pouvez indiquer l'un des éléments suivants : le nom d'un partage SMB créé à l'aide de la console de gestion Microsoft ou de l'interface de ligne de commandes ONTAP ; un nom permettant à Astra Trident de créer le partage SMB. Vous pouvez également laisser vide le paramètre pour empêcher l'accès à un partage commun aux volumes. Ce paramètre est facultatif pour les ONTAP sur site. Ce paramètre est requis pour Amazon FSX pour les systèmes back-end ONTAP et ne peut pas être vide.	smb-share
nasType	<b>Doit être réglé sur smb.</b> Si nul, la valeur par défaut est nfs .	smb
securityStyle	Style de sécurité pour les nouveaux volumes. <b>Doit être défini sur ntfs ou mixed pour les volumes SMB.</b>	ntfs Ou mixed pour les volumes SMB
unixPermissions	Mode pour les nouveaux volumes. <b>Doit rester vide pour les volumes SMB.</b>	« »

## Options et exemples de configuration du NAS ONTAP

Découvrez comment créer et utiliser des pilotes NAS ONTAP avec votre installation Astra Trident. Cette section fournit des exemples de configuration back-end et des détails sur le mappage des systèmes back-end aux classes de stockage.

## Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDrive rName	Nom du pilote de stockage	« ontap-nas », « ontap-nas-economy », « ontap-nas-flexgroup », « ontap-san », « ontap-san-economy »
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + dataLIF
managementLIF	Adresse IP d'un cluster ou LIF de gestion De SVM Un nom de domaine complet (FQDN) peut être spécifié. Peut être défini pour utiliser des adresses IPv6 si Astra Trident a été installé à l'aide de l'indicateur IPv6. Les adresses IPv6 doivent être définies entre crochets, par exemple [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Pour un basculement MetroCluster transparent, consultez le <a href="#">[mcc-best]</a> .	« 10.0.0.1 », « [2001:1234:abcd::fefe] »
dataLIF	Adresse IP de la LIF de protocole. Nous vous recommandons de spécifier dataLIF. Si elle n'est pas fournie, Astra Trident extrait les LIF 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. Peut être modifié après le réglage initial. Reportez-vous à la . Peut être défini pour utiliser des adresses IPv6 si Astra Trident a été installé à l'aide de l'indicateur IPv6. Les adresses IPv6 doivent être définies entre crochets, par exemple [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. <b>Omettre pour MetroCluster.</b> Voir la <a href="#">[mcc-best]</a> .	Adresse spécifiée ou dérivée d'un SVM, si non spécifiée (non recommandé)
svm	Machine virtuelle de stockage à utiliser <b>omet pour MetroCluster.</b> Voir la <a href="#">[mcc-best]</a> .	Dérivé si un SVM managementLIF est spécifié
autoExportPo licy	Activer la création et la mise à jour automatiques des règles d'exportation [booléennes]. À l'aide autoExportPolicy des options et autoExportCIDRs, Astra Trident peut gérer automatiquement les règles d'export.	faux
autoExportCI DRs	Liste des CIDR permettant de filtrer les adresses IP des nœuds Kubernetes par rapport à lorsque autoExportPolicy est activé. À l'aide autoExportPolicy des options et autoExportCIDRs, Astra Trident peut gérer automatiquement les règles d'export.	["0.0.0.0/0", ":/0"]

Paramètre	Description	Valeur par défaut
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	« »
clientCertificate	Valeur encodée en Base64 du certificat client. Utilisé pour l'authentification par certificat	« »
clientPrivateKey	Valeur encodée en Base64 de la clé privée du client. Utilisé pour l'authentification par certificat	« »
trustedCACertificate	Valeur encodée en Base64 du certificat CA de confiance. Facultatif. Utilisé pour l'authentification par certificat	« »
username	Nom d'utilisateur pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants	
password	Mot de passe pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants	
storagePrefix	Préfixe utilisé pour le provisionnement des nouveaux volumes dans la SVM. Ne peut pas être mis à jour une fois que vous l'avez défini	« trident »
limitAggregateUsage	Echec du provisionnement si l'utilisation est supérieure à ce pourcentage. <b>Ne s'applique pas à Amazon FSX pour ONTAP</b>	« » (non appliqué par défaut)
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur. Limite également la taille maximale des volumes gérés pour les qtrees et les LUN, et qtreesPerFlexvol permet de personnaliser le nombre maximal de qtrees par FlexVol.	« » (non appliqué par défaut)
lunsPerFlexvol	Nombre maximal de LUN par FlexVol, doit être compris dans la plage [50, 200]	« 100 »
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, {"api":false, "method":true} n'utilisez debugTraceFlags que si vous effectuez un dépannage et que vous avez besoin d'un viddage de journal détaillé.	nul
nasType	Configurez la création de volumes NFS ou SMB. Les options sont nfs, smb ou NULL. La valeur null par défaut sur les volumes NFS.	nfs

Paramètre	Description	Valeur par défaut
nfsMountOptions	Liste des options de montage NFS séparée par des virgules. Les options de montage des volumes Kubernetes persistants sont généralement spécifiées dans les classes de stockage, mais si aucune option de montage n'est spécifiée dans une classe de stockage, Astra Trident utilisera les options de montage spécifiées dans le fichier de configuration du système back-end. Si aucune option de montage n'est spécifiée dans la classe de stockage ou le fichier de configuration, Astra Trident ne définit aucune option de montage sur un volume persistant associé.	« »
qtreesPerFlexVol	Nombre maximal de qtrees par FlexVol, qui doit être compris dans la plage [50, 300]	« 200 »
smbShare	Vous pouvez indiquer l'un des éléments suivants : le nom d'un partage SMB créé à l'aide de la console de gestion Microsoft ou de l'interface de ligne de commandes ONTAP ; un nom permettant à Astra Trident de créer le partage SMB. Vous pouvez également laisser vide le paramètre pour empêcher l'accès à un partage commun aux volumes. Ce paramètre est facultatif pour les ONTAP sur site. Ce paramètre est requis pour Amazon FSX pour les systèmes back-end ONTAP et ne peut pas être vide.	smb-share
useREST	Paramètre booléen pour utiliser les API REST de ONTAP. <code>useREST</code> Lorsqu'il est défini sur <code>true</code> , Astra Trident utilisera les API REST ONTAP pour communiquer avec le back-end. Lorsqu'il est défini sur <code>false</code> , Astra Trident utilisera les appels ZAPI ONTAP pour communiquer avec le back-end. Cette fonctionnalité requiert ONTAP 9.11.1 et versions ultérieures. En outre, le rôle de connexion ONTAP utilisé doit avoir accès à l' <code>ontap application</code> . Ceci est satisfait par les rôles et prédéfinis <code>vsadmin</code> <code>cluster-admin</code> . Depuis la version Astra Trident 24.06 et ONTAP 9.15.1 ou version ultérieure, <code>useREST</code> est défini sur <code>true</code> par défaut. Passez <code>useREST</code> à <code>false</code> pour utiliser les appels ZAPI ONTAP.	<code>true</code> Pour ONTAP 9.15.1 ou version ultérieure, sinon <code>false</code> .
limitVolumePoolSize	Taille de FlexVol maximale requise lors de l'utilisation de qtrees dans le back-end ONTAP-nas-Economy.	« » (non appliqué par défaut)

#### Options de configuration back-end pour les volumes de provisionnement

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

Paramètre	Description	Valeur par défaut
spaceAllocation	Allocation d'espace pour les LUN	« vrai »
spaceReserve	Mode de réservation d'espace ; « aucun » (fin) ou « volume » (épais)	« aucun »
snapshotPolicy	Règle Snapshot à utiliser	« aucun »
qosPolicy	QoS policy group à affecter pour les volumes créés. Choisissez une de qosPolicy ou adaptiveQosPolicy par pool de stockage/back-end	« »
adaptiveQosPolicy	Groupe de règles de QoS adaptative à attribuer aux volumes créés. Choisissez une de qosPolicy ou adaptiveQosPolicy par pool de stockage/back-end. Non pris en charge par l'économie ontap-nas.	« »
snapshotReserve	Pourcentage de volume réservé pour les snapshots	« 0 » si snapshotPolicy est « aucun », sinon « »
splitOnClone	Séparer un clone de son parent lors de sa création	« faux »
encryption	Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume. La valeur par défaut est <code>false</code> . Pour utiliser cette option, NVE doit être sous licence et activé sur le cluster. Si NAE est activé sur le back-end, tous les volumes provisionnés dans Astra Trident seront activés par NAE. Pour plus d'informations, reportez-vous à la section : <a href="#">"Fonctionnement d'Astra Trident avec NVE et NAE"</a> .	« faux »
tieringPolicy	Règle de hiérarchisation à utiliser « aucun »	« Snapshot uniquement » pour la configuration SVM-DR antérieure à ONTAP 9.5
unixPermissions	Mode pour les nouveaux volumes	« 777 » pour les volumes NFS ; vide (non applicable) pour les volumes SMB
snapshotDir	Contrôle l'accès au <code>.snapshot</code> répertoire	« faux »
exportPolicy	Export policy à utiliser	« par défaut »
securityStyle	Style de sécurité pour les nouveaux volumes. Prise en charge et <code>unix</code> styles de sécurité par NFS mixed. Prise en charge SMB <code>mixed</code> et <code>ntfs</code> styles de sécurité.	NFS par défaut est <code>unix</code> . SMB la valeur par défaut est <code>ntfs</code> .
nameTemplate	Modèle pour créer des noms de volume personnalisés.	« »

 Avec Astra Trident, les groupes de règles de QoS doivent être utilisés avec ONTAP 9.8 ou version ultérieure. Il est recommandé d'utiliser un groupe de règles de qualité de service non partagé et de s'assurer que le groupe de règles est appliqué à chaque composant individuellement. Un groupe de règles de QoS partagé appliquera le plafond du débit total de toutes les charges de travail.

## Exemples de provisionnement de volumes

Voici un exemple avec des valeurs par défaut définies :

```
---
version: 1
storageDriverName: ontap-nas
backendName: customBackendName
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
labels:
  k8scluster: dev1
  backend: dev1-nasbackend
svm: trident_svm
username: cluster-admin
password: <password>
limitAggregateUsage: 80%
limitVolumeSize: 50Gi
nfsMountOptions: nfsvers=4
debugTraceFlags:
  api: false
  method: true
defaults:
  spaceReserve: volume
  qosPolicy: premium
  exportPolicy: myk8scluster
  snapshotPolicy: default
  snapshotReserve: '10'
```

Pour `ontap-nas` et `ontap-nas-flexgroups`, Astra Trident utilise désormais un nouveau calcul pour s'assurer que le FlexVol est correctement dimensionné avec le pourcentage `snapshotReserve` et le volume persistant. Lorsque l'utilisateur demande de volume persistant, Astra Trident crée le FlexVol d'origine avec plus d'espace en utilisant le nouveau calcul. Ce calcul garantit que l'utilisateur reçoit l'espace inscriptible demandé dans la demande de volume persistant et qu'il ne dispose pas d'un espace minimal par rapport à ce qu'il a demandé. Avant le 21.07, lorsque l'utilisateur demande une demande de volume persistant (par exemple, 5 Gio), et le `snapshotReserve` à 50 %, ils ne bénéficient que d'un espace inscriptible de 2,5 Gio. En effet, ce que l'utilisateur a demandé est le volume entier et est un pourcentage de ce volume `snapshotReserve`. Dans Trident 21.07, l'utilisateur demande l'espace inscriptible, et Astra Trident définit le `snapshotReserve` nombre comme le pourcentage du volume dans son ensemble. Cela ne s'applique pas à `ontap-nas-economy`. Voir l'exemple suivant pour voir comment cela fonctionne :

Le calcul est le suivant :

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

Pour les snapshots Reserve = 50 %, et demande en volume PVC = 5 Gio, la taille totale du volume est  $2/0,5 =$

10 Gio et la taille disponible est de 5 Gio, ce que l'utilisateur a demandé dans la demande de demande de volume persistant. `volume show` La commande doit afficher des résultats similaires à cet exemple :

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

Les systèmes back-end des installations précédentes provisionnent les volumes comme expliqué ci-dessus lors de la mise à niveau d'Astra Trident. Pour les volumes que vous avez créés avant la mise à niveau, vous devez redimensionner leurs volumes afin que la modification puisse être observée. Par exemple, une demande de volume persistant de 2 Gio associée à `snapshotReserve=50` la précédente a donné lieu à un volume qui fournit 1 Gio d'espace inscriptible. Le redimensionnement du volume à 3 Gio, par exemple, fournit l'application avec 3 Gio d'espace inscriptible sur un volume de 6 Gio.

#### Exemples de configuration minimaux

Les exemples suivants montrent des configurations de base qui laissent la plupart des paramètres par défaut. C'est la façon la plus simple de définir un back-end.



Si vous utilisez Amazon FSX sur NetApp ONTAP avec Trident, nous vous recommandons de spécifier des noms DNS pour les LIF au lieu d'adresses IP.

#### Exemple d'économie NAS ONTAP

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

#### Exemple de FlexGroup NAS ONTAP

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

## Exemple MetroCluster

Vous pouvez configurer le back-end pour éviter de devoir mettre à jour manuellement la définition du back-end après le basculement et le rétablissement pendant "[RéPLICATION ET RESTAURATION DES SVM](#)".

Pour un basculement et un rétablissement transparents, préciser le SVM en utilisant `managementLIF` et omettre les `dataLIF` paramètres et `svm`. Par exemple :

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

## Exemple de volumes SMB

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

## Exemple d'authentification basée sur un certificat

Il s'agit d'un exemple de configuration back-end minimale. `clientCertificate`, `clientPrivateKey` Et `trustedCACertificate` (facultatif, si vous utilisez une autorité de certification approuvée) sont renseignés `backend.json` et prennent respectivement les valeurs codées en base64 du certificat client, de la clé privée et du certificat de l'autorité de certification approuvée.

```
---  
version: 1  
backendName: DefaultNASBackend  
storageDriverName: ontap-nas  
managementLIF: 10.0.0.1  
dataLIF: 10.0.0.15  
svm: nfs_svm  
clientCertificate: ZXR0ZXJwYXB...ICMgJ3BhcGVyc2  
clientPrivateKey: vciwKIyAgZG...0cnksIGRlc2NyaX  
trustedCACertificate: zcyBbaG...b3Igb3duIGNsYXNz  
storagePrefix: myPrefix_
```

## Exemple de règle d'export automatique

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

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

## Exemple d'adresses IPv6

Cet exemple illustre managementLIF l'utilisation d'une adresse IPv6.

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

## Exemple d'Amazon FSX pour ONTAP avec des volumes SMB

Le smbShare paramètre est requis pour FSX for ONTAP utilisant des volumes SMB.

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

## Exemple de configuration back-end avec nomTemplate

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

## Exemples de systèmes back-end avec pools virtuels

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

ASTRA Trident définit les étiquettes de provisionnement dans le champ « Commentaires ». Les commentaires sont définis sur FlexVol pour ontap-nas ou FlexGroup pour ontap-nas-flexgroup. Astra Trident copie toutes les étiquettes présentes sur un pool virtuel vers le volume de stockage lors du provisionnement. Pour plus de commodité, les administrateurs du stockage peuvent définir des étiquettes par pool virtuel et les volumes de groupe par étiquette.

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

## Exemple de NAS ONTAP

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

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

## Exemple de FlexGroup NAS ONTAP

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

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

## Exemple d'économie NAS ONTAP

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

```
  encryption: 'false'  
  unixPermissions: '0775'
```

### Mappage des systèmes back-end aux classes de stockage

Les définitions de classe de stockage suivantes font référence [Exemples de systèmes back-end avec pools virtuels](#). En utilisant ce `parameters.selector` champ, chaque classe de stockage indique quels pools virtuels peuvent être utilisés pour héberger un volume. Les aspects définis dans le pool virtuel sélectionné seront définis pour le volume.

- La `protection-gold` classe de stockage est mappée sur le premier et le second pool virtuel du `ontap-nas-flexgroup` back-end. Il s'agit des seuls pools offrant une protection de niveau Gold.

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

- La `protection-not-gold` classe de stockage est mappée sur le troisième et le quatrième pool virtuel du `ontap-nas-flexgroup` back-end. Ce sont les seuls pools offrant un niveau de protection autre que l'or.

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

- La `app-mysqldb` classe de stockage est mappée sur le quatrième pool virtuel du `ontap-nas` back-end. Il s'agit du seul pool offrant la configuration du 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=mysqldb"
  fsType: "ext4"

```

- La protection-silver-creditpoints-20k classe de stockage sera mappée sur le troisième pool virtuel du ontap-nas-flexgroup back-end. Il s'agit de la seule piscine 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"

```

- La creditpoints-5k classe de stockage est mappée sur le troisième pool virtuel du ontap-nas back-end et sur le second pool virtuel du ontap-nas-economy back-end. Il s'agit des seules offres de pool avec 5000 points de crédit.

```

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

```

Astra Trident va décider du pool virtuel sélectionné et s'assurer que les besoins en stockage sont satisfaits.

#### **Mise à jour dataLIF après la configuration initiale**

Vous pouvez modifier la LIF de données après la configuration initiale en exécutant la commande suivante pour fournir le nouveau fichier JSON back-end avec la LIF de données mise à jour.

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

 Si des demandes de volume persistant sont associées à un ou plusieurs pods, tous les pods correspondants doivent être arrêtés, puis réintégrés dans le but de permettre la nouvelle LIF de données d'être effective.

## Amazon FSX pour NetApp ONTAP

### Utilisez Astra Trident avec Amazon FSX pour NetApp ONTAP

"Amazon FSX pour NetApp ONTAP" Est un service AWS entièrement géré qui permet aux clients de lancer et d'exécuter des systèmes de fichiers optimisés par le système d'exploitation du stockage NetApp ONTAP. La solution FSX pour ONTAP vous permet d'exploiter les fonctionnalités, les performances et les capacités d'administration de NetApp que vous connaissez bien, tout en profitant de la simplicité, de l'agilité, de la sécurité et de l'évolutivité du stockage de données sur AWS. FSX pour ONTAP prend en charge les fonctionnalités du système de fichiers ONTAP et les API d'administration.

Vous pouvez intégrer votre système de fichiers Amazon FSX pour NetApp ONTAP avec Astra Trident pour vous assurer que les clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS) peuvent provisionner des volumes persistants de bloc et de fichier sauvegardés par ONTAP.

Un système de fichiers est la ressource principale d'Amazon FSX, similaire à un cluster ONTAP sur site. Au sein de chaque SVM, vous pouvez créer un ou plusieurs volumes, qui sont des conteneurs de données qui stockent les fichiers et les dossiers dans votre système de fichiers. Avec Amazon FSX pour NetApp ONTAP, Data ONTAP sera fourni en tant que système de fichiers géré dans le cloud. Le nouveau type de système de fichiers est appelé **NetApp ONTAP**.

Avec Astra Trident avec Amazon FSX pour NetApp ONTAP, vous pouvez vous assurer que les clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS) peuvent provisionner des volumes persistants de bloc et de fichier sauvegardés par ONTAP.

### De formation

En outre "Exigences d'Astra Trident", pour intégrer FSX for ONTAP avec Astra Trident, vous avez besoin des éléments suivants :

- Un cluster Amazon EKS ou un cluster Kubernetes autogéré avec `kubectl` installé.
- Système de fichiers Amazon FSX for NetApp ONTAP et machine virtuelle de stockage (SVM) accessibles depuis les nœuds workers de votre cluster.
- Nœuds de travail préparés pour "[NFS ou iSCSI](#)".



Assurez-vous de suivre les étapes de préparation de nœud requises pour Amazon Linux et Ubuntu "[Images de machine Amazon](#)" (amis) en fonction de votre type d'ami EKS.

## Considérations

- Volumes SMB :
  - Les volumes SMB sont pris en charge à l'aide du `ontap-nas` pilote uniquement.
  - Les volumes SMB ne sont pas pris en charge par le module d'extension Astra Trident EKS.
  - Astra Trident prend en charge les volumes SMB montés sur des pods qui s'exécutent uniquement sur des nœuds Windows. Voir "["Préparez-vous au provisionnement des volumes SMB"](#)" pour plus de détails.
- Avant Astra Trident 24.02, les volumes créés sur des systèmes de fichiers Amazon FSX pour lesquels les sauvegardes automatiques sont activées ne pouvaient pas être supprimés par Trident. Pour éviter ce problème dans Astra Trident 24.02 ou version ultérieure, spécifiez `fsxFilesystemID`, `AWS`, `AWS apiRegion` `apikey` et `AWS secretKey` dans le fichier de configuration back-end pour AWS FSX pour ONTAP.



Si vous spécifiez un rôle IAM dans Astra Trident, vous pouvez omettre de spécifier explicitement les `apiRegion` champs, `apiKey` et `secretKey` dans Astra Trident. Pour plus d'informations, reportez-vous "["Exemples et options de configuration de FSX pour ONTAP"](#)" à .

## Authentification

Astra Trident propose deux modes d'authentification.

- Basé sur les informations d'identification (recommandé) : stocke les informations d'identification de manière sécurisée dans AWS secrets Manager. Vous pouvez utiliser `fsxadmin` l'utilisateur pour votre système de fichiers ou l' `vsadmin` utilisateur configuré pour votre SVM.



ASTRA Trident prévoit d'être exécuté en tant qu' `vsadmin` `utilisateur SVM ou en tant qu' `utilisateur avec un nom différent qui a le même rôle. Amazon FSX pour NetApp ONTAP a un `fsxadmin` `utilisateur qui remplace de façon limitée l'utilisateur du cluster ONTAP `admin`. Nous recommandons vivement d'utiliser `vsadmin` Astra Trident.

- Basé sur des certificats : Astra Trident communiquera avec le SVM sur votre système de fichiers FSX à l'aide d'un certificat installé sur votre SVM.

Pour plus d'informations sur l'activation de l'authentification, reportez-vous à la section authentification de votre type de pilote :

- "["Authentification NAS de ONTAP"](#)"
- "["Authentification SAN de ONTAP"](#)"

## Trouvez plus d'informations

- "["Documentation Amazon FSX pour NetApp ONTAP"](#)"
- "["Billet de blog sur Amazon FSX pour NetApp ONTAP"](#)"

## Créez un rôle IAM et un code secret AWS

Vous pouvez configurer les pods Kubernetes pour accéder aux ressources AWS en vous authentifiant en tant que rôle IAM AWS au lieu de fournir des informations d'identification

## AWS explicites.



Pour vous authentifier à l'aide d'un rôle IAM AWS, un cluster Kubernetes doit être déployé à l'aide d'EKS.

### Créez un secret AWS Secret Manager

Dans cet exemple, vous créez un secret AWS Secret Manager pour stocker les informations d'identification Astra Trident CSI :

```
aws secretsmanager create-secret --name trident-secret --description "Trident CSI credentials" --secret-string "{\"user\":\"vsadmin\", \"password\":\"<svmpassword>\"}"
```

### Créer une politique IAM

Les exemples suivants créent une politique IAM à l'aide de l'interface de ligne de commande AWS :

```
aws iam create-policy --policy-name AmazonFSxNCSIDriverPolicy --policy-document file://policy.json --description "This policy grants access to Trident CSI to FSxN and Secret manager"
```

### Fichier JSON de règles :

```

policy.json:
{
  "Statement": [
    {
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx>CreateVolume",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:UntagResource",
        "fsx:UpdateVolume",
        "fsx:TagResource",
        "fsx:DeleteVolume"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Resource": "arn:aws:secretsmanager:<aws-region>:<aws-account-
id>:secret:<aws-secret-manager-name>"
    }
  ],
  "Version": "2012-10-17"
}

```

### Créer un rôle IAM pour le compte de service

L'exemple suivant crée un rôle IAM pour le compte de service dans EKS :

```

eksctl create iamserviceaccount --name trident-controller --namespace trident
--cluster <my-cluster> --role-name <AmazonEKS_FSxN_CSI_DriverRole> --role-only
--attach-policy-arn arn:aws:iam::aws:policy/service-
role/AmazonFSxNCSIDriverPolicy --approve

```

### Installer Astra Trident

ASTRA Trident simplifie la gestion du stockage Amazon FSX pour NetApp ONTAP dans Kubernetes pour que vos développeurs et administrateurs puissent donner la priorité au déploiement d'applications.

Vous pouvez installer Astra Trident à l'aide de l'une des méthodes suivantes :

- Gouvernail

- Module complémentaire EKS

If you want to make use of the snapshot functionality, install the CSI snapshot controller add-on. Refer to <https://docs.aws.amazon.com/eks/latest/userguide/csi-snapshot-controller.html>.

### Installez Astra Trident via Helm

#### 1. Téléchargez le package d'installation d'Astra Trident

Le package d'installation d'Astra Trident contient tout ce dont vous avez besoin pour déployer l'opérateur Trident et installer Astra Trident. Téléchargez et extrayez la dernière version du programme d'installation d'Astra Trident à partir de la section des ressources sur GitHub.

```
wget https://github.com/NetApp/trident/releases/download/v24.06.0/trident-installer-24.06.0.tar.gz
tar -xf trident-installer-24.06.0.tar.gz
cd trident-installer
```

#### 2. Définissez les valeurs des indicateurs **cloud Provider** et **cloud Identity** à l'aide des variables d'environnement suivantes :

```
export CP="AWS"
export CI="'eks.amazonaws.com/role-arn:
arn:aws:iam::<accountID>:role/<AmazonEKS_FSnX_CSI_DriverRole>'"
```

L'exemple suivant installe Astra Trident et définit le `cloud-provider` drapeau sur `$CP`, et `cloud-identity` sur `$CI`:

```
helm install trident trident-operator-100.2406.0.tgz --set
cloudProvider=$CP --set cloudIdentity=$CI --namespace trident
```

Vous pouvez utiliser `helm list` la commande pour consulter les détails de l'installation tels que le nom, l'espace de noms, le graphique, l'état, la version de l'application et le numéro de révision.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14 14:31:22.463122
+0300 IDT	deployed	trident-operator-100.2406.1	24.06.1

## Installez Astra Trident via le module complémentaire EKS

Le module complémentaire Astra Trident EKS inclut les derniers correctifs de sécurité et de bogues, et il est validé par AWS pour fonctionner avec Amazon EKS. Le module complémentaire EKS vous permet de vous assurer de manière cohérente que vos clusters Amazon EKS sont sécurisés et stables et de réduire la quantité de travail à effectuer pour installer, configurer et mettre à jour des modules complémentaires.

### Prérequis

Vérifiez les points suivants avant de configurer le module complémentaire Astra Trident pour AWS EKS :

- Un compte de cluster Amazon EKS avec abonnement complémentaire
- Autorisations AWS sur AWS Marketplace :  
"aws-marketplace:ViewSubscriptions",  
"aws-marketplace:Subscribe",  
"aws-marketplace:Unsubscribe"
- Type ami : Amazon Linux 2 (AL2\_x86\_64) ou Amazon Linux 2 ARM (AL2\_ARM\_64)
- Type de nœud : AMD ou ARM
- Un système de fichiers Amazon FSX pour NetApp ONTAP

### Activez le module complémentaire Astra Trident pour AWS

## Groupe EKS

Les exemples de commandes suivants installent le module complémentaire Astra Trident EKS :

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v24.6.1-eksbuild  
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v24.6.1-eksbuild.1 (avec une version dédiée)
```



Lorsque vous configurez le paramètre facultatif `cloudIdentity`, assurez-vous de spécifier `cloudProvider` lors de l'installation de Trident à l'aide du module complémentaire EKS.

## Console de gestion

1. Ouvrez la console Amazon EKS à l'adresse <https://console.aws.amazon.com/eks/home#/clusters>.
2. Dans le volet de navigation de gauche, cliquez sur **clusters**.
3. Cliquez sur le nom du cluster pour lequel vous souhaitez configurer le module complémentaire NetApp Trident CSI.
4. Cliquez sur **Compléments**, puis cliquez sur **obtenir plus de modules complémentaires**.
5. Sur la page **S\*elect add-ons**, procédez comme suit :
  - a. Dans la section EKS-addons d'AWS Marketplace, cochez la case **Astra Trident by NetApp**.
  - b. Cliquez sur **Suivant**.
6. Sur la page **configurer les compléments sélectionnés**, procédez comme suit :
  - a. Sélectionnez la **version** que vous souhaitez utiliser.
  - b. Pour **Sélectionner le rôle IAM**, laisser à **non défini**.
  - c. Développez **Paramètres de configuration facultatifs**, suivez le schéma de configuration **Compléments** et définissez le paramètre `configurationValues` dans la section **valeurs de configuration** sur le fil de rôle que vous avez créé à l'étape précédente (la valeur doit être au format suivant : `eks.amazonaws.com/role-arn` : `arn:aws:iam::464262061435:role/AmazonEKS_FSXN_CSI_DriverRole`). Si vous sélectionnez remplacer pour la méthode de résolution des conflits, un ou plusieurs des paramètres du module complémentaire existant peuvent être remplacés par les paramètres du module complémentaire Amazon EKS. Si vous n'activez pas cette option et qu'il y a un conflit avec vos paramètres existants, l'opération échoue. Vous pouvez utiliser le message d'erreur qui en résulte pour résoudre le conflit. Avant de sélectionner cette option, assurez-vous que le module complémentaire Amazon EKS ne gère pas les paramètres que vous devez gérer vous-même.



Lorsque vous configurez le paramètre facultatif `cloudIdentity`, assurez-vous de spécifier `cloudProvider` lors de l'installation de Trident à l'aide du module complémentaire EKS.

7. Choisissez **Suivant**.
8. Sur la page **consulter et ajouter**, choisissez **Créer**.

Une fois l'installation du module complémentaire terminée, le module complémentaire installé s'affiche.

## CLI AWS

1. Créez le add-on.json fichier :

```
add-on.json
{
  "clusterName": "<eks-cluster>",
  "addonName": "netapp_trident-operator",
  "addonVersion": "v24.6.1-eksbuild.1",
  "serviceAccountRoleArn": "arn:aws:iam::123456:role/astratrident-
role",
  "configurationValues": "{\"cloudIdentity\":
  \"'eks.amazonaws.com/role-arn: arn:aws:iam::123456:role/astratrident-
role'\"}",
  "cloudProvider": "AWS"
}
```



Lorsque vous configurez le paramètre facultatif `cloudIdentity`, assurez-vous que vous spécifiez AWS en tant que `cloudProvider` lors de l'installation de Trident à l'aide du module complémentaire EKS.

2. Installer le module complémentaire Astra Trident EKS »

```
aws eks create-addon --cli-input-json file://add-on.json
```

## Mettez à jour le module complémentaire Astra Trident EKS

## Group EKS

- Vérifiez la version actuelle de votre module complémentaire FSxN Trident CSI. Remplacez `my-cluster` par le nom de votre cluster.

```
eksctl get addon --name netapp_trident-operator --cluster my-cluster
```

### Exemple de sortie :

NAME	VERSION	STATUS	ISSUES
IAMROLE	UPDATE AVAILABLE	CONFIGURATION VALUES	
netapp_trident-operator	v24.6.1-eksbuild.1	ACTIVE	0
	{"cloudIdentity": "'eks.amazonaws.com/role-arn': 'arn:aws:iam::139763910815:role/AmazonEKS_FSXN_CSI_DriverRole'"}		

- Mettez à jour le complément à la version renvoyée sous **MISE À JOUR DISPONIBLE** dans la sortie de l'étape précédente.

```
eksctl update addon --name netapp_trident-operator --version v24.6.1-eksbuild.1 --cluster my-cluster --force
```

Si vous supprimez l' `--force` option et que l'un des paramètres du module complémentaire Amazon EKS entre en conflit avec vos paramètres existants, la mise à jour du module complémentaire Amazon EKS échoue ; un message d'erreur s'affiche pour vous aider à résoudre le conflit. Avant de spécifier cette option, assurez-vous que le module complémentaire Amazon EKS ne gère pas les paramètres que vous devez gérer, car ces paramètres sont remplacés par cette option. Pour plus d'informations sur les autres options de ce paramètre, reportez-vous à la section ["Addons"](#). Pour plus d'informations sur la gestion de terrain Amazon EKS Kubernetes, reportez-vous à la section ["Gestion de terrain Kubernetes"](#).

## Console de gestion

1. Ouvrez la console Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters>.
2. Dans le volet de navigation de gauche, cliquez sur **clusters**.
3. Cliquez sur le nom du cluster pour lequel vous souhaitez mettre à jour le module complémentaire NetApp Trident CSI.
4. Cliquez sur l'onglet **Compléments**.
5. Cliquez sur **Astra Trident by NetApp**, puis sur **Modifier**.
6. Sur la page **configurer Astra Trident par NetApp**, procédez comme suit :
  - a. Sélectionnez la **version** que vous souhaitez utiliser.
  - b. (Facultatif) vous pouvez développer les **Paramètres de configuration facultatifs** et les modifier si nécessaire.
  - c. Cliquez sur **Enregistrer les modifications**.

## CLI AWS

L'exemple suivant met à jour le module complémentaire EKS :

```
aws eks update-addon --cluster-name my-cluster netapp_trident-operator vpc-cni --addon-version v24.6.1-eksbuild.1 \
```

```
--service-account-role-arn arn:aws:iam::111122223333:role/role-name
--configuration-values '{}' --resolve-conflicts --preserve
```

## Désinstallez/supprimez le module complémentaire Astra Trident EKS

Vous avez deux options pour supprimer un module complémentaire Amazon EKS :

- **Préserver le logiciel complémentaire sur votre cluster** – cette option supprime la gestion Amazon EKS de tous les paramètres. Il supprime également la possibilité pour Amazon EKS de vous informer des mises à jour et de mettre à jour automatiquement le module complémentaire Amazon EKS après avoir lancé une mise à jour. Cependant, il conserve le logiciel complémentaire sur votre cluster. Cette option fait du complément une installation auto-gérée, plutôt qu'un module complémentaire Amazon EKS. Avec cette option, vous n'avez plus à subir de temps d'indisponibilité. Conservez `--preserve` l'option dans la commande pour conserver le complément.
- **Supprimer entièrement le logiciel complémentaire de votre cluster** – nous vous recommandons de supprimer le module complémentaire Amazon EKS de votre cluster uniquement s'il n'y a pas de ressources qui en dépendent sur votre cluster. Supprimez l'`--preserve` option de la `delete` commande pour supprimer le complément.



Si le complément est associé à un compte IAM, le compte IAM n'est pas supprimé.

### Groupe EKS

La commande suivante désinstalle le module complémentaire Astra Trident EKS :

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

### Console de gestion

1. Ouvrez la console Amazon EKS à l'adresse <https://console.aws.amazon.com/eks/home#/clusters>.
2. Dans le volet de navigation de gauche, cliquez sur **clusters**.
3. Cliquez sur le nom du cluster pour lequel vous souhaitez supprimer le module complémentaire NetApp Trident CSI.
4. Cliquez sur l'onglet **Compléments**, puis cliquez sur **Astra Trident by NetApp**.\*
5. Cliquez sur **Supprimer**.
6. Dans la boîte de dialogue **Remove netapp\_trident-operator confirmation**, procédez comme suit :
  - a. Si vous souhaitez qu'Amazon EKS cesse de gérer les paramètres du module complémentaire, sélectionnez **préserver sur le cluster**. Procédez ainsi si vous souhaitez conserver l'extension logicielle sur votre cluster afin de pouvoir gérer tous les paramètres du module complémentaire vous-même.
  - b. Entrez **netapp\_trident-operator**.
  - c. Cliquez sur **Supprimer**.

### CLI AWS

Remplacez `my-cluster` par le nom de votre cluster, puis exécutez la commande suivante.

```
aws eks delete-addon --cluster-name my-cluster --addon-name netapp_trident-operator --preserve
```

## Configurez le back-end de stockage

### Intégration des pilotes SAN et NAS de ONTAP

Vous pouvez créer un fichier backend en utilisant les informations d'identification du SVM (nom d'utilisateur et mot de passe) stockées dans AWS Secret Manager, comme illustré ci-dessous :

## YAML

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFilesystemID: fs-xxxxxxxxxx
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxxx:secret:secret-
name"
    type: awsarn
```

## JSON

```
{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
      "fsxFilesystemID": "fs-xxxxxxxxxx"
    },
    "managementLIF": null,
    "credentials": {
      "name": "arn:aws:secretsmanager:us-west-2:xxxxxxxx:secret:secret-
name",
      "type": "awsarn"
    }
  }
}
```

Pour plus d'informations sur la création de systèmes back-end, consultez les pages suivantes :

- "Configurez un back-end avec les pilotes NAS ONTAP"
- "Configurez un back-end avec les pilotes SAN ONTAP"

#### Détails du pilote FSX pour ONTAP

Vous pouvez intégrer Astra Trident avec Amazon FSX pour NetApp ONTAP à l'aide des pilotes suivants :

- `ontap-san`: Chaque volume persistant provisionné est un LUN au sein de son propre volume Amazon FSX pour NetApp ONTAP. Recommandé pour le stockage en mode bloc.
- `ontap-nas`: Chaque volume persistant provisionné est un volume Amazon FSX pour NetApp ONTAP complet. Recommandé pour les protocoles NFS et SMB.
- `ontap-san-economy`: Chaque volume persistant provisionné est une LUN avec un nombre configurable de LUN par volume Amazon FSX pour NetApp ONTAP.
- `ontap-nas-economy`: Chaque volume persistant provisionné est un qtree, avec un nombre configurable de qtree par volume Amazon FSX pour NetApp ONTAP.
- `ontap-nas-flexgroup`: Chaque volume persistant provisionné est un volume Amazon FSX pour NetApp ONTAP FlexGroup complet.

Pour plus de détails sur le pilote, reportez-vous à "[Pilotes NAS](#)" et "[Pilotes SAN](#)".

#### Exemples de configurations

##### Configuration pour AWS FSX pour ONTAP avec le gestionnaire de code secret

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFilesystemID: fs-xxxxxxxxxx
    managementLIF:
      credentials:
        name: "arn:aws:secretsmanager:us-west-2:xxxxxxxx:secret:secret-
name"
        type: awsarn
```

## Configuration de la classe de stockage pour les volumes SMB

A l'aide de `nasType`, `node-stage-secret-name`, et `node-stage-secret-namespace`, vous pouvez spécifier un volume SMB et fournir les informations d'identification Active Directory requises. Les volumes SMB sont pris en charge à l'aide du `ontap-nas` pilote uniquement.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: nas-smb-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## Configuration avancée back-end et exemples

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Exemple
version		Toujours 1
storageDriverName	Nom du pilote de stockage	ontap-nas ontap-nas-economy, ontap-nas-flexgroup, , ontap-san ontap-san-economy
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + dataLIF

Paramètre	Description	Exemple
managementLIF	<p>Adresse IP d'un cluster ou LIF de gestion De SVM Un nom de domaine complet (FQDN) peut être spécifié. Peut être défini pour utiliser des adresses IPv6 si Astra Trident a été installé à l'aide de l'indicateur IPv6. Les adresses IPv6 doivent être définies entre crochets, telles que [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si vous fournissez <code>fsxFilesystemID</code> sous le <code>aws</code> champ, vous n'avez pas besoin de fournir le <code>managementLIF</code> car Astra Trident récupère les informations du SVM <code>managementLIF</code> auprès d'AWS. Donc, vous devez fournir des informations d'identification pour un utilisateur sous la SVM (par exemple : <code>vsadmin</code>) et l'utilisateur doit avoir le <code>vsadmin</code> rôle.</p>	« 10.0.0.1 », « [2001:1234:abcd::fefe] »
dataLIF	<p>Adresse IP de la LIF de protocole. <b>Pilotes NAS ONTAP:</b> Nous vous recommandons de spécifier <code>dataLIF</code>. Si elle n'est pas fournie, Astra Trident extrait les LIF 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. Peut être modifié après le réglage initial. Reportez-vous à la . <b>Pilotes SAN ONTAP :</b> ne pas spécifier pour iSCSI. Astra Trident utilise le mappage de LUN sélectif de ONTAP pour découvrir les LIFs iSCSI nécessaires pour établir une session multi-chemins. Un avertissement est généré si <code>dataLIF</code> est explicitement défini. Peut être défini pour utiliser des adresses IPv6 si Astra Trident a été installé à l'aide de l'indicateur IPv6. Les adresses IPv6 doivent être définies entre crochets, telles que [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p>	

Paramètre	Description	Exemple
autoExportPolicy	Activer la création et la mise à jour automatiques des règles d'exportation [booléennes]. À l'aide <code>autoExportPolicy</code> des options et <code>autoExportCIDRs</code> , Astra Trident peut gérer automatiquement les règles d'export.	false
autoExportCIDRs	Liste des CIDR permettant de filtrer les adresses IP des nœuds Kubernetes par rapport à lorsque <code>autoExportPolicy</code> est activé. À l'aide <code>autoExportPolicy</code> des options et <code>autoExportCIDRs</code> , Astra Trident peut gérer automatiquement les règles d'export.	« [« 0.0.0.0/0 », «:/0 »] »
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	« »
clientCertificate	Valeur encodée en Base64 du certificat client. Utilisé pour l'authentification par certificat	« »
clientPrivateKey	Valeur encodée en Base64 de la clé privée du client. Utilisé pour l'authentification par certificat	« »
trustedCACertificate	Valeur encodée en Base64 du certificat CA de confiance. Facultatif. Utilisé pour l'authentification basée sur des certificats.	« »
username	Nom d'utilisateur pour la connexion au cluster ou au SVM. Utilisé pour l'authentification basée sur les identifiants. Par exemple, vsadmin.	
password	Mot de passe pour se connecter au cluster ou au SVM. Utilisé pour l'authentification basée sur les identifiants.	
svm	Serveur virtuel de stockage à utiliser	Dérivé si une LIF de gestion SVM est spécifiée.
storagePrefix	Préfixe utilisé pour le provisionnement des nouveaux volumes dans la SVM. Ne peut pas être modifié après sa création. Pour mettre à jour ce paramètre, vous devez créer un nouveau backend.	trident

Paramètre	Description	Exemple
limitAggregateUsage	<b>Ne spécifiez pas pour Amazon FSX pour NetApp ONTAP.</b> Les fournies <code>fsxadmin</code> et <code>vsadmin</code> ne contiennent pas les autorisations requises pour récupérer l'utilisation des agrégats et les limiter à l'aide d'Astra Trident.	Ne pas utiliser.
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur. Limite également la taille maximale des volumes gérés pour les qtrees et les LUN, et <code>qtreePerFlexvol</code> permet de personnaliser le nombre maximal de qtrees par FlexVol.	« » (non appliqué par défaut)
lunsPerFlexvol	Le nombre maximal de LUN par FlexVol doit être compris dans la plage [50, 200]. SAN uniquement.	« 100 »
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, <code>{"api":false, "method":true}</code> n'utilisez <code>debugTraceFlags</code> que si vous effectuez un dépannage et que vous avez besoin d'un vidage de journal détaillé.	nul
nfsMountOptions	Liste des options de montage NFS séparée par des virgules. Les options de montage des volumes Kubernetes persistants sont généralement spécifiées dans les classes de stockage, mais si aucune option de montage n'est spécifiée dans une classe de stockage, Astra Trident utilisera les options de montage spécifiées dans le fichier de configuration du système back-end. Si aucune option de montage n'est spécifiée dans la classe de stockage ou le fichier de configuration, Astra Trident ne définit aucune option de montage sur un volume persistant associé.	« »
nasType	Configurez la création de volumes NFS ou SMB. Les options sont <code>nfs</code> , <code>smb</code> ou <code>null</code> . <b>Doit être défini sur <code>smb</code> pour les volumes SMB.</b> La valeur <code>null</code> par défaut sur les volumes NFS.	<code>nfs</code>

Paramètre	Description	Exemple
qtreesPerFlexvol	Nombre maximal de qtrees par FlexVol, qui doit être compris dans la plage [50, 300]	"200"
smbShare	<p>Vous pouvez indiquer l'un des éléments suivants : nom d'un partage SMB créé à l'aide de la console de gestion Microsoft ou de l'interface de ligne de commande ONTAP, ou nom permettant à Astra Trident de créer le partage SMB.</p> <p>Ce paramètre est requis pour Amazon FSX pour les systèmes back-end ONTAP.</p>	smb-share
useREST	<p>Paramètre booléen pour utiliser les API REST de ONTAP. <b>Tech Preview</b></p> <p>useREST est fourni sous forme de <b>aperçu technique</b> recommandé pour les environnements de test et non pour les charges de travail de production. Lorsqu'il est défini sur true, Astra Trident utilise les API REST ONTAP pour communiquer avec le back-end. Cette fonctionnalité requiert ONTAP 9.11.1 et versions ultérieures. En outre, le rôle de connexion ONTAP utilisé doit avoir accès à l' ontap application. Ceci est satisfait par les rôles et prédéfinis vsadmin cluster-admin .</p>	false
aws	<p>Vous pouvez spécifier ce qui suit dans le fichier de configuration d'AWS FSX pour ONTAP : -</p> <p>fsxFilesystemID: spécifiez l'ID du système de fichiers AWS FSX. -</p> <p>apiRegion: Nom de la région de l'API AWS. -</p> <p>apikey: Clé d'API AWS. -</p> <p>secretKey: Clé secrète AWS.</p>	"" "" ""

Paramètre	Description	Exemple
credentials	Spécifiez les informations d'identification du SVM FSX à stocker dans AWS Secret Manager. - name: Amazon Resource Name (ARN) du secret, qui contient les références de SVM. - type: Réglé sur awsarn. Pour plus d'informations, reportez-vous à la section " <a href="#">Créez un secret AWS secrets Manager</a> ".	

#### Options de configuration back-end pour les volumes de provisionnement

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

Paramètre	Description	Valeur par défaut
spaceAllocation	Allocation d'espace pour les LUN	true
spaceReserve	Mode de réservation d'espace ; "none" (fin) ou "volume" (épais)	none
snapshotPolicy	Règle Snapshot à utiliser	none
qosPolicy	QoS policy group à affecter pour les volumes créés. Choisissez une de qosPolicy ou adaptiveQosPolicy par pool de stockage ou back-end. Avec Astra Trident, les groupes de règles de QoS doivent être utilisés avec ONTAP 9.8 ou version ultérieure. Nous recommandons l'utilisation d'un groupe de règles de qualité de service non partagé et nous assurer que le groupe de règles est appliqué à chaque composant individuellement. Un groupe de règles de QoS partagé appliquera le plafond du débit total de toutes les charges de travail.	« »
adaptiveQosPolicy	Groupe de règles de QoS adaptative à attribuer aux volumes créés. Choisissez une de qosPolicy ou adaptiveQosPolicy par pool de stockage ou back-end. Non pris en charge par l'économie ontap-nas.	« »
snapshotReserve	Pourcentage du volume réservé pour les instantanés "0"	Si <code>snapshotPolicy</code> est none, else « »
splitOnClone	Séparer un clone de son parent lors de sa création	false

Paramètre	Description	Valeur par défaut
encryption	Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume. La valeur par défaut est <code>false</code> . Pour utiliser cette option, NVE doit être sous licence et activé sur le cluster. Si NAE est activé sur le back-end, tous les volumes provisionnés dans Astra Trident seront activés par NAE. Pour plus d'informations, reportez-vous à la section : <a href="#">"Fonctionnement d'Astra Trident avec NVE et NAE"</a> .	<code>false</code>
luksEncryption	Activez le cryptage LUKS. Reportez-vous à la <a href="#">"Utiliser la configuration de clé unifiée Linux (LUKS)"</a> . SAN uniquement.	« »
tieringPolicy	Règle de hiérarchisation à utiliser <code>none</code>	<code>snapshot-only</code> Pour la configuration pré-ONTAP 9.5 SVM-DR
unixPermissions	Mode pour les nouveaux volumes. <b>Laisser vide pour les volumes SMB.</b>	« »
securityStyle	Style de sécurité pour les nouveaux volumes. Prise en charge <code>et unix</code> styles de sécurité par NFS <code>mixed</code> . Prise en charge SMB <code>mixed</code> et <code>ntfs</code> styles de sécurité.	NFS par défaut est <code>unix</code> . SMB la valeur par défaut est <code>ntfs</code> .

### Préparez-vous au provisionnement des volumes SMB

Vous pouvez provisionner des volumes SMB à l'aide du `ontap-nas` pilote. Avant de terminer [l'intégration des pilotes SAN et NAS de ONTAP](#), procédez comme suit.

#### Avant de commencer

Avant de pouvoir provisionner des volumes SMB à l'aide du `ontap-nas` pilote, vous devez disposer des éléments suivants.

- Cluster Kubernetes avec un nœud de contrôleur Linux et au moins un nœud worker Windows exécutant Windows Server 2019. Astra Trident prend en charge les volumes SMB montés sur des pods qui s'exécutent uniquement sur des nœuds Windows.
- Au moins un secret Astra Trident contenant vos identifiants Active Directory. Pour générer un secret `smbcreds`:

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

- Un proxy CSI configuré en tant que service Windows. Pour configurer un `csi-proxy`, reportez-vous

"GitHub : proxy CSI" à la section ou "GitHub : proxy CSI pour Windows" pour les nœuds Kubernetes s'exécutant sous Windows.

## Étapes

1. Création de partages SMB. Vous pouvez créer les partages d'administration SMB de deux manières, soit à l'aide du "Console de gestion Microsoft" composant logiciel enfichable dossiers partagés, soit à l'aide de l'interface de ligne de commande ONTAP. Pour créer les partages SMB à l'aide de l'interface de ligne de commandes ONTAP :

- a. Si nécessaire, créez la structure du chemin d'accès au répertoire pour le partage.

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

- b. Créer un partage SMB associé au SVM spécifié :

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

- c. Vérifiez que le partage a été créé :

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



Reportez-vous "Créez un partage SMB" à pour plus de détails.

2. Lors de la création du back-end, vous devez configurer le suivant pour spécifier les volumes SMB. Pour toutes les options de configuration du back-end FSX for ONTAP, reportez-vous à "Exemples et options de configuration de FSX pour ONTAP" la section .

Paramètre	Description	Exemple
smbShare	Vous pouvez indiquer l'un des éléments suivants : nom d'un partage SMB créé à l'aide de la console de gestion Microsoft ou de l'interface de ligne de commande ONTAP, ou nom permettant à Astra Trident de créer le partage SMB. Ce paramètre est requis pour Amazon FSX pour les systèmes back-end ONTAP.	smb-share
nasType	<b>Doit être réglé sur smb.</b> Si nul, la valeur par défaut est nfs .	smb
securityStyle	Style de sécurité pour les nouveaux volumes. <b>Doit être défini sur ntfs ou mixed pour les volumes SMB.</b>	ntfs Ou mixed pour les volumes SMB

Paramètre	Description	Exemple
unixPermissions	Mode pour les nouveaux volumes. <b>Doit rester vide pour les volumes SMB.</b>	« »

## Configurez une classe de stockage et un PVC

Configurez un objet StorageClass Kubernetes et créez la classe de stockage pour indiquer à Astra Trident comment provisionner les volumes. Créez un volume persistant et une demande de volume persistant qui utilisent la classe de stockage Kubernetes configurée pour demander l'accès au volume persistant. Vous pouvez ensuite monter le volume persistant sur un pod.

### Créer une classe de stockage

#### Configuration d'un objet StorageClass Kubernetes

Le système "[Objet classe de stockage Kubernetes](#)" identifie Astra Trident en tant que mécanisme de provisionnement utilisé pour cette classe indique à Astra Trident comment provisionner un volume. Par exemple :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
```

Reportez-vous "[Kubernetes et objets Trident](#)" à pour plus de détails sur l'interaction des classes de stockage avec les PersistentVolumeClaim paramètres et pour le contrôle de la façon dont Astra Trident provisionne les volumes.

### Créer une classe de stockage

#### Étapes

- Il s'agit d'un objet Kubernetes. Utilisez donc `kubectl` pour le créer dans Kubernetes.

```
kubectl create -f storage-class-ontapnas.yaml
```

- Vous devriez désormais voir une classe de stockage **Basic-csi** dans Kubernetes et Astra Trident. Astra Trident devrait avoir découvert les pools sur le système back-end.

```
kubectl get sc basic-csi
NAME          PROVISIONER          AGE
basic-csi     csi.trident.netapp.io  15h
```

### Créer le volume persistant et la demande de volume persistant

Un "[Volume persistant](#)" (PV) est une ressource de stockage physique provisionnée par l'administrateur du cluster sur un cluster Kubernetes. La "[PersistentVolumeClaim](#)" demande de volume persistant est une demande d'accès au volume persistant sur le cluster.

Le PVC peut être configuré pour demander un stockage d'une certaine taille ou d'un certain mode d'accès. À l'aide de la classe de stockage associée, l'administrateur du cluster peut contrôler plus que la taille du volume persistant et le mode d'accès, tels que les performances ou le niveau de service.

Après avoir créé le volume persistant et la demande de volume persistant, vous pouvez monter le volume dans un pod.

### Exemples de manifestes

#### Exemple de manifeste de volume persistant

Cet exemple de manifeste montre un volume persistant de base de 10Gi associé à StorageClass basic-csi.

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv-storage
  labels:
    type: local
spec:
  storageClassName: basic-csi
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteMany
  hostPath:
    path: "/my/host/path"
```

## Exemples de manifestes de demande de volume persistant

Ces exemples présentent les options de configuration de base de la PVC.

### PVC avec accès RWO

Cet exemple montre une demande de volume persistant de base avec accès RWX associée à une classe de stockage nommée basic-csi.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

### PVC avec NVMe/TCP

Cet exemple montre une demande de volume persistant de base pour NVMe/TCP avec accès RWO associée à une classe de stockage nommée protection-gold.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san-nvme
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 300Mi
  storageClassName: protection-gold
```

## Créer le volume persistant et la demande de volume persistant

### Étapes

1. Créer la PV.

```
kubectl create -f pv.yaml
```

## 2. Vérifiez l'état du PV.

```
kubectl get pv
NAME          CAPACITY  ACCESS MODES  RECLAIM POLICY  STATUS     CLAIM
STORAGECLASS  REASON    AGE
pv-storage    4Gi       RWO          Retain        Available
7s
```

## 3. Créez la PVC.

```
kubectl create -f pvc.yaml
```

## 4. Vérifiez l'état de la demande de volume persistant.

```
kubectl get pvc
NAME          STATUS  VOLUME      CAPACITY  ACCESS MODES  STORAGECLASS  AGE
pvc-storage  Bound  pv-name  2Gi       RWO          5m
```

Reportez-vous "[Kubernetes et objets Trident](#)" à pour plus de détails sur l'interaction des classes de stockage avec les `PersistentVolumeClaim` paramètres et pour le contrôle de la façon dont Astra Trident provisionne les volumes.

### Attributs d'Astra Trident

Ces paramètres déterminent quels pools de stockage gérés par Astra Trident doivent être utilisés pour provisionner les volumes d'un type donné.

Attribut	Type	Valeurs	Offre	Demande	Pris en charge par
support <sup>1</sup>	chaîne	hdd, hybride, ssd	Le pool contient des supports de ce type ; hybride signifie les deux	Type de support spécifié	ontap-nas, ontap-nas-économie, ontap-nas-flexgroup, ontap-san, solidfire-san
Type de provisionnement	chaîne	fin, épais	Le pool prend en charge cette méthode de provisionnement	Méthode de provisionnement spécifiée	thick : tous les systèmes ONTAP ; thin : tous les systèmes ONTAP et solidfire-san

Attribut	Type	Valeurs	Offre	Demande	Pris en charge par
Type de dos	chaîne	ontap-nas, économie ontap-nas, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Le pool appartient à ce type de système back-end	Backend spécifié	Tous les conducteurs
snapshots	bool	vrai, faux	Le pool prend en charge les volumes dotés de snapshots	Volume sur lequel les snapshots sont activés	ontap-nas, ontap-san, solidfire-san, gcp-cvs
clones	bool	vrai, faux	Le pool prend en charge les volumes de clonage	Volume sur lequel les clones sont activés	ontap-nas, ontap-san, solidfire-san, gcp-cvs
le cryptage	bool	vrai, faux	Le pool prend en charge les volumes chiffrés	Volume avec chiffrement activé	ontap-nas, économie ontap-nas, ontap-nas-flexgroups, ontap-san
LES IOPS	int	entier positif	Le pool est en mesure de garantir l'IOPS dans cette plage	Volume garanties IOPS	solidfire-san

<sup>1</sup> : non pris en charge par les systèmes ONTAP Select

## Déploiement de l'application exemple

Déploiement de l'application exemple.

### Étapes

1. Montez le volume dans un pod.

```
kubectl create -f pv-pod.yaml
```

Ces exemples montrent les configurations de base pour attacher le PVC à un pod : **Configuration de base** :

```

kind: Pod
apiVersion: v1
metadata:
  name: pv-pod
spec:
  volumes:
    - name: pv-storage
      persistentVolumeClaim:
        claimName: basic
  containers:
    - name: pv-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/my/mount/path"
          name: pv-storage

```



Vous pouvez surveiller la progression à l'aide de `kubectl get pod --watch`.

2. Vérifiez que le volume est monté sur `/my/mount/path`.

```
kubectl exec -it task-pv-pod -- df -h /my/mount/path
```

Filesystem	Size
Used Avail Use% Mounted on	
192.168.188.78:/trident_pvc_ae45ed05_3ace_4e7c_9080_d2a83ae03d06	1.1G
320K 1.0G 1% /my/mount/path	

1. Vous pouvez maintenant supprimer le Pod. L'application Pod n'existera plus, mais le volume restera.

```
kubectl delete pod task-pv-pod
```

### Configurez le module d'extension Astra Trident EKS sur un cluster EKS

ASTRA Trident simplifie la gestion du stockage Amazon FSX pour NetApp ONTAP dans Kubernetes pour que vos développeurs et administrateurs puissent donner la priorité au déploiement d'applications. Le module complémentaire Astra Trident EKS inclut les derniers correctifs de sécurité et de bogues, et il est validé par AWS pour fonctionner avec Amazon EKS. Le module complémentaire EKS vous permet de vous assurer de

manière cohérente que vos clusters Amazon EKS sont sécurisés et stables et de réduire la quantité de travail à effectuer pour installer, configurer et mettre à jour des modules complémentaires.

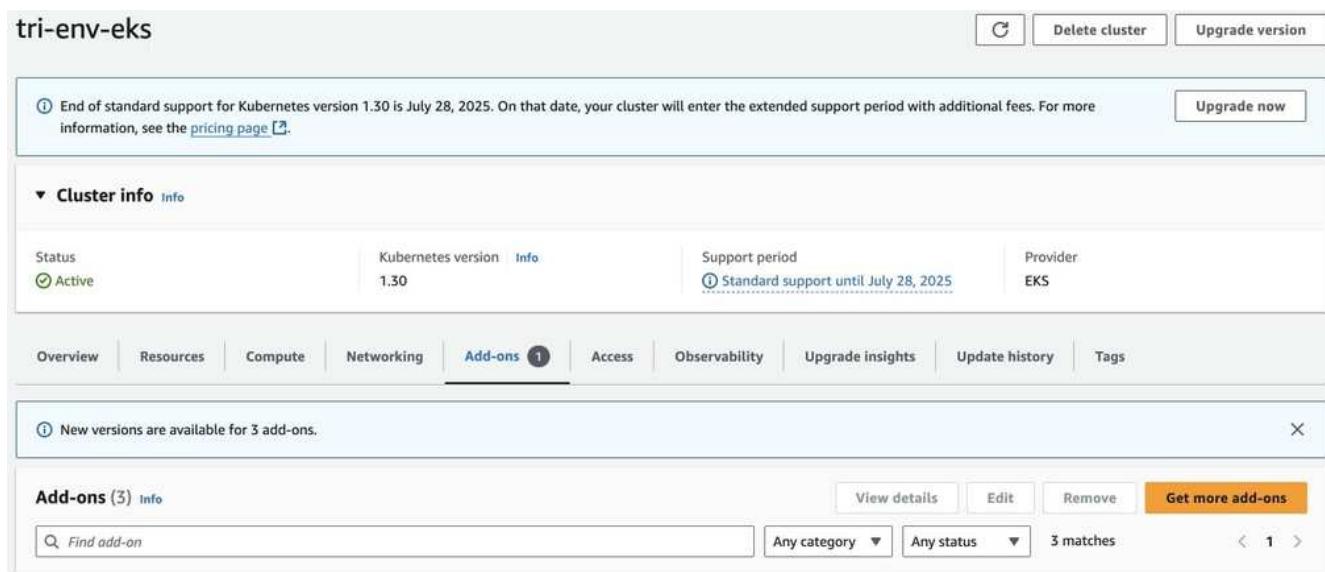
## Prérequis

Vérifiez les points suivants avant de configurer le module complémentaire Astra Trident pour AWS EKS :

- Un compte de cluster Amazon EKS avec abonnement complémentaire
- Autorisations AWS sur AWS Marketplace :  
"aws-marketplace:ViewSubscriptions",  
"aws-marketplace:Subscribe",  
"aws-marketplace:Unsubscribe"
- Type ami : Amazon Linux 2 (AL2\_x86\_64) ou Amazon Linux 2 ARM (AL2\_ARM\_64)
- Type de nœud : AMD ou ARM
- Un système de fichiers Amazon FSX pour NetApp ONTAP

## Étapes

1. Sur votre cluster EKS Kubernetes, accédez à l'onglet **Add-ons**.



The screenshot shows the AWS EKS Cluster Management console for a cluster named "tri-env-eks". The "Add-ons" tab is selected. A message at the top indicates that standard support for Kubernetes version 1.30 ends on July 28, 2025, and provides a link to the pricing page. Below this, the "Cluster info" section shows the cluster is active, running Kubernetes version 1.30, and has a support period until July 28, 2025, provided by EKS. A notification at the bottom of the "Add-ons" tab indicates that new versions are available for 3 add-ons. The "Add-ons" section lists 3 matches, with buttons for "View details", "Edit", "Remove", and "Get more add-ons".

2. Accédez à **add-ons** AWS Marketplace et choisissez la catégorie *Storage*.

## AWS Marketplace add-ons (1)



Discover, subscribe to and configure EKS add-ons to enhance your EKS clusters.

Find add-on

### Filtering options

Any category ▾

NetApp, Inc. ▾

Any pricing model ▾

Clear filters

NetApp, Inc.

< 1 >

### NetApp **NetApp Trident**



NetApp Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. [Product details](#)

Standard Contract

Category	Listed by	Supported versions	Pricing starting at
storage	<a href="#">NetApp, Inc.</a>	1.30, 1.29, 1.28, 1.27, 1.26, 1.25, 1.24, 1.23	<a href="#">View pricing details</a>

Cancel

Next

3. Localisez **NetApp Trident** et cochez la case du module complémentaire Astra Trident.
4. Choisissez la version souhaitée du module complémentaire.

**NetApp Trident**

[Remove add-on](#)

Listed by	Category	Status
 NetApp	storage	<input checked="" type="checkbox"/> Ready to install

**i** You're subscribed to this software

You can view the terms and pricing details for this product or choose another offer if one is available.

[View subscription](#) [X](#)

**Version**  
Select the version for this add-on.

v24.6.1-eksbuild.1 [▼](#)

**Select IAM role**  
Select an IAM role to use with this add-on. To create a new custom role, follow the instructions in the [Amazon EKS User Guide](#) .

Not set [▼](#) [C](#)

**► Optional configuration settings**

[Cancel](#) [Previous](#) [Next](#)

5. Sélectionnez l'option rôle IAM à hériter du nœud.

## Review and add

### Step 1: Select add-ons

Edit

#### Selected add-ons (1)

Find add-on

< 1 >

Add-on name	Type	Status
-------------	------	--------

netapp_trident-operator	storage	Ready to install
-------------------------	---------	------------------

### Step 2: Configure selected add-ons settings

Edit

#### Selected add-ons version (1)

< 1 >

Add-on name	Version	IAM role for service account (IRSA)
-------------	---------	-------------------------------------

netapp_trident-operator	v24.6.1-eksbuild.1	Not set
-------------------------	--------------------	---------

Cancel

Previous

Create

6. (Facultatif) configurez tous les paramètres de configuration facultatifs selon les besoins et sélectionnez **Suivant**.

Suivez le schéma de configuration **Add-on** et définissez le paramètre `configurationValues` dans la section **Configuration Values** sur le fil de rôle que vous avez créé à l'étape précédente (la valeur doit être au format suivant : `eks.amazonaws.com/role-arn` :

`arn:aws:iam::464262061435:role/AmazonEKS_FSXN_CSI_DriverRole`). Si vous sélectionnez remplacer pour la méthode de résolution des conflits, un ou plusieurs des paramètres du module complémentaire existant peuvent être remplacés par les paramètres du module complémentaire Amazon EKS. Si vous n'activez pas cette option et qu'il y a un conflit avec vos paramètres existants, l'opération échoue. Vous pouvez utiliser le message d'erreur qui en résulte pour résoudre le conflit. Avant de sélectionner cette option, assurez-vous que le module complémentaire Amazon EKS ne gère pas les paramètres que vous devez gérer vous-même.



Lorsque vous configurez le paramètre facultatif `cloudIdentity`, assurez-vous que vous spécifiez AWS en tant que `cloudProvider` lors de l'installation de Trident à l'aide du module complémentaire EKS.

**Select IAM role**  
Select an IAM role to use with this add-on. To create a new custom role, follow the instructions in the [Amazon EKS User Guide](#).

Not set ▼ C

**Optional configuration settings**

**Add-on configuration schema**  
Refer to the JSON schema below. The configuration values entered in the code editor will be validated against this schema.

```
{
  "$id": "http://example.com/example.json",
  "$schema": "https://json-schema.org/draft/2019-09/schema",
  "default": {},
  "examples": [
    {
      "cloudIdentity": ""
    }
  ],
  "properties": {
    "cloudIdentity": {
      "default": "",
      "examples": [
        "eks.amazonaws.com/role-arn: arn:aws:iam::139763910815:role/AmazonEKS_FSXN_CSI_DriverRole"
      ]
    }
  }
}
```

**Configuration values** Info  
Specify any additional JSON or YAML configurations that should be applied to the add-on.

```
1  {
2    "cloudIdentity": "eks.amazonaws.com/role-arn: arn:aws
3      :iam::139763910815:role
4      /AmazonEKS_FSXN_CSI_DriverRole",
5    "cloudProvider": "AWS"
6  }
```

7. Sélectionnez **Créer**.

8. Vérifiez que l'état du complément est *Active*.

**Add-ons (1) Info**

Q. netapp View details Edit Remove Get more add-ons

Any category Any status 1 match < 1 >

<b>NetApp Astra Trident by NetApp</b>	
Astra Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. <a href="#">Product details</a>	
Category	Status
storage	<span style="color: green;">Active</span>
Version	v24.6.1-eksbuild.1
IAM role for service account	(IRSA)
Listed by	<a href="#">NetApp, Inc.</a>
Not set	
<span style="border: 1px solid #ccc; padding: 2px 10px;">View subscription</span>	

**Installez/désinstallez le module complémentaire Astra Trident EKS à l'aide de l'interface de ligne de commande**

**Installez le module complémentaire Astra Trident EKS à l'aide de l'interface de ligne de commande :**

L'exemple de commande suivant installe le module complémentaire Astra Trident EKS :

```
eksctl create addon --cluster K8s-arm --name netapp_trident-operator --version v24.6.1-eksbuild
```

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v24.6.1-eksbuild.1 (avec une version dédiée)
```



Lorsque vous configurez le paramètre facultatif `cloudIdentity`, assurez-vous de spécifier `cloudProvider` lors de l'installation de Trident à l'aide du module complémentaire EKS.

## Désinstallez le module complémentaire Astra Trident EKS à l'aide de l'interface de ligne de commande :

La commande suivante désinstalle le module complémentaire Astra Trident EKS :

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

## Création de systèmes back-end avec kubectl

Un système back-end définit la relation entre Astra Trident et un système de stockage. Il explique à Astra Trident comment communiquer avec ce système de stockage et comment Astra Trident doit provisionner des volumes à partir de celui-ci. Après l'installation d'Astra Trident, l'étape suivante consiste à créer un système back-end. La `TridentBackendConfig` définition personnalisée des ressources (CRD) vous permet de créer et de gérer des systèmes back-end Trident directement via l'interface Kubernetes. Pour cela, vous pouvez utiliser `kubectl` ou l'outil CLI équivalent pour votre distribution Kubernetes.

### TridentBackendConfig

`TridentBackendConfig` (`tbc`, `tbconfig`, `tbackendconfig`) Est un système CRD frontend et namespaces qui vous permet de gérer les systèmes back-end Astra Trident à l'aide de `kubectl`. Kubernetes et les administrateurs du stockage peuvent désormais créer et gérer des systèmes back-end directement via l'interface de ligne de commande Kubernetes sans avoir besoin d'un utilitaire de ligne de commande dédié (`tridentctl`).

Lors de la création d'un `TridentBackendConfig` objet, les événements suivants se produisent :

- Un système back-end est créé automatiquement par Astra Trident en fonction de la configuration que vous fournissez. Ceci est représenté en interne sous la forme d'une `TridentBackend` CR (`tbe`, `tridentbackend`).
- Le système `TridentBackendConfig` est lié de manière unique à un `TridentBackend` qui a été créé par Astra Trident.

Chacun `TridentBackendConfig` gère un mappage un-à-un avec un `TridentBackend`. le premier est l'interface fournie à l'utilisateur pour concevoir et configurer des systèmes back-end ; le second est la façon dont Trident représente l'objet back-end réel.



`TridentBackend` Les services CRS sont créés automatiquement par Astra Trident. Vous ne devez pas les modifier. Si vous souhaitez effectuer des mises à jour vers des systèmes back-end, modifiez l'objet pour procéder `TridentBackendConfig` à cette opération.

Reportez-vous à l'exemple suivant pour connaître le format de `TridentBackendConfig` la CR :

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret

```

Vous pouvez également consulter les exemples de configuration de la plate-forme/du service de stockage souhaité dans le ["programme d'installation trident"](#) répertoire.

``spec`` Prend en charge les paramètres de configuration spécifiques au back-end. Dans cet exemple, le back-end utilise le ``ontap-san`` pilote de stockage et les paramètres de configuration qui sont tabulés ici. Pour obtenir la liste des options de configuration du pilote de stockage souhaité, reportez-vous au [xref:{relative\\_path}backends.html\["informations de configuration backend pour votre pilote de stockage"\]](#).

La `spec` section inclut également `credentials` les champs et `deletionPolicy`, qui sont récemment introduits dans la `TridentBackendConfig` CR :

- `credentials`: Ce paramètre est un champ obligatoire qui contient les informations d'identification utilisées pour s'authentifier auprès du système/service de stockage. Cette configuration est définie sur un code secret Kubernetes créé par l'utilisateur. Les informations d'identification ne peuvent pas être transmises en texte brut et entraînent une erreur.
- `deletionPolicy`: Ce champ définit ce qui doit se produire lorsque le `TridentBackendConfig` est supprimé. Il peut prendre l'une des deux valeurs possibles :
  - `delete`: Cela entraîne la suppression de la `TridentBackendConfig` CR et du back-end associé. Il s'agit de la valeur par défaut.
  - `retain`: Lorsqu'une `TridentBackendConfig` demande de modification est supprimée, la définition du back-end est toujours présente et peut être gérée avec `tridentctl`. La définition de la stratégie de suppression `retain` permet aux utilisateurs de revenir à une version antérieure (antérieure à 21.04) et de conserver les systèmes back-end créés. La valeur de ce champ peut être mise à jour après la création d'un `TridentBackendConfig`.

 Le nom d'un backend est défini à l'aide de `spec.backendName`. S'il n'est pas spécifié, le nom du backend est défini sur le nom de `TridentBackendConfig` l'objet (metadata.name). Il est recommandé de définir explicitement les noms de back-end à l'aide de `spec.backendName`.

 Les systèmes back-end créés avec `tridentctl` n'ont pas d'objet associé `TridentBackendConfig`. Vous pouvez choisir de gérer ces systèmes back-end avec `kubectl` en créant une `TridentBackendConfig` demande de modification. Veillez à spécifier des paramètres de configuration identiques (tels que `spec.backendName`, , , `spec.storagePrefix` `spec.storageDriverName` etc.). ASTRA Trident lie automatiquement le nouveau système créé `TridentBackendConfig` avec le back-end pré-existant.

## Présentation des étapes

Pour créer un nouveau back-end à l'aide de `kubectl`, procédez comme suit :

1. Créer un "[Le secret de Kubernetes](#)". le secret contient les informations d'identification dont Astra Trident a besoin pour communiquer avec le cluster/service de stockage.
2. Créer un `TridentBackendConfig` objet. Elle contient des informations spécifiques sur le cluster/service de stockage et fait référence au secret créé à l'étape précédente.

Après avoir créé un backend, vous pouvez observer son état en utilisant et en `kubectl get tbc <tbc-name> -n <trident-namespace>` rassemblant des détails supplémentaires.

### Étape 1 : créez un code secret Kubernetes

Créez un secret qui contient les informations d'identification d'accès pour le back-end. Ce point est unique à chaque service/plateforme de stockage. Voici un exemple :

```
kubectl -n trident create -f backend-tbc-ontap-san-secret.yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-san-secret
type: Opaque
stringData:
  username: cluster-admin
  password: password
```

Ce tableau récapitule les champs à inclure dans le Secret pour chaque plate-forme de stockage :

Description des champs secrets de la plate-forme de stockage	Secret	Description des champs
Azure NetApp Files	ID client	ID client d'un enregistrement d'application
Cloud Volumes Service pour GCP	id_clé_privée	ID de la clé privée. Partie de la clé API pour le compte de service GCP avec le rôle d'administrateur CVS

Description des champs secrets de la plate-forme de stockage	Secret	Description des champs
Cloud Volumes Service pour GCP	clé_privée	Clé privée. Partie de la clé API pour le compte de service GCP avec le rôle d'administrateur CVS
Element (NetApp HCI/SolidFire)	Point final	MVIP pour le cluster SolidFire avec les identifiants de locataire
ONTAP	nom d'utilisateur	Nom d'utilisateur pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants
ONTAP	mot de passe	Mot de passe pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants
ONTAP	ClientPrivateKey	Valeur encodée en Base64 de la clé privée du client. Utilisé pour l'authentification basée sur des certificats
ONTAP	ChapUsername	Nom d'utilisateur entrant. Requis si useCHAP=vrai. Pour ontap-san et ontap-san-economy
ONTAP	Chapeau InitiatorSecret	Secret de l'initiateur CHAP. Requis si useCHAP=vrai. Pour ontap-san et ontap-san-economy
ONTAP	ChapTargetUsername	Nom d'utilisateur cible. Requis si useCHAP=vrai. Pour ontap-san et ontap-san-economy
ONTAP	ChapTargetInitiatorSecret	Secret de l'initiateur cible CHAP. Requis si useCHAP=vrai. Pour ontap-san et ontap-san-economy

Le secret créé à cette étape sera référencé dans le `spec.credentials` champ de l'`TridentBackendConfig` objet créé à l'étape suivante.

## Étape 2 : créer la `TridentBackendConfig` CR

Vous êtes maintenant prêt à créer votre `TridentBackendConfig` CR. Dans cet exemple, un back-end qui utilise le `ontap-san` pilote est créé à l'aide de l'`TridentBackendConfig` objet illustré ci-dessous :

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

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

### Étape 3 : vérifier l'état du TridentBackendConfig CR

Maintenant que vous avez créé la TridentBackendConfig demande de modification, vous pouvez vérifier son état. Voir l'exemple suivant :

```
kubectl -n trident get tbc backend-tbc-ontap-san
NAME          BACKEND NAME      BACKEND UUID
PHASE  STATUS
backend-tbc-ontap-san  ontap-san-backend  8d24fce7-6f60-4d4a-8ef6-
bab2699e6ab8    Bound    Success
```

Un back-end a été créé avec succès et lié à la TridentBackendConfig demande de modification.

La phase peut prendre l'une des valeurs suivantes :

- **Bound:** La TridentBackendConfig CR est associée à un back-end, et ce back-end contient configRef défini sur l'uid de la TridentBackendConfig CR.
- **Unbound:** Représenté à l'aide de "". L' TridentBackendConfig` objet n'est pas lié à un backend. Par défaut, toutes les demandes de modification nouvellement créées `TridentBackendConfig sont dans cette phase. Une fois la phase modifiée, elle ne peut plus revenir à Unbound.
- **Deleting:** La TridentBackendConfig demande de modification deletionPolicy a été définie sur supprimer. Lorsque la TridentBackendConfig CR est supprimée, elle passe à l'état Suppression.
  - Si aucune demande de volume persistant n'existe sur le back-end, la suppression du entraîne la suppression d'Astra Trident, TridentBackendConfig le back-end ainsi que la TridentBackendConfig demande de remboursement.
  - Si un ou plusieurs ESV sont présents sur le back-end, il passe à l'état de suppression. La

TridentBackendConfig CR passe ensuite également en phase de suppression. Le back-end et TridentBackendConfig sont supprimés uniquement après la suppression de toutes les ESV.

- **Lost:** Le back-end associé à la TridentBackendConfig CR a été accidentellement ou délibérément supprimé et la TridentBackendConfig CR a toujours une référence au back-end supprimé. La TridentBackendConfig demande de modification peut toujours être supprimée quelle que soit la `deletionPolicy` valeur.
- **Unknown:** Astra Trident n'est pas en mesure de déterminer l'état ou l'existence du back-end associé au TridentBackendConfig CR. Par exemple, si le serveur d'API ne répond pas ou si le `tridentbackends.trident.netapp.io` CRD est manquant. Cela peut nécessiter une intervention.

À ce stade, un système back-end est créé avec succès ! Plusieurs opérations peuvent également être gérées, telles que "["mises à jour du système back-end et suppressions"](#)".

#### (Facultatif) étape 4 : pour plus de détails

Vous pouvez exécuter la commande suivante pour obtenir plus d'informations sur votre système back-end :

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

NAME	BACKEND NAME	BACKEND UUID	
PHASE	STATUS	STORAGE DRIVER	DELETION POLICY
backend-tbc-ontap-san	Bound	ontap-san-backend	8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
		Success	ontap-san
			delete

En outre, vous pouvez également obtenir un vimage YAML/JSON de TridentBackendConfig.

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

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  creationTimestamp: "2021-04-21T20:45:11Z"
  finalizers:
  - trident.netapp.io
  generation: 1
  name: backend-tbc-ontap-san
  namespace: trident
  resourceVersion: "947143"
  uid: 35b9d777-109f-43d5-8077-c74a4559d09c
spec:
  backendName: ontap-san-backend
  credentials:
    name: backend-tbc-ontap-san-secret
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  storageDriverName: ontap-san
  svm: trident_svm
  version: 1
status:
  backendInfo:
    backendName: ontap-san-backend
    backendUUID: 8d24fce7-6f60-4d4a-8ef6-bab2699e6ab8
  deletionPolicy: delete
  lastOperationStatus: Success
  message: Backend 'ontap-san-backend' created
  phase: Bound

```

backendInfo Contient le backendName et le backendUUID du back-end créé en réponse à la TridentBackendConfig demande de modification. Le lastOperationStatus champ indique le statut de la dernière opération de TridentBackendConfig la demande de modification, qui peut être déclenchée par l'utilisateur (par exemple, lors du redémarrage d'Astra Trident par l'utilisateur spec) ou par Astra Trident. Il peut s'agir d'un succès ou d'un échec. phase Représente l'état de la relation entre la TridentBackendConfig CR et le back-end. Dans l'exemple ci-dessus, phase a la valeur liée, ce qui signifie que la TridentBackendConfig CR est associée au back-end.

Vous pouvez exécuter `kubectl -n trident describe tbc <tbc-cr-name>` la commande pour obtenir des détails sur les journaux d'événements.

 Vous ne pouvez pas mettre à jour ou supprimer un back-end contenant un objet associé à TridentBackendConfig l'aide de `tridentctl`. Pour comprendre les étapes impliquées dans le passage entre `tridentctl` et `TridentBackendConfig`, ["voir ici"](#).

## Gestion des systèmes back-end

### Effectuer la gestion back-end avec kubectl

Découvrez comment effectuer des opérations de gestion back-end à l'aide de kubectl.

#### Supprimer un back-end

En supprimant un `TridentBackendConfig`, vous demandez à Astra Trident de supprimer/conserver les systèmes back-end (sur la base de `deletionPolicy` la). Pour supprimer un back-end, assurez-vous que `deletionPolicy` est défini sur supprimer. Pour supprimer uniquement le `TridentBackendConfig`, assurez-vous que `deletionPolicy` est défini sur conserver. Cela permet de s'assurer que le back-end est toujours présent et peut être géré à l'aide de `tridentctl`.

Exécutez la commande suivante :

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

ASTRA Trident ne supprime pas les secrets Kubernetes utilisés par `TridentBackendConfig`. L'utilisateur Kubernetes est chargé de nettoyer les secrets. Il faut faire attention lors de la suppression des secrets. Vous devez supprimer les secrets uniquement s'ils ne sont pas utilisés par les systèmes back-end.

#### Afficher les systèmes back-end 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 la liste de tous les systèmes back-end existants. Cette liste inclura également les systèmes back-end créés avec `tridentctl`.

#### Mettre à jour un back-end

Il peut y avoir plusieurs raisons de mettre à jour un backend :

- Les informations d'identification du système de stockage ont été modifiées. Pour mettre à jour les informations d'identification, le secret Kubernetes utilisé dans l'``TridentBackendConfig`` objet doit être mis à jour. Avec Astra Trident, le système back-end est automatiquement mis à jour avec les dernières informations d'identification fournies. Exécutez la commande suivante pour mettre à jour le code secret Kubernetes :

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

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

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

- Vous pouvez également modifier la CR existante à l'aide de la commande suivante :

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

-  i
- En cas d'échec d'une mise à jour du back-end, le système back-end continue de rester dans sa dernière configuration connue. Vous pouvez afficher les journaux pour 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 `update`.

## Gestion back-end avec tridentctl

Découvrez comment effectuer des opérations de gestion back-end à l'aide de `tridentctl`.

### Créer un back-end

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

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

Si la création du système back-end échoue, la configuration du système back-end était erronée. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs -n trident
```

Une fois que vous avez identifié et corrigé le problème avec le fichier de configuration, il vous suffit d'exécuter à nouveau la `create` commande.

### Supprimer un back-end

Pour supprimer un back-end d'Astra Trident, procédez comme suit :

1. Récupérer le nom du système back-end :

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

2. Supprimer le backend :

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



Si Astra Trident a provisionné des volumes et des snapshots à partir de ce backend qui existe toujours, la suppression du back-end empêche les nouveaux volumes d'être provisionnés. Le système back-end continuera à exister dans un état « Suppression » et Trident continuera à gérer ces volumes et ces snapshots jusqu'à leur suppression.

#### Affichez les systèmes back-end existants

Pour afficher les systèmes back-end dont Trident a conscience, procédez comme suit :

- Pour obtenir un récapitulatif, 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 back-end

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

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

En cas d'échec de la mise à jour back-end, quelque chose était incorrect avec la configuration back-end ou vous avez tenté une mise à jour non valide. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs -n trident
```

Une fois que vous avez identifié et corrigé le problème avec le fichier de configuration, il vous suffit d'exécuter à nouveau la `update` commande.

#### Identifier les classes de stockage qui utilisent un système back-end

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

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

Cela s'applique également aux systèmes back-end créés par l'utilisation de `TridentBackendConfig`.

## Passez d'une option de gestion back-end à une autre

Découvrez les différentes façons de gérer les systèmes back-end avec Astra Trident.

### Options de gestion des systèmes back-end

Avec l'introduction de `TridentBackendConfig`, les administrateurs disposent désormais de deux méthodes uniques de gestion des systèmes back-end. Ceci pose les questions suivantes :

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

### Gestion des `tridentctl` systèmes back-end avec `TridentBackendConfig`

Cette section décrit les étapes requises pour gérer les systèmes back-end créés `tridentctl` directement via l'interface Kubernetes en créant `TridentBackendConfig` des objets.

Cela s'applique aux scénarios suivants :

- Systèmes back-end existants, qui n'ont pas de système `TridentBackendConfig` parce qu'ils ont été créés avec `tridentctl`.
- Nouveaux systèmes back-end créés avec `tridentctl`, alors que d'autres `TridentBackendConfig` objets existent.

Dans les deux cas, le système back-end restera présent. Avec Astra Trident, qui planifie les volumes et les exécute. Les administrateurs peuvent choisir l'une des deux options suivantes :

- Continuez à utiliser `tridentctl` pour gérer les systèmes back-end créés à l'aide de celui-ci.
- Lier les systèmes back-end créés à l'aide d'`tridentctl` à un nouvel `TridentBackendConfig` objet. Cela signifie que les systèmes back-end seront gérés sans utilisation `kubectl tridentctl`.

Pour gérer un back-end pré-existant à l'aide de `kubectl`, vous devez créer un `TridentBackendConfig` qui se lie au back-end existant. Voici un aperçu du fonctionnement de ces éléments :

1. Créez un code secret Kubernetes. Le secret est qu'Astra Trident doit communiquer avec le cluster/service de stockage.
2. Créer un `TridentBackendConfig` objet. Elle 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 back-end existant.

### Étape 0 : identifier le back-end

Pour créer un `TridentBackendConfig` qui se lie à un back-end existant, vous devez obtenir la configuration back-end. Dans cet exemple, supposons qu'un back-end a 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 : créez un code secret Kubernetes

Créez un secret qui contient les informations d'identification du back-end, 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 une TridentBackendConfig demande de modification

L'étape suivante consiste à créer une `TridentBackendConfig` demande de modification qui sera automatiquement lié au pré-existant `ontap-nas-backend` (comme dans cet exemple). Assurez-vous que les exigences suivantes sont respectées :

- Le même nom de back-end est défini dans `spec.backendName`.
- Les paramètres de configuration sont identiques au back-end d'origine.
- Les pools virtuels (le cas échéant) doivent conserver le même ordre que dans le back-end d'origine.
- Les identifiants sont fournis via un code secret Kubernetes et non en texte brut.

Dans ce cas, le `se` `TridentBackendConfig` présente comme suit :

```

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: mysql
        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 : vérifier l'état du TridentBackendConfig CR

Une fois le TridentBackendConfig créé, sa phase doit être Bound. Il devrait également refléter le même nom de back-end et UUID que celui du back-end existant.

```

kubectl get tbc tbc-ontap-nas-backend -n trident
NAME                  BACKEND NAME      BACKEND UUID
PHASE    STATUS
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
| STATE  | VOLUMES | 
+-----+-----+
+-----+-----+-----+
| ontap-nas-backend | ontap-nas      | 52f2eb10-e4c6-4160-99fc-
96b3be5ab5d7 | online |      25 |
+-----+-----+
+-----+-----+-----+

```

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

#### Gestion des TridentBackendConfig systèmes back-end avec tridentctl

`tridentctl` elle peut être utilisée pour lister les systèmes back-end créés à l'aide de `TridentBackendConfig`. En outre, les administrateurs peuvent choisir de gérer intégralement ces systèmes back-end `tridentctl` en supprimant et en `TridentBackendConfig` veillant à ce que `spec.deletionPolicy` soit défini sur `retain`.

#### Étape 0 : identifier le back-end

Supposons, par exemple, que le backend suivant a 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 |
+-----+-----+
+-----+-----+

```

A partir de la sortie, il est vu 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`. Ce paramètre doit être défini sur `retain`. Cela permet de s'assurer que lorsqu'une `TridentBackendConfig` demande de modification est supprimée, la définition du back-end est toujours présente et peut 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, sauf si `deletionPolicy` est défini sur `retain`.

## Étape 2 : supprimez la `TridentBackendConfig CR`

La dernière étape consiste à supprimer la `TridentBackendConfig` demande de modification. Après avoir confirmé que `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 `TridentBackendConfig` l'objet, Astra Trident le supprime simplement sans vraiment supprimer le back-end lui-même.

# Créer et gérer des classes de stockage

## Créer une classe de stockage

Configurez un objet `StorageClass` Kubernetes et créez la classe de stockage pour indiquer à Astra Trident comment provisionner les volumes.

### Configuration d'un objet `StorageClass` Kubernetes

Le système "[Objet classe de stockage Kubernetes](#)" identifie Astra Trident en tant que mécanisme de provisionnement utilisé pour cette classe et indique à Astra Trident comment provisionner un volume. Par exemple :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: <Name>
provisioner: csi.trident.netapp.io
mountOptions: <Mount Options>
parameters:
  <Trident Parameters>
allowVolumeExpansion: true
volumeBindingMode: Immediate
```

Reportez-vous "[Kubernetes et objets Trident](#)" à pour plus de détails sur l'interaction des classes de stockage avec les PersistentVolumeClaim paramètres et pour le contrôle de la façon dont Astra Trident provisionne les volumes.

## Créer une classe de stockage

Après avoir créé l'objet StorageClass, vous pouvez créer la classe de stockage. [Échantillons de classe de stockage](#) fournit des exemples de base que vous pouvez utiliser ou modifier.

### Étapes

1. Il s'agit d'un objet Kubernetes. Utilisez donc `kubectl` pour le créer dans Kubernetes.

```
kubectl create -f sample-input/storage-class-basic-csi.yaml
```

2. Vous devriez désormais voir une classe de stockage **Basic-csi** dans Kubernetes et Astra Trident. Astra Trident devrait avoir découvert les pools sur le système back-end.

```

kubectl get sc basic-csi
NAME          PROVISIONER          AGE
basic-csi     csi.trident.netapp.io  15h

./tridentctl -n trident get storageclass basic-csi -o json
{
  "items": [
    {
      "Config": {
        "version": "1",
        "name": "basic-csi",
        "attributes": {
          "backendType": "ontap-nas"
        },
        "storagePools": null,
        "additionalStoragePools": null
      },
      "storage": {
        "ontapnas_10.0.0.1": [
          "aggr1",
          "aggr2",
          "aggr3",
          "aggr4"
        ]
      }
    }
  ]
}

```

### Échantillons de classe de stockage

ASTRA Trident offre ["définition simple de classes de stockage pour des systèmes back-end spécifiques"](#).

Vous pouvez également modifier `sample-input/storage-class-csi.yaml.templ` le fichier fourni avec le programme d'installation et le remplacer `BACKEND_TYPE` par le nom du pilote de stockage.

```

./tridentctl -n trident get backend
+-----+-----+
+-----+-----+
|     NAME      | STORAGE DRIVER |                         UUID          |
STATE  | VOLUMES  |
+-----+-----+
+-----+-----+
| nas-backend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |          0 |
+-----+-----+
+-----+-----+
cp sample-input/storage-class-csi.yaml.template sample-input/storage-class-
basic-csi.yaml

# Modify __BACKEND_TYPE__ with the storage driver field above (e.g.,
ontap-nas)
vi sample-input/storage-class-basic-csi.yaml

```

## Gérer les classes de stockage

Vous pouvez afficher les classes de stockage existantes, définir une classe de stockage par défaut, identifier le back-end de la classe de stockage et supprimer les classes de stockage.

### Afficher les classes de stockage existantes

- Pour afficher les classes de stockage Kubernetes existantes, exécutez la commande suivante :

```
kubectl get storageclass
```

- Pour afficher les détails de la classe de stockage Kubernetes, exécutez la commande suivante :

```
kubectl get storageclass <storage-class> -o json
```

- Pour afficher les classes de stockage synchronisées d'Astra Trident, exécutez la commande suivante :

```
tridentctl get storageclass
```

- Pour afficher les détails de la classe de stockage synchronisée d'Astra Trident, exécutez la commande suivante :

```
tridentctl get storageclass <storage-class> -o json
```

## Définir une classe de stockage par défaut

Kubernetes 1.6 a ajouté la possibilité de définir une classe de stockage par défaut. Cette classe de stockage sera utilisée pour provisionner un volume persistant si un utilisateur ne en spécifie pas une dans une demande de volume persistant.

- Définissez une classe de stockage par défaut en définissant l'annotation `storageclass.kubernetes.io/is-default-class` sur `true` dans la définition de la classe de stockage. Selon la spécification, toute autre valeur ou absence de l'annotation est interprétée comme fausse.
- Vous pouvez configurer une classe de stockage existante comme classe de stockage par défaut à l'aide de la commande suivante :

```
kubectl patch storageclass <storage-class-name> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

- De même, vous pouvez supprimer l'annotation de classe de stockage par défaut à l'aide de la commande suivante :

```
kubectl patch storageclass <storage-class-name> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

Il existe également des exemples dans le bundle du programme d'installation de Trident qui incluent cette annotation.



Votre cluster ne doit contenir qu'une seule classe de stockage par défaut à la fois. Kubernetes n'empêche pas techniquement d'en avoir plusieurs, mais il se comporte comme s'il n'existe aucune classe de stockage par défaut.

## Identifier le système back-end pour une classe de stockage

Voici un exemple du type de questions que vous pouvez répondre avec le fichier JSON qui `tridentctl` affiche pour les objets backend Astra Trident. Cela utilise l' `jq` utilitaire, que vous devrez peut-être installer en premier.

```
tridentctl get storageclass -o json | jq '[.items[] | {storageClass: .Config.name, backends: [.storage] | unique}]'
```

## Supprimer une classe de stockage

Pour supprimer une classe de stockage de Kubernetes, exécutez la commande suivante :

```
kubectl delete storageclass <storage-class>
```

<storage-class> doit être remplacé par votre classe de stockage.

Tout volume persistant créé dans le cadre de cette classe de stockage n'est pas affecté. Astra Trident va continuer à les gérer.



ASTRA Trident applique un espace vide `fsType` aux volumes qu'il crée. Pour les systèmes back-end iSCSI, il est recommandé d'appliquer la `parameters.fsType` classe de stockage. Vous devez supprimer les classes de stockage existantes et les recréer avec les classes `parameters.fsType` spécifiées.

## Provisionnement et gestion des volumes

### Provisionner un volume

Créez un volume persistant et une demande de volume persistant qui utilisent la classe de stockage Kubernetes configurée pour demander l'accès au volume persistant. Vous pouvez ensuite monter le volume persistant sur un pod.

#### Présentation

Un "[Volume persistant](#)" (PV) est une ressource de stockage physique provisionnée par l'administrateur du cluster sur un cluster Kubernetes. La "[PersistentVolumeClaim](#)" demande de volume persistant est une demande d'accès au volume persistant sur le cluster.

Le PVC peut être configuré pour demander un stockage d'une certaine taille ou d'un certain mode d'accès. À l'aide de la classe de stockage associée, l'administrateur du cluster peut contrôler plus que la taille du volume persistant et le mode d'accès, tels que les performances ou le niveau de service.

Après avoir créé le volume persistant et la demande de volume persistant, vous pouvez monter le volume dans un pod.

#### Exemples de manifestes

## Exemple de manifeste de volume persistant

Cet exemple de manifeste montre un volume persistant de base de 10Gi associé à StorageClass basic-csi.

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: pv-storage
  labels:
    type: local
spec:
  storageClassName: basic-csi
  capacity:
    storage: 10Gi
  accessModes:
    - ReadWriteOnce
  hostPath:
    path: "/my/host/path"
```

## Exemples de manifestes de demande de volume persistant

Ces exemples présentent les options de configuration de base de la PVC.

### PVC avec accès RWO

Cet exemple montre une demande de volume persistant de base avec accès RWO associée à une classe de stockage nommée basic-csi.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

### PVC avec NVMe/TCP

Cet exemple montre une demande de volume persistant de base pour NVMe/TCP avec accès RWO associée à une classe de stockage nommée protection-gold.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san-nvme
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 300Mi
  storageClassName: protection-gold
```

## Échantillons de manifeste de pod

Ces exemples présentent les configurations de base pour fixer la demande de volume persistant à un pod.

### Configuration de base

```
kind: Pod
apiVersion: v1
metadata:
  name: pv-pod
spec:
  volumes:
    - name: pv-storage
      persistentVolumeClaim:
        claimName: basic
  containers:
    - name: pv-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
  volumeMounts:
    - mountPath: "/my/mount/path"
      name: pv-storage
```

## Configuration NVMe/TCP de base

```
---
apiVersion: v1
kind: Pod
metadata:
  creationTimestamp: null
  labels:
    run: nginx
    name: nginx
spec:
  containers:
    - image: nginx
      name: nginx
      resources: {}
  volumeMounts:
    - mountPath: "/usr/share/nginx/html"
      name: task-pv-storage
  dnsPolicy: ClusterFirst
  restartPolicy: Always
  volumes:
    - name: task-pv-storage
      persistentVolumeClaim:
        claimName: pvc-san-nvme
```

## Créer le volume persistant et la demande de volume persistant

### Étapes

1. Créer la PV.

```
kubectl create -f pv.yaml
```

2. Vérifiez l'état du PV.

```
kubectl get pv
NAME      CAPACITY  ACCESS MODES  RECLAIM POLICY  STATUS      CLAIM
STORAGECLASS  REASON  AGE
pv-storage  4Gi      RWO          Retain        Available
7s
```

3. Créer la PVC.

```
kubectl create -f pvc.yaml
```

4. Vérifiez l'état de la demande de volume persistant.

```
kubectl get pvc
NAME          STATUS  VOLUME      CAPACITY  ACCESS MODES  STORAGECLASS  AGE
pvc-storage   Bound   pv-name   2Gi        RWO          5m
```

5. Montez le volume dans un pod.

```
kubectl create -f pv-pod.yaml
```



Vous pouvez surveiller la progression à l'aide de `kubectl get pod --watch`.

6. Vérifiez que le volume est monté sur `/my/mount/path`.

```
kubectl exec -it task-pv-pod -- df -h /my/mount/path
```

7. Vous pouvez maintenant supprimer le Pod. L'application Pod n'existera plus, mais le volume restera.

```
kubectl delete pod task-pv-pod
```

Reportez-vous "[Kubernetes et objets Trident](#)" à pour plus de détails sur l'interaction des classes de stockage avec les `PersistentVolumeClaim` paramètres et pour le contrôle de la façon dont Astra Trident provisionne les volumes.

## Développement des volumes

Astra Trident permet aux utilisateurs de Kubernetes d'étendre leurs volumes après leur création. Trouvez des informations sur les configurations requises pour développer les volumes iSCSI et NFS.

### Développez un volume iSCSI

Vous pouvez développer un volume persistant iSCSI à l'aide du mécanisme de provisionnement CSI.



L'extension de volume iSCSI est prise en charge par les `ontap-san` `solidfire-san` pilotes, `ontap-san-economy` et requiert Kubernetes 1.16 et versions ultérieures.

#### Étape 1 : configurer la classe de stockage pour prendre en charge l'extension de volume

Modifiez la définition de classe de stockage pour définir le `allowVolumeExpansion` champ sur `true`.

```
cat storageclass-ontapsan.yaml
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-san
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
allowVolumeExpansion: True
```

Pour une classe de stockage existante, modifiez-la pour inclure le `allowVolumeExpansion` paramètre.

#### Étape 2 : créez une demande de volume persistant avec la classe de stockage que vous avez créée

Modifiez la définition de la PVC et mettez à jour le `spec.resources.requests.storage` pour refléter la nouvelle taille souhaitée, qui doit être supérieure à la taille d'origine.

```
cat pvc-ontapsan.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: san-pvc
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-san
```

Astra Trident crée un volume persistant qui l'associe à cette demande de volume persistant.

```
kubectl get pvc
NAME      STATUS      VOLUME                                     CAPACITY
ACCESS MODES      STORAGECLASS      AGE
san-pvc    Bound      pvc-8a814d62-bd58-4253-b0d1-82f2885db671   1Gi
RWO                  ontap-san      8s

kubectl get pv
NAME                                     CAPACITY      ACCESS MODES
RECLAIM POLICY      STATUS      CLAIM      STORAGECLASS      REASON      AGE
pvc-8a814d62-bd58-4253-b0d1-82f2885db671   1Gi          RWO
Delete      Bound      default/san-pvc      ontap-san      10s
```

### Étape 3 : définissez un pod qui fixe la demande de volume persistant

Reliez le volume persistant à un pod pour qu'il soit redimensionné. Lors du redimensionnement d'un volume persistant iSCSI, deux scénarios sont possibles :

- Si le volume persistant est connecté à un pod, Astra Trident étend le volume en back-end, reanalyse le système et redimensionne le système de fichiers.
- Pour redimensionner un volume persistant non connecté, Astra Trident étend le volume sur le back-end. Une fois le volume de volume persistant lié à un pod, Trident analyse de nouveau le périphérique et redimensionne le système de fichiers. Kubernetes met ensuite à jour la taille de la demande de volume persistant une fois l'opération d'extension terminée.

Dans cet exemple, un pod est créé et utilise le san-pvc.

```

kubectl get pod
NAME          READY   STATUS    RESTARTS   AGE
ubuntu-pod    1/1     Running   0          65s

kubectl describe pvc san-pvc
Name:          san-pvc
Namespace:     default
StorageClass:  ontap-san
Status:        Bound
Volume:        pvc-8a814d62-bd58-4253-b0d1-82f2885db671
Labels:        <none>
Annotations:   pv.kubernetes.io/bind-completed: yes
                pv.kubernetes.io/bound-by-controller: yes
                volume.beta.kubernetes.io/storage-provisioner:
                csi.trident.netapp.io
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:      1Gi
Access Modes:  RWO
VolumeMode:    Filesystem
Mounted By:   ubuntu-pod

```

#### Étape 4 : développez le volume persistant

Pour redimensionner la PV créée de 1Gi à 2Gi, modifiez la définition de la PVC et mettez à jour le spec.resources.requests.storage à 2Gi.

```

kubectl edit pvc san-pvc
# Please edit the object below. Lines beginning with a '#' will be
ignored,
# and an empty file will abort the edit. If an error occurs while saving
this file will be
# reopened with the relevant failures.
#
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    pv.kubernetes.io/bind-completed: "yes"
    pv.kubernetes.io/bound-by-controller: "yes"
    volume.beta.kubernetes.io/storage-provisioner: csi.trident.netapp.io
  creationTimestamp: "2019-10-10T17:32:29Z"
  finalizers:
  - kubernetes.io/pvc-protection
  name: san-pvc
  namespace: default
  resourceVersion: "16609"
  selfLink: /api/v1/namespaces/default/persistentvolumeclaims/san-pvc
  uid: 8a814d62-bd58-4253-b0d1-82f2885db671
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 2Gi
...

```

#### Étape 5 : validation de l'extension

Vous pouvez valider le bon fonctionnement de l'extension en contrôlant la taille de la demande de volume persistant, du volume persistant et du volume Astra Trident :

```

kubectl get pvc san-pvc
NAME      STATUS      VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
san-pvc    Bound      pvc-8a814d62-bd58-4253-b0d1-82f2885db671  2Gi
RWO          ontap-san   11m

kubectl get pv
NAME                                     CAPACITY  ACCESS MODES
RECLAIM POLICY  STATUS      CLAIM      STORAGECLASS  REASON  AGE
pvc-8a814d62-bd58-4253-b0d1-82f2885db671  2Gi        RWO
Delete        Bound      default/san-pvc  ontap-san           12m

tridentctl get volumes -n trident
+-----+-----+-----+
+-----+-----+-----+
|           NAME           | SIZE   | STORAGE CLASS |
PROTOCOL |           BACKEND UUID           | STATE  | MANAGED  |
+-----+-----+-----+
+-----+-----+-----+
| pvc-8a814d62-bd58-4253-b0d1-82f2885db671 | 2.0 GiB | ontap-san    |
block    | a9b7bfff-0505-4e31-b6c5-59f492e02d33 | online | true      |
+-----+-----+-----+
+-----+-----+-----+

```

## Développez un volume NFS

ASTRA Trident prend en charge l'extension de volume pour les volumes NFS PVS provisionnés sur ontap-nas, ontap-nas-economy, ontap-nas-flexgroup gcp-cvs et les azure-netapp-files systèmes back-end.

### Étape 1 : configurer la classe de stockage pour prendre en charge l'extension de volume

Pour redimensionner un PV NFS, l'administrateur doit d'abord configurer la classe de stockage pour permettre l'extension du volume en définissant le `allowVolumeExpansion` champ sur `true`:

```

cat storageclass-ontapnas.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontapnas
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
allowVolumeExpansion: true

```

Si vous avez déjà créé une classe de stockage sans cette option, vous pouvez simplement modifier la classe de stockage existante en utilisant `kubectl edit storageclass` pour autoriser l'extension de volume.

## Étape 2 : créez une demande de volume persistant avec la classe de stockage que vous avez créée

```
cat pvc-ontapnas.yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: ontapnas20mb
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 20Mi
  storageClassName: ontapnas
```

Astra Trident doit créer un volume persistant NFS 20MiB pour cette demande de volume persistant :

```
kubectl get pvc
NAME           STATUS    VOLUME
CAPACITY      ACCESS MODES  STORAGECLASS      AGE
ontapnas20mb  Bound     pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  20Mi
RWO           ontapnas   9s

kubectl get pv pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7
NAME
RECLAIM POLICY  STATUS    CLAIM
AGE
pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  20Mi      RWO
Delete        Bound     default/ontapnas20mb  ontapnas
2m42s
```

## Étape 3 : développez le volume persistant

Pour redimensionner le nouveau volume persistant de 20 Mio à 1 Gio, modifiez la demande de volume persistant et définissez `spec.resources.requests.storage` cette valeur sur 1 Gio :

```

kubectl edit pvc ontapnas20mb
# Please edit the object below. Lines beginning with a '#' will be
ignored,
# and an empty file will abort the edit. If an error occurs while saving
this file will be
# reopened with the relevant failures.
#
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    pv.kubernetes.io/bind-completed: "yes"
    pv.kubernetes.io/bound-by-controller: "yes"
    volume.beta.kubernetes.io/storage-provisioner: csi.trident.netapp.io
  creationTimestamp: 2018-08-21T18:26:44Z
  finalizers:
  - kubernetes.io/pvc-protection
  name: ontapnas20mb
  namespace: default
  resourceVersion: "1958015"
  selfLink: /api/v1/namespaces/default/persistentvolumeclaims/ontapnas20mb
  uid: c1bd7fa5-a56f-11e8-b8d7-fa163e59eaab
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
...

```

#### Étape 4 : validation de l'extension

Vous pouvez valider le redimensionnement correctement en contrôlant la taille de la demande de volume persistant, de la volume persistant et du volume Astra Trident :

```

kubectl get pvc ontapnas20mb
NAME           STATUS  VOLUME
CAPACITY      ACCESS MODES  STORAGECLASS      AGE
ontapnas20mb  Bound    pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  1Gi
RWO           ontapnas  4m44s

kubectl get pv pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7
NAME
RECLAIM POLICY  STATUS  CLAIM
AGE
pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7  1Gi      RWO
Delete        Bound    default/ontapnas20mb  ontapnas
5m35s

tridentctl get volume pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7 -n trident
+-----+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE  | STORAGE CLASS  |
PROTOCOL |           BACKEND UUID           | STATE  | MANAGED  |
+-----+-----+-----+
+-----+-----+-----+
| pvc-08f3d561-b199-11e9-8d9f-5254004dfdb7 | 1.0 GiB | ontapnas      |
file     | c5a6f6a4-b052-423b-80d4-8fb491a14a22 | online | true      |
+-----+-----+-----+
+-----+-----+-----+

```

## Importer des volumes

Vous pouvez importer des volumes de stockage existants en tant que volume persistant Kubernetes à l'aide de `tridentctl import`.

### Présentation et considérations

Vous pouvez importer un volume dans Astra Trident et :

- Conteneurisation d'une application et réutilisation de son jeu de données existant
- Utilisez un clone d'un jeu de données pour une application éphémère
- Reconstruction d'un cluster Kubernetes en panne
- Migration des données applicatives pendant la reprise après incident

### Considérations

Avant d'importer un volume, consultez les considérations suivantes.

- ASTRA Trident peut importer des volumes ONTAP de type RW (lecture-écriture) uniquement. Les volumes de type DP (protection des données) sont des volumes de destination SnapMirror. Vous devez rompre la relation de miroir avant d'importer le volume dans Astra Trident.

- Nous vous suggérons d'importer des volumes sans connexions actives. Pour importer un volume activement utilisé, clonez-le, puis effectuez l'importation.



C'est particulièrement important pour les volumes en mode bloc, car Kubernetes ignorerait la connexion précédente et pourrait facilement relier un volume actif à un pod. Cela peut entraîner une corruption des données.

- Bien qu' `StorageClass` il doive être spécifié sur une demande de volume persistant, Astra Trident n'utilise pas ce paramètre lors de l'importation. Les classes de stockage sont utilisées lors de la création du volume pour sélectionner un pool disponible en fonction des caractéristiques de stockage. Comme le volume existe déjà, aucune sélection de pool n'est requise pendant l'importation. Par conséquent, l'importation n'échouera pas même si le volume existe sur un back-end ou un pool qui ne correspond pas à la classe de stockage spécifiée dans le PVC.
- La taille du volume existant est déterminée et définie dans la PVC. Une fois le volume importé par le pilote de stockage, le volume persistant est créé avec un SécurRef dans la demande de volume persistant.
  - La règle de récupération est initialement définie sur `retain` dans le volume persistant. Une fois que Kubernetes a réussi à relier la demande de volume persistant et le volume persistant, la règle de récupération est mise à jour pour correspondre à la règle de récupération de la classe de stockage.
  - Si la règle de récupération de la classe de stockage est `delete`, le volume de stockage sera supprimé lors de la suppression du volume persistant.
- Par défaut, Astra Trident gère la demande de volume persistant et renomme le FlexVol et le LUN sur le back-end. Vous pouvez passer `--no-manage` l'indicateur pour importer un volume non géré. Si vous utilisez `--no-manage`, Astra Trident n'exécute aucune opération supplémentaire sur la demande de volume persistant ou le volume persistant pour le cycle de vie des objets. Le volume de stockage n'est pas supprimé lorsque le volume persistant est supprimé et d'autres opérations telles que le clone de volume et le redimensionnement de volume sont également ignorées.



Cette option est utile si vous souhaitez utiliser Kubernetes pour des workloads conteneurisés, mais que vous souhaitez gérer le cycle de vie du volume de stockage en dehors de Kubernetes.

- Une annotation est ajoutée pour la demande de volume persistant et la volume persistant, qui servent un double objectif : indiquer l'importation du volume et gérer la demande de volume persistant. Cette annotation ne doit pas être modifiée ni supprimée.

## Importer un volume

Vous pouvez utiliser `tridentctl import` pour importer un volume.

### Étapes

1. Créez le fichier de demande de volume persistant (PVC) (par exemple ) qui sera utilisé pour créer la demande de volume persistant `pvc.yaml`. Le fichier PVC doit inclure `name`, `namespace`, `accessModes` et `storageClassName`. Vous pouvez également spécifier `unixPermissions` dans votre définition de PVC.

Voici un exemple de spécification minimale :

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: my_claim
  namespace: my_namespace
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: my_storage_class
```



N'incluez pas de paramètres supplémentaires tels que le nom du volume persistant ou la taille du volume. Cela peut entraîner l'échec de la commande d'importation.

2. Utilisez `tridentctl import` la commande pour spécifier le nom du back-end Astra Trident contenant le volume et le nom qui identifie de manière unique le volume sur le stockage (par exemple : ONTAP FlexVol, Element Volume, chemin Cloud Volumes Service). L' `-f` argument est requis pour spécifier le chemin d'accès au fichier PVC.

```
tridentctl import volume <backendName> <volumeName> -f <path-to-pvc-file>
```

## Exemples

Consultez les exemples d'importation de volume suivants pour les pilotes pris en charge.

### NAS ONTAP et FlexGroup NAS ONTAP

ASTRA Trident prend en charge l'importation de volumes à l'aide des `ontap-nas` pilotes et `ontap-nas-flexgroup`.



- Le `ontap-nas-economy` pilote ne peut pas importer et gérer des qtrees.
- Les `ontap-nas` pilotes et `ontap-nas-flexgroup` n'autorisent pas les noms de volumes dupliqués.

Chaque volume créé avec le `ontap-nas` pilote est un FlexVol sur le cluster ONTAP. L'importation de volumes FlexVol avec `ontap-nas` le pilote fonctionne de la même manière. Une FlexVol qui existe déjà sur un cluster ONTAP peut être importée en tant que `ontap-nas` demande de volume persistant. De même, les volumes FlexGroup peuvent être importés en tant que `ontap-nas-flexgroup` ESV.

### Exemples de NAS ONTAP

Voici un exemple d'importation de volume géré et de volume non géré.

## Volume géré

L'exemple suivant importe un volume nommé `managed_volume` sur un back-end nommé `ontap_nas`:

```
tridentctl import volume ontap_nas managed_volume -f <path-to-pvc-file>

+-----+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE   | STORAGE CLASS  |
PROTOCOL |           BACKEND UUID           |  STATE  |  MANAGED  |
+-----+-----+-----+
+-----+-----+-----+
| pvc-bf5ad463-afbb-11e9-8d9f-5254004dfdb7 | 1.0 GiB | standard      |
file      | c5a6f6a4-b052-423b-80d4-8fb491a14a22 | online   | true       |
+-----+-----+-----+
+-----+-----+-----+
```

## Volume non géré

Lors de l'utilisation de l'``--no-manage`` argument, Astra Trident ne renomme pas le volume.

L'exemple suivant importe `unmanaged_volume` sur le `ontap_nas` back-end :

```
tridentctl import volume nas_blog unmanaged_volume -f <path-to-pvc-
file> --no-manage

+-----+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE   | STORAGE CLASS  |
PROTOCOL |           BACKEND UUID           |  STATE  |  MANAGED  |
+-----+-----+-----+
+-----+-----+-----+
| pvc-df07d542-afbc-11e9-8d9f-5254004dfdb7 | 1.0 GiB | standard      |
file      | c5a6f6a4-b052-423b-80d4-8fb491a14a22 | online   | false       |
+-----+-----+-----+
+-----+-----+-----+
```

## SAN ONTAP

ASTRA Trident prend en charge l'importation de volume à l'aide du `ontap-san` pilote. L'importation de volume n'est pas prise en charge à l'aide du `ontap-san-economy` pilote.

ASTRA Trident peut importer des volumes ONTAP SAN FlexVols qui contiennent un LUN unique. Cela est cohérent avec le `ontap-san` pilote, qui crée une FlexVol pour chaque demande de volume persistant et une LUN au sein de la FlexVol. ASTRA Trident importe le FlexVol et l'associe à la définition de l'ESV.

## Exemples de SAN ONTAP

Voici un exemple d'importation de volume géré et de volume non géré.

### Volume géré

Pour les volumes gérés, Astra Trident renomme le FlexVol au `pvc-<uuid>` format et le LUN dans le FlexVol à `lun0`.

L'exemple suivant importe le `ontap-san-managed` FlexVol présent sur le `ontap_san_default` back-end :

```
tridentctl import volume ontapsan_san_default ontap-san-managed -f pvc-
basic-import.yaml -n trident -d

+-----+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE  | STORAGE CLASS |
PROTOCOL |           BACKEND UUID           | STATE | MANAGED |
+-----+-----+-----+
+-----+-----+-----+
| pvc-d6ee4f54-4e40-4454-92fd-d00fc228d74a | 20 MiB | basic      |
block    | cd394786-ddd5-4470-adc3-10c5ce4ca757 | online | true      |
+-----+-----+-----+
+-----+-----+-----+
```

### Volume non géré

L'exemple suivant importe `unmanaged_example_volume` sur le `ontap_san` back-end :

```
tridentctl import volume -n trident san_blog unmanaged_example_volume
-f pvc-import.yaml --no-manage
+-----+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE  | STORAGE CLASS |
PROTOCOL |           BACKEND UUID           | STATE | MANAGED |
+-----+-----+-----+
+-----+-----+-----+
| pvc-1fc999c9-ce8c-459c-82e4-ed4380a4b228 | 1.0 GiB | san-blog      |
block    | e3275890-7d80-4af6-90cc-c7a0759f555a | online | false      |
+-----+-----+-----+
+-----+-----+-----+
```

Si des LUN sont mappées à des igroups qui partagent un IQN avec un IQN de nœud Kubernetes, comme illustré dans l'exemple suivant, vous recevrez l'erreur : `LUN already mapped to initiator(s) in this group`. Vous devez supprimer l'initiateur ou annuler le mappage de la LUN pour importer le volume.

Vserver	Igroup	Protocol	OS	Type	Initiators
svm0	k8s-nodename.example.com-fe5d36f2-cded-4f38-9eb0-c7719fc2f9f3	iscsi	linux	iqn.1994-05.com.redhat:4c2e1cf35e0	
svm0	unmanaged-example-igroup	mixed	linux	iqn.1994-05.com.redhat:4c2e1cf35e0	

## Elément

ASTRA Trident prend en charge le logiciel NetApp Element et l'importation de volumes NetApp HCI à l'aide du solidfire-san pilote.



Le pilote d'élément prend en charge les noms de volume dupliqués. Toutefois, Astra Trident renvoie une erreur si des noms de volumes sont dupliqués. Pour contourner ce problème, clonez le volume, indiquez un nom de volume unique et importez le volume cloné.

## Exemple d'élément

L'exemple suivant importe un element-managed volume sur le back-end element\_default.

```
tridentctl import volume element_default element-managed -f pvc-basic-import.yaml -n trident -d

+-----+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE  | STORAGE CLASS  |
PROTOCOL |           BACKEND UUID           | STATE  | MANAGED  |
+-----+-----+-----+
+-----+-----+-----+
| pvc-970ce1ca-2096-4ecd-8545-ac7edc24a8fe | 10 GiB | basic-element |
block    | d3ba047a-ea0b-43f9-9c42-e38e58301c49 | online | true    |
+-----+-----+-----+
+-----+-----+-----+
```

## Google Cloud Platform

ASTRA Trident prend en charge l'importation de volume à l'aide du gcp-cvs pilote.



Pour importer un volume soutenu par NetApp Cloud Volumes Service dans Google Cloud Platform, identifiez le volume par son chemin d'accès au volume. Le chemin du volume est la partie du chemin d'exportation du volume après :/. Par exemple, si le chemin d'exportation est 10.0.0.1:/adroit-jolly-swift, le chemin du volume est adroit-jolly-swift.

## Exemple de Google Cloud Platform

L'exemple suivant importe un `gcp-cvs` volume sur le back-end `gcpcvs_YEppr` avec le chemin du volume de `adroit-jolly-swift`.

```
tridentctl import volume gcpcvs_YEppr adroit-jolly-swift -f <path-to-pvc-file> -n trident

+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE  | STORAGE CLASS | 
PROTOCOL |           BACKEND UUID           | STATE | MANAGED | 
+-----+-----+-----+
+-----+-----+-----+
| pvc-a46ccab7-44aa-4433-94b1-e47fc8c0fa55 | 93 GiB | gcp-storage | file
| e1a6e65b-299e-4568-ad05-4f0a105c888f | online | true     | 
+-----+-----+-----+
+-----+-----+-----+
```

## Azure NetApp Files

ASTRA Trident prend en charge l'importation de volume à l'aide du `azure-netapp-files` pilote.



Pour importer un volume Azure NetApp Files, identifiez-le par son chemin d'accès au volume. Le chemin du volume est la partie du chemin d'exportation du volume après `:/`. Par exemple, si le chemin de montage est `10.0.0.2:/importvol1`, le chemin du volume est `importvol1`.

## Exemple Azure NetApp Files

L'exemple suivant importe un `azure-netapp-files` volume sur le back-end `azurenappfiles_40517` avec le chemin du volume `importvol1`.

```
tridentctl import volume azurenappfiles_40517 importvol1 -f <path-to-pvc-file> -n trident

+-----+-----+
+-----+-----+-----+
|           NAME           |  SIZE  | STORAGE CLASS | 
PROTOCOL |           BACKEND UUID           | STATE | MANAGED | 
+-----+-----+-----+
+-----+-----+-----+
| pvc-0ee95d60-fd5c-448d-b505-b72901b3a4ab | 100 GiB | anf-storage | 
file     | 1c01274f-d94b-44a3-98a3-04c953c9a51e | online | true     | 
+-----+-----+-----+
+-----+-----+-----+
```

## Personnaliser les noms et les étiquettes des volumes

Avec Astra Trident, vous pouvez attribuer des noms et des étiquettes significatifs aux volumes que vous créez. Vous pouvez ainsi identifier et mapper facilement les volumes vers leurs ressources Kubernetes respectives. Vous pouvez également définir des modèles au niveau du back-end pour créer des noms de volume personnalisés et des étiquettes personnalisées. Tous les volumes que vous créez, importez ou clonez seront conformes aux modèles.

### Avant de commencer

Prise en charge des noms et des libellés de volumes personnalisables :

1. Opérations de création, d'importation et de clonage de volumes.
2. Dans le cas du pilote ontap-nas-Economy, seul le nom du volume Qtree est conforme au modèle de nom.
3. Dans le cas d'un pilote ontap-san-Economy, seul le nom de LUN est conforme au modèle de nom.

### Limites

1. Les noms de volume personnalisables sont uniquement compatibles avec les pilotes ONTAP sur site.
2. Les noms de volume personnalisables ne s'appliquent pas aux volumes existants.

### Comportements clés des noms de volume personnalisables

1. Si une défaillance survient en raison d'une syntaxe incorrecte dans un modèle de nom, la création du back-end échoue. Toutefois, si l'application modèle échoue, le volume sera nommé conformément à la convention de nommage existante.
2. Le préfixe de stockage n'est pas applicable lorsqu'un volume est nommé à l'aide d'un modèle de nom de la configuration back-end. Toute valeur de préfixe souhaitée peut être directement ajoutée au modèle.

### Exemples de configuration back-end avec modèle de nom et étiquettes

Les modèles de noms personnalisés peuvent être définis au niveau de la racine et/ou du pool.

## Exemple de niveau racine

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

## Exemple au niveau du pool

```
{  
  "version": 1,  
  "storageDriverName": "ontap-nas",  
  "backendName": "ontap-nfs-backend",  
  "managementLIF": "<ip address>",  
  "svm": "svm0",  
  "username": "<admin>",  
  "password": "<password>",  
  "useREST": true,  
  "storage": [  
    {  
      "labels": {"labelname": "label1", "name": "{{ .volume.Name }}"},  
      "defaults": {  
        "nameTemplate": "pool01_{{ .volume.Name }}_{{ .labels.cluster }}_{{ .volume.Namespace }}_{{ .volume.RequestName }}"  
      }  
    },  
    {  
      "labels": {"cluster": "label2", "name": "{{ .volume.Name }}"},  
      "defaults": {  
        "nameTemplate": "pool02_{{ .volume.Name }}_{{ .labels.cluster }}_{{ .volume.Namespace }}_{{ .volume.RequestName }}"  
      }  
    }  
  ]  
}
```

## Exemples de modèles de noms

### Exemple 1 :

```
"nameTemplate": "{{ .config.StoragePrefix }}_{{ .volume.Name }}_{{ .config.BackendName }}"
```

### Exemple 2 :

```
"nameTemplate": "pool_{{ .config.StoragePrefix }}_{{ .volume.Name }}_{{ slice .volume.RequestName 1 5 }}""
```

## Points à prendre en compte

1. Dans le cas des importations en volume, les étiquettes ne sont mises à jour que si le volume existant comporte des étiquettes dans un format spécifique. Par exemple :  

```
{"provisioning": {"Cluster": "ClusterA", "PVC": "pvcname"}}
```
2. Dans le cas des importations de volume gérées, le nom du volume suit le modèle de nom défini au niveau racine dans la définition du back-end.
3. ASTRA Trident ne prend pas en charge l'utilisation d'un opérateur Slice avec le préfixe de stockage.
4. Si les modèles ne donnent pas de noms de volumes uniques, Astra Trident ajoutera quelques caractères aléatoires pour créer des noms de volumes uniques.
5. Si le nom personnalisé d'un volume économique NAS dépasse 64 caractères, Astra Trident nommera les volumes conformément à la convention de nommage existante. Pour tous les autres pilotes ONTAP, si le nom du volume dépasse la limite de nom, le processus de création du volume échoue.

## Partager un volume NFS entre les espaces de noms

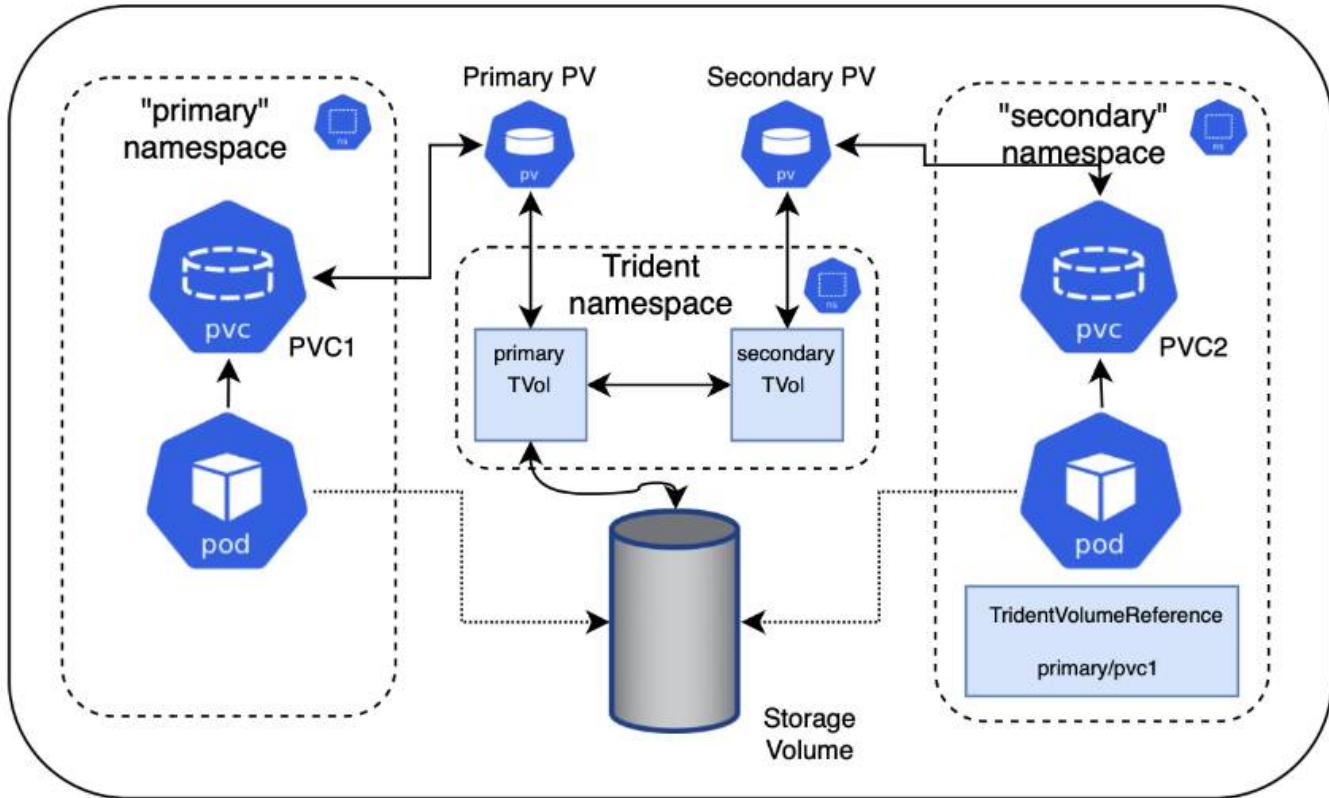
Avec Astra Trident, vous pouvez créer un volume dans un espace de noms principal et le partager dans un ou plusieurs espaces de noms secondaires.

### Caractéristiques

Le système Astra TridentVolumeReference CR vous permet de partager en toute sécurité des volumes NFS ReadWriteMany (RWX) sur un ou plusieurs espaces de noms Kubernetes. Cette solution Kubernetes-native présente plusieurs avantages :

- Plusieurs niveaux de contrôle d'accès pour assurer la sécurité
- Fonctionne avec tous les pilotes de volume NFS Trident
- Pas de dépendance à tridentctl ou à toute autre fonctionnalité Kubernetes non native

Ce schéma illustre le partage de volumes NFS entre deux espaces de noms Kubernetes.



## Démarrage rapide

Vous pouvez configurer le partage de volumes NFS en quelques étapes seulement.

1

### Configurez la PVC source pour partager le volume

Le propriétaire de l'espace de noms source autorise l'accès aux données dans la demande de volume persistant source.

2

### Accorder l'autorisation de créer une demande de modification dans l'espace de noms de destination

L'administrateur de cluster accorde l'autorisation au propriétaire de l'espace de noms de destination pour créer le CR TridentVolumeReference.

3

### Créer TridentVolumeReference dans l'espace de noms de destination

Le propriétaire de l'espace de noms de destination crée le CR TridentVolumeReference pour faire référence au PVC source.

4

### Créez la demande de volume persistant subordonnée dans l'espace de noms de destination

Le propriétaire de l'espace de noms de destination crée le PVC subalterne pour utiliser la source de données à partir du PVC source.

## Configurer les espaces de noms source et de destination

Pour garantir la sécurité, le partage de l'espace de noms croisé nécessite une collaboration et une action du propriétaire de l'espace de noms source, de l'administrateur de cluster et du propriétaire de l'espace de noms de destination. Le rôle utilisateur est désigné dans chaque étape.

### Étapes

1. **Propriétaire de l'espace de noms source** : Créez le PVC (pvc1) dans l'espace de noms source qui accorde l'autorisation de partager avec l'espace de noms de destination (namespace2) à l'aide de shareToNamespace l'annotation.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc1
  namespace: namespace1
  annotations:
    trident.netapp.io/shareToNamespace: namespace2
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: trident-csi
  resources:
    requests:
      storage: 100Gi
```

Astra Trident crée le volume persistant et son volume de stockage NFS back-end.

- Vous pouvez partager le PVC sur plusieurs espaces de noms à l'aide d'une liste délimitée par des virgules. Par exemple trident.netapp.io/shareToNamespace: namespace2, namespace3, namespace4, .
- Vous pouvez partager sur tous les espaces de noms à l'aide de \*. Par exemple, trident.netapp.io/shareToNamespace: \*
- Vous pouvez mettre à jour la demande de volume persistant pour inclure l' `shareToNamespace` annotation à tout moment.



2. **Cluster admin**: Créez le rôle personnalisé et kubeconfig pour accorder l'autorisation au propriétaire de l'espace de noms de destination de créer le CR TridentVolumeReference dans l'espace de noms de destination.
3. **Nom de l'espace de noms de destination propriétaire** : Créez un CR TridentVolumeReference dans l'espace de noms de destination qui fait référence à l'espace de noms source pvc1 .

```

apiVersion: trident.netapp.io/v1
kind: TridentVolumeReference
metadata:
  name: my-first-tvr
  namespace: namespace2
spec:
  pvcName: pvc1
  pvcNamespace: namespace1

```

4. **Propriétaire de l'espace de noms de destination** : Créez un PVC (namespace2)(pvc2 dans l'espace de noms de destination ) en utilisant shareFromPVC l'annotation pour désigner le PVC source.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  annotations:
    trident.netapp.io/shareFromPVC: namespace1/pvc1
  name: pvc2
  namespace: namespace2
spec:
  accessModes:
    - ReadWriteMany
  storageClassName: trident-csi
  resources:
    requests:
      storage: 100Gi

```



La taille du PVC de destination doit être inférieure ou égale à la PVC source.

## Résultats

ASTRA Trident lit l' `shareFromPVC`annotation sur la demande de volume persistant de destination et crée le volume persistant de destination en tant que volume subalterne sans ressource de stockage propre qui pointe vers le volume persistant source et partage la ressource de stockage PV source. La demande de volume persistant et la demande de volume persistant de destination apparaissent comme normales.

## Supprimer un volume partagé

Vous pouvez supprimer un volume partagé entre plusieurs namespaces. Astra Trident supprimera l'accès au volume de l'espace de noms source et maintiendra l'accès aux autres espaces de noms qui partagent le volume. Lorsque tous les namespaces qui réfèrent au volume sont supprimés, Astra Trident supprime le volume.

### `tridentctl get` Permet d'interroger les volumes subordonnés

A l'aide de l'[tridentctl`utilitaire, vous pouvez exécuter la `get` commande pour obtenir des volumes subordonnés. Pour plus d'informations, reportez-vous au lien .../Trident-

Usage:

```
tridentctl get [option]
```

Alarmes :

- `--parentOfSubordinate` string: Limiter la requête au volume source subordonné.
- `--subordinateOf` string: Limiter la requête aux subordonnés de volume.

## Limites

- Astra Trident ne peut pas empêcher les espaces de noms de destination d'écrire sur le volume partagé. Nous vous recommandons d'utiliser un verrouillage de fichiers ou d'autres processus pour éviter d'écraser les données du volume partagé.
- Vous ne pouvez pas révoquer l'accès au PVC source en supprimant les annotations ou ou `shareFromNamespace` en `shareToNamespace` supprimant la `TridentVolumeReference` demande de modification. Pour annuler l'accès, vous devez supprimer le PVC subalterne.
- Les snapshots, clones et la mise en miroir ne sont pas possibles sur les volumes subordonnés.

## Pour en savoir plus

Pour en savoir plus sur l'accès aux volumes multi-espaces de noms :

- Visitez "[Partage de volumes entre les espaces de noms : dites bonjour à l'accès aux volumes situés à l'échelle d'un espace de noms](#)".
- Regardez la démo sur "[NetAppTV](#)".

## RéPLICATION de volumes à l'aide de SnapMirror

À l'aide d'Astra Control Provisioner, vous pouvez créer des relations de miroir entre un volume source sur un cluster et le volume de destination sur le cluster peering pour la réPLICATION des données pour la reprise après incident. Vous pouvez utiliser une définition de ressource personnalisée (CRD) avec un espace de nom pour effectuer les opérations suivantes :

- Création de relations de symétrie entre les volumes (ESV)
- Supprimez les relations de symétrie entre les volumes
- Rompez les relations de symétrie
- Promotion du volume secondaire en cas d'incident (basculements)
- Transition sans perte des applications d'un cluster à un autre (en cas de basculements ou de migrations planifiés)

## Conditions préalables à la réPLICATION

Assurez-vous que les conditions préalables suivantes sont remplies avant de commencer :

### Clusters ONTAP

- **Astra Control Provisioner** : Astra Control Provisioner version 23.10 ou ultérieure doit exister sur les clusters Kubernetes source et de destination qui utilisent ONTAP en tant que backend.
- **Licences** : les licences asynchrones de SnapMirror ONTAP utilisant le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Pour plus d'informations, reportez-vous à la section "[Présentation des licences SnapMirror dans ONTAP](#)" .

### Peering

- **Cluster et SVM** : les systèmes back-end de stockage ONTAP doivent être peering. Pour plus d'informations, reportez-vous à la section "[Présentation du cluster et de SVM peering](#)" .



S'assurer que les noms de SVM utilisés dans la relation de réPLICATION entre deux clusters ONTAP sont uniques.

- **Astra Control Provisioner et SVM** : les SVM distants à peering doivent être disponibles pour Astra Control Provisioner sur le cluster de destination.

### Pilotes pris en charge

- La réPLICATION de volume est prise en charge pour les pilotes ontap-nas et ontap-san.

## Créer une demande de volume persistant en miroir

Suivez ces étapes et utilisez les exemples CRD pour créer une relation miroir entre les volumes principal et secondaire.

### Étapes

1. Effectuez les étapes suivantes sur le cluster Kubernetes principal :

- a. Créez un objet StorageClass avec le `trident.netapp.io/replication: true` paramètre.

#### Exemple

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  fsType: "nfs"
  trident.netapp.io/replication: "true"
```

- b. Créez une demande de volume persistant avec une classe de stockage précédemment créée.

### Exemple

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

- c. Créez une demande de modification MirrorRelationship avec des informations locales.

### Exemple

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

ASTRA Control Provisioner récupère les informations internes du volume et l'état actuel de la protection des données (DP) du volume, puis remplit le champ d'état de MirrorRelationship.

- d. Obtenir le CR TridentMirrorRelationship pour obtenir le nom interne et la SVM du PVC.

```
kubectl get tmr csi-nas
```

```

kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
    "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1

```

2. Effectuez les étapes suivantes sur le cluster Kubernetes secondaire :

- Créez une classe de stockage avec le paramètre `trident.netapp.io/replication: true`.

**Exemple**

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/replication: true

```

- Créez une demande de modification `MirrorRelationship` avec les informations de destination et de source.

**Exemple**

```

kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: established
  volumeMappings:
  - localPVCName: csi-nas
    remoteVolumeHandle:
    "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"

```

ASTRA Control Provisioner crée une relation SnapMirror avec le nom de la stratégie de relation configurée (ou par défaut pour ONTAP) et l'initialise.

- c. Créez une demande de volume persistant avec une classe de stockage précédemment créée pour agir en tant que classe secondaire (destination SnapMirror).

#### Exemple

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

ASTRA Control Provisioner vérifiera le CRD TridentMirrorRelationship et ne créera pas le volume si la relation n'existe pas. Si la relation existe, Astra Control Provisioner s'assurera que le nouveau volume FlexVol est placé sur un SVM peering avec le SVM distant défini dans le MirrorRelationship.

#### États de réplication des volumes

Une relation de miroir Trident (TMR) est une relation CRD qui représente une extrémité d'une relation de réplication entre les ESV. La TMR de destination a un état qui indique à Astra Control provisioner l'état souhaité. La TMR de destination a les États suivants :

- **Établi** : le PVC local est le volume de destination d'une relation miroir, et il s'agit d'une nouvelle relation.
- **Promu** : Le PVC local est ReadWrite et montable, sans relation de miroir actuellement en vigueur.
- **Rétablissement** : Le PVC local est le volume de destination d'une relation miroir et était également auparavant dans cette relation miroir.
  - L'état rétabli doit être utilisé si le volume de destination était déjà en relation avec le volume source car il écrase le contenu du volume de destination.
  - L'état rétabli échouera si le volume n'était pas auparavant dans une relation avec la source.

#### Promotion de la demande de volume persistant secondaire en cas de basculement non planifié

Effectuez l'étape suivante sur le cluster Kubernetes secondaire :

- Mettez à jour le champ `spec.state` de TridentMirrorRelationship vers `promoted`.

## Promotion de la demande de volume persistant secondaire lors d'un basculement planifié

Lors d'un basculement planifié (migration), effectuez les étapes suivantes pour promouvoir la demande de volume persistant secondaire :

### Étapes

1. Sur le cluster Kubernetes principal, créez un snapshot de la demande de volume persistant et attendez que le snapshot soit créé.
2. Sur le cluster Kubernetes principal, créez la CR SnapshotInfo pour obtenir des informations internes.

### Exemple

```
kind: SnapshotInfo
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  snapshot-name: csi-nas-snapshot
```

3. Sur le cluster Kubernetes secondaire, mettez à jour le champ `spec.state` du `TridentMirrorRelationship` CR en `promu` et `spec.promotedSnapshotHandle` en tant que nom interne du snapshot.
4. Sur le cluster Kubernetes secondaire, confirmez l'état (champ `status.state`) de `TridentMirrorRelationship` à promu.

## Restaurer une relation de miroir après un basculement

Avant de restaurer une relation de symétrie, choisissez le côté que vous voulez faire comme nouveau principal.

### Étapes

1. Sur le cluster Kubernetes secondaire, assurez-vous que les valeurs du champ `spec.remoteVolumeHandle` du champ `TridentMirrorRelationship` sont mises à jour.
2. Sur le cluster Kubernetes secondaire, mettez à jour le champ `spec.mirror` de `TridentMirrorRelationship` sur `reestablished`.

## Opérations supplémentaires

ASTRA Control Provisioner prend en charge les opérations suivantes sur les volumes principal et secondaire :

### Répliquer la demande de volume persistant primaire sur une nouvelle demande de volume secondaire

Assurez-vous que vous avez déjà un PVC primaire et un PVC secondaire.

### Étapes

1. Supprimez les CRD `PersistentVolumeClaim` et `TridentMirrorRelationship` du cluster secondaire (destination) établi.
2. Supprimez le CRD `TridentMirrorRelationship` du cluster principal (source).
3. Créez un nouveau CRD `TridentMirrorRelationship` sur le cluster principal (source) pour le nouveau PVC secondaire (destination) que vous souhaitez établir.

## Redimensionner une PVC en miroir, principale ou secondaire

La demande de volume persistant peut être redimensionnée normalement, ONTAP étendra automatiquement les flexvols de destination si la quantité de données dépasse la taille actuelle.

## Supprimer la réplication d'une demande de volume persistant

Pour supprimer la réplication, effectuez l'une des opérations suivantes sur le volume secondaire actuel :

- Supprimez MirrorRelationship sur le PVC secondaire. Cela interrompt la relation de réplication.
- Ou, mettez à jour le champ spec.state à *promu*.

## Suppression d'une demande de volume persistant (qui était auparavant mise en miroir)

Le mécanisme de provisionnement Astra Control vérifie si des demandes de volume persistant sont répliquées et libère la relation de réplication avant toute tentative de suppression du volume.

## Supprimer une TMR

La suppression d'une TMR d'un côté d'une relation symétrique entraîne la transition de la TMR restante vers l'état *promu* avant que Astra Control Provisioner ne termine la suppression. Si la TMR sélectionnée pour la suppression est déjà à l'état *promoted*, il n'y a pas de relation miroir existante et la TMR sera supprimée et Astra Control Provisioner promouvra le PVC local à *ReadWrite*. Cette suppression libère les métadonnées SnapMirror pour le volume local dans ONTAP. Si ce volume est utilisé dans une relation miroir à l'avenir, il doit utiliser une nouvelle TMR avec un état de réplication *établi* volume lors de la création de la nouvelle relation miroir.

## Mettre à jour les relations miroir lorsque ONTAP est en ligne

Les relations miroir peuvent être mises à jour à tout moment après leur établissement. Vous pouvez utiliser les *state: promoted* champs ou *state: reestablished* pour mettre à jour les relations. Lors de la promotion d'un volume de destination en volume *ReadWrite* standard, vous pouvez utiliser *promotedSnapshotHandle* pour spécifier un snapshot spécifique dans lequel restaurer le volume actuel.

## Mettre à jour les relations en miroir lorsque ONTAP est hors ligne

Vous pouvez utiliser un CRD pour effectuer une mise à jour SnapMirror sans qu'Astra Control ne dispose d'une connectivité directe au cluster ONTAP. Reportez-vous à l'exemple de format de TridentActionMirrorUpdate suivant :

### Exemple

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

*status.state* Reflète l'état du CRD TridentActionMirrorUpdate. Il peut prendre une valeur de *succeed*, *In Progress* ou *FAILED*.

## Activez le mécanisme de provisionnement Astra Control

Les versions 23.10 et ultérieures de Trident comprennent l'option d'utiliser Astra Control Provisioner qui permet aux utilisateurs d'Astra Control sous licence d'accéder à des fonctionnalités avancées de provisionnement du stockage. ASTRA Control Provisioner offre cette fonctionnalité étendue en plus des fonctionnalités standard d'Astra Trident CSI. Vous pouvez utiliser cette procédure pour activer et installer Astra Control Provisioner.

Votre abonnement à Astra Control Service inclut automatiquement la licence pour l'utilisation d'Astra Control Provisioner.

Dans les prochaines mises à jour d'Astra Control, Astra Control Provisioner remplacera Astra Trident en tant que mécanisme de provisionnement et d'orchestration du stockage, et sera obligatoire pour l'utilisation d'Astra Control. Pour cette raison, il est fortement recommandé aux utilisateurs d'Astra Control d'activer Astra Control Provisioner. ASTRA Trident continuera à rester open source et sera publié, maintenu, pris en charge et mis à jour avec le nouveau CSI et d'autres fonctionnalités de NetApp.

### Comment savoir si j'ai besoin d'activer Astra Control provisionner ?

Si vous ajoutez un cluster à Astra Control Service qui ne possède pas encore Astra Trident, le cluster sera marqué comme **Eligible**. Après "[Ajoutez le cluster à Astra Control](#)", Astra Control Provisioner sera automatiquement activé.

Si votre cluster n'est pas marqué **Eligible**, il sera marqué **Partially eligible** pour l'une des raisons suivantes :

- Il utilise une version plus ancienne d'Astra Trident
- Il utilise une Astra Trident 23.10 qui ne dispose pas encore de l'option de provisionnement activée
- Il s'agit d'un type de cluster qui ne permet pas l'activation automatique

‘Partially eligible’ Dans certains cas, utilisez ces instructions pour activer manuellement le mécanisme de provisionnement Astra Control pour votre cluster.

Choose an Azure Kubernetes Service cluster to enable application data management and the Astra Control storage operator.

⚠ Some Kubernetes cluster(s) below have private networking. [Learn more](#)

Cluster	Location	Eligibility
sandbox-ragnarok-aks-02	centraluseuap	Eligible
sandbox-ragnarok-aks-03	centraluseuap	Partially eligible
sandbox-rstephe2-aks-01	centraluseuap	Eligible

Back Next

## Avant d'activer Astra Control Provisioner

Si vous disposez d'une Astra Trident sans Astra Control Provisioner et que vous souhaitez activer Astra Control Provisioner, effectuez d'abord les opérations suivantes :

- Si vous avez installé Astra Trident, vérifiez que sa version se trouve dans une fenêtre à quatre versions:** Vous pouvez effectuer une mise à niveau directe vers Astra Trident 24.02 avec Astra Control Provisioner si votre Astra Trident se trouve dans une fenêtre à quatre versions de la version 24.02. Par exemple, vous pouvez effectuer une mise à niveau directe d'Astra Trident 23.04 vers la version 24.02.
- Confirmez que votre cluster a une architecture système AMD64 :** l'image Astra Control Provisioner est fournie dans les architectures CPU AMD64 et ARM64, mais seul AMD64 est pris en charge par Astra Control.

## Étapes

- Accédez au registre d'images NetApp Astra Control :
  - Connectez-vous à l'interface utilisateur d'Astra Control Service et enregistrez votre ID de compte Astra Control.
    - Sélectionnez l'icône de figure en haut à droite de la page.
    - Sélectionnez **accès API**.
    - Notez votre ID de compte.
  - A partir de la même page, sélectionnez **générer jeton API** et copiez la chaîne de jeton API dans le presse-papiers et enregistrez-la dans votre éditeur.
  - Connectez-vous au registre Astra Control à l'aide de la méthode de votre choix :

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. (Registres personnalisés uniquement) Suivez ces étapes pour déplacer l'image vers votre registre personnalisé. Si vous n'utilisez pas de registre, suivez les étapes de l'opérateur Trident dans la [section suivante](#).



Vous pouvez utiliser Podman à la place de Docker pour les commandes suivantes. Si vous utilisez un environnement Windows, PowerShell est recommandé.

## Docker

- Extrayez l'image Astra Control Provisioner du Registre :



L'image extraite ne prend pas en charge plusieurs plates-formes et ne prend en charge que la même plate-forme que l'hôte qui a extrait l'image, comme Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

Exemple :

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform linux/amd64
```

- Marquer l'image :

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

- Envoyez l'image vers votre registre personnalisé :

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

## Grue

- Copiez le manifeste Astra Control Provisioner dans votre registre personnalisé :

```
crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

- Déterminez si la méthode d'installation d'Astra Trident d'origine utilisait un.
- Activez Astra Control Provisioner dans Astra Trident en utilisant la méthode d'installation que vous avez utilisée initialement :

## Opérateur Astra Trident

- a. ["Téléchargez le programme d'installation d'Astra Trident et extrayez-le".](#)
- b. Si vous n'avez pas encore installé Astra Trident ou si vous avez supprimé l'opérateur de votre déploiement Astra Trident d'origine :
  - i. Créez le CRD :

```
kubectl create -f  
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.1  
6.yaml
```

- ii. Créez l'espace de noms trident (kubectl create namespace trident) ou **confirmez** que l'espace de noms trident existe toujours (kubectl get all -n trident). Si l'espace de noms a été supprimé, créez-le à nouveau.
- c. Mettez à jour Astra Trident vers la version 24.06.0 :

 Pour les clusters exécutant Kubernetes 1.24 ou version antérieure, utilisez `bundle_pre_1_25.yaml`. Pour les clusters exécutant Kubernetes 1.25 ou version ultérieure, utilisez `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-  
name.yaml>
```

- d. Vérifiez que Astra Trident est en cours d'exécution :

```
kubectl get torc -n trident
```

Réponse :

NAME	AGE
trident	21m

- e. si vous avez un registre qui utilise des secrets, créez un secret à utiliser pour extraire l'image Astra Control Provisioner :

```
kubectl create secret docker-registry <secret_name> -n trident  
--docker-server=<my_custom_registry> --docker-username=<username>  
--docker-password=<token>
```

- f. Modifiez la CR TridentOrchestrator et apportez les modifications suivantes :

```
kubectl edit torc trident -n trident
```

- i. Définissez un emplacement de Registre personnalisé pour l'image Astra Trident ou extrayez-le du Registre Astra Control ou (tridentImage: <my\_custom\_registry>/trident:24.02.0 tridentImage: netapp/trident:24.06.0).
- ii. Activez le mécanisme de provisionnement Astra Control (enableACP: true).
- iii. Définissez l'emplacement de registre personnalisé pour l'image Astra Control Provisioner ou extrayez-le du registre Astra Control ou (acpImage: <my\_custom\_registry>/trident-acp:24.02.0 acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0).
- iv. Si vous avez établi **secrets d'extraction d'image** précédemment dans cette procédure, vous pouvez les définir ici (imagePullSecrets: - <secret\_name>). Utilisez le même nom secret que celui que vous avez établi lors des étapes précédentes.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.06.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.06.0
  imagePullSecrets:
  - <secret_name>
```

g. Enregistrez et quittez le fichier. Le processus de déploiement commence automatiquement.

h. Vérifiez que l'opérateur, le déploiement et les réplicateurs sont créés.

```
kubectl get all -n trident
```



Il ne doit y avoir que **une instance** de l'opérateur dans un cluster Kubernetes. Ne créez pas plusieurs déploiements de l'opérateur Astra Trident.

- i. Vérifiez que le trident-acp conteneur est en cours d'exécution et que acpVersion l'état est 24.02.0 Installed:

```
kubectl get torc -o yaml
```

Réponse :

```
status:  
  acpVersion: 24.02.0  
  currentInstallationParams:  
    ...  
    acpImage: <registry>/trident-acp:24.02.0  
    enableACP: "true"  
    ...  
    ...  
  status: Installed
```

### tridentctl

- [Téléchargez le programme d'installation d'Astra Trident et extrayez-le](#).
- [Si vous disposez d'une Astra Trident, désinstallez-la du cluster qui l'héberge](#).
- Installer Astra Trident avec Astra Control Provisioner activé (--enable-acp=true) :

```
./tridentctl -n trident install --enable-acp=true --acp  
-image=mycustomregistry/trident-acp:24.02
```

- Vérifiez que le mécanisme de provisionnement Astra Control a été activé :

```
./tridentctl -n trident version
```

Réponse :

VERSION	CLIENT VERSION	ACP VERSION	SERVER
24.02.0	24.02.0	24.02.0	24.02.0

### Gouvernail

- Si vous avez installé Astra Trident 23.07.1 ou une version antérieure, ["désinstaller"](#) l'opérateur et d'autres composants.
- Si votre cluster Kubernetes s'exécute sur la version 1.24 ou antérieure, supprimez la psp :

```
kubectl delete psp tridentoperatorpod
```

- Ajout du référentiel Astra Trident Helm :

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

d. Mettre à jour le graphique Helm :

```
helm repo update netapp-trident
```

Réponse :

```
Hang tight while we grab the latest from your chart
repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. □Happy Helming!□
```

e. Répertorier les images :

```
./tridentctl images -n trident
```

Réponse :

```
| v1.28.0 | netapp/trident:24.06.0|
|          | docker.io/netapp/trident-
autosupport:24.06|
|          | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|          | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
|          | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
|          | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|          | registry.k8s.io/sig-storage/csi-node-
driver-registrar:v2.10.0 |
|          | netapp/trident-operator:24.06.0 (optional)
```

f. Vérifier que trident-Operator 24.06.0 est disponible :

```
helm search repo netapp-trident/trident-operator --versions
```

Réponse :

NAME	CHART VERSION	APP VERSION
DESCRIPTION		
netapp-trident/trident-operator	100.2406.0	24.06.0

g. Utilisez `helm install` et exécutez l'une des options suivantes qui incluent ces paramètres :

- Un nom pour votre emplacement de déploiement
- Version d'Astra Trident
- Nom de l'image Astra Control Provisioner
- Indicateur d'activation du provisionneur
- (Facultatif) Un chemin de registre local. Si vous utilisez un registre local, votre "["Images Trident"](#) peut se trouver dans un registre ou dans des registres différents, mais toutes les images CSI doivent se trouver dans le même registre.
- Espace de noms Trident

### Options

- Images sans registre

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-
acp:24.06.0 --set enableACP=true --set operatorImage=netapp/trident-
operator:24.06.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.06
--set tridentImage=netapp/trident:24.06.0 --namespace trident
```

- Images dans un ou plusieurs registres

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.06.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.06
--set tridentImage=netapp/trident:24.06.0 --namespace trident
```

Vous pouvez utiliser `helm list` pour vérifier les détails de l'installation tels que le nom, l'espace de noms, le graphique, l'état, la version de l'application, et le numéro de révision.

Si vous rencontrez des problèmes pour déployer Trident à l'aide d'Helm, exécutez cette commande pour désinstaller complètement Astra Trident :

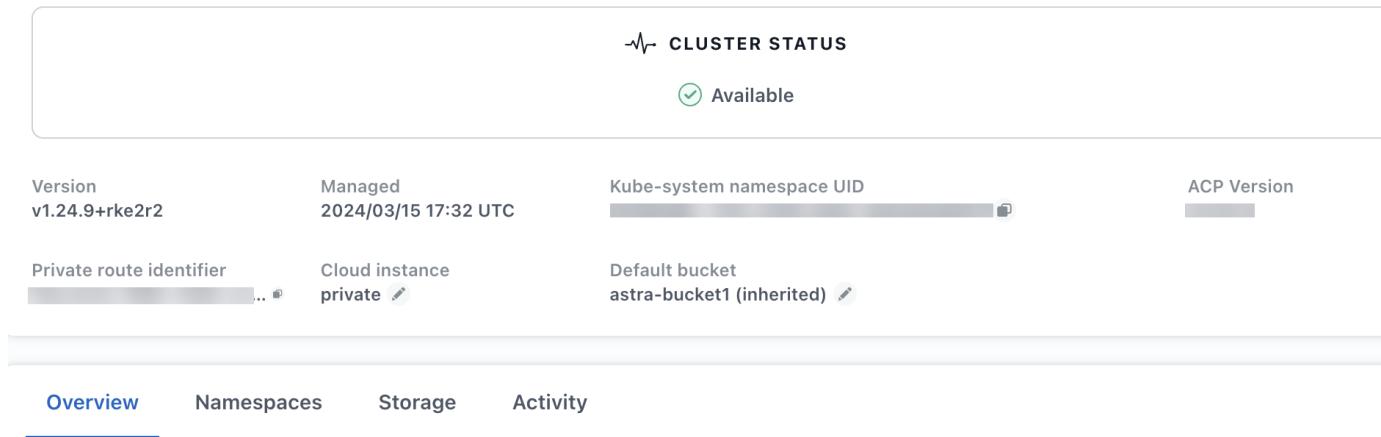
```
./tridentctl uninstall -n trident
```

**Ne pas "Retirez complètement les CRD Astra Trident" dans le cadre de votre désinstallation avant de tenter à nouveau d'activer Astra Control Provisioner.**

## Résultat

La fonctionnalité Astra Control Provisioner est activée et vous pouvez utiliser toutes les fonctions disponibles pour la version que vous exécutez.

Une fois Astra Control Provisioner installé, le cluster qui héberge le provisionneur dans l'interface utilisateur Astra Control affiche un `ACP version` champ plutôt que `Trident version` et le numéro de version installée actuel.



CLUSTER STATUS

Available

Version v1.24.9+rke2r2	Managed 2024/03/15 17:32 UTC	Kube-system namespace UID	ACP Version
Private route identifier	Cloud instance private	Default bucket astra-bucket1 (inherited)	

Overview   Namespaces   Storage   Activity

## Pour en savoir plus

- ["Documentation sur les mises à niveau d'Astra Trident"](#)

## Utiliser la topologie CSI

ASTRA Trident peut créer et attacher de manière sélective des volumes aux nœuds présents dans un cluster Kubernetes en utilisant le ["Fonction de topologie CSI"](#).

### Présentation

Grâce à la fonction de topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Les fournisseurs cloud permettent aujourd'hui aux administrateurs Kubernetes de frayer des nœuds basés sur une zone. Les nœuds peuvent se trouver dans différentes zones de disponibilité au sein d'une région ou entre différentes régions. Astra Trident utilise la topologie CSI pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multi-zones.



En savoir plus sur la fonctionnalité topologie CSI ["ici"](#).

Kubernetes propose deux modes de liaison de volumes :

- Lorsque `VolumeBindingMode` cette option est définie sur `Immediate`, Astra Trident crée le volume sans reconnaissance de la topologie. La liaison de volumes et le provisionnement dynamique sont gérés au moment de la création de la demande de volume persistant. Il s'agit de la valeur par défaut `VolumeBindingMode` et convient aux clusters qui n'appliquent pas de contraintes de topologie. Les volumes persistants sont créés sans dépendance vis-à-vis des exigences de planification du pod

demandeur.

- Avec la `VolumeBindingMode` valeur définie sur `WaitForFirstConsumer`, la création et la liaison d'un volume persistant pour une demande de volume persistant sont retardées jusqu'à ce qu'un pod qui utilise la demande de volume persistant soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification appliquées en fonction des besoins de topologie.



Le `WaitForFirstConsumer` mode de liaison ne nécessite pas d'étiquettes de topologie. Il peut être utilisé indépendamment de la fonction de topologie CSI.

## Ce dont vous avez besoin

Pour utiliser la topologie CSI, vous devez disposer des éléments suivants :

- Cluster Kubernetes exécutant une "[Version Kubernetes prise en charge](#)"

```
kubectl version
Client Version: version.Info{Major:"1", Minor:"19",
GitVersion:"v1.19.3",
GitCommit:"1e11e4a2108024935ecfcb2912226cedead99df",
GitTreeState:"clean", BuildDate:"2020-10-14T12:50:19Z",
GoVersion:"go1.15.2", Compiler:"gc", Platform:"linux/amd64"}
Server Version: version.Info{Major:"1", Minor:"19",
GitVersion:"v1.19.3",
GitCommit:"1e11e4a2108024935ecfcb2912226cedead99df",
GitTreeState:"clean", BuildDate:"2020-10-14T12:41:49Z",
GoVersion:"go1.15.2", Compiler:"gc", Platform:"linux/amd64"}
```

- Les nœuds du cluster doivent avoir des étiquettes qui permettent de prendre en compte la topologie (`topology.kubernetes.io/region` et `topology.kubernetes.io/zone`). Ces étiquettes **doivent être présentes sur les nœuds du cluster** avant d'installer Astra Trident pour qu'Astra Trident soit compatible avec la topologie.

```

kubectl get nodes -o=jsonpath='{range .items[*]}{{.metadata.name},\n{.metadata.labels}}{"\n"}{end}' | grep --color "topology.kubernetes.io"
[node1,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kubernetes.io/arch":"amd64","kubernetes.io/hostname":"node1","kubernetes.io/os":"linux","node-
role.kubernetes.io/master":"","topology.kubernetes.io/region":"us-
east1","topology.kubernetes.io/zone":"us-east1-a"}]
[node2,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kubernetes.io/arch":"amd64","kubernetes.io/hostname":"node2","kubernetes.io/os":"linux","node-
role.kubernetes.io/worker":"","topology.kubernetes.io/region":"us-
east1","topology.kubernetes.io/zone":"us-east1-b"}]
[node3,
{"beta.kubernetes.io/arch":"amd64","beta.kubernetes.io/os":"linux","kubernetes.io/arch":"amd64","kubernetes.io/hostname":"node3","kubernetes.io/os":"linux","node-
role.kubernetes.io/worker":"","topology.kubernetes.io/region":"us-
east1","topology.kubernetes.io/zone":"us-east1-c"}]

```

## Étape 1 : création d'un back-end conscient de la topologie

Les systèmes back-end de stockage Astra Trident peuvent être conçus pour provisionner des volumes de manière sélective selon les zones de disponibilité. Chaque back-end peut porter un bloc facultatif `supportedTopologies` représentant une liste de zones et de régions prises en charge. Pour les classes de stockage qui utilisent un tel backend, un volume ne sera créé que si une application est planifiée dans une région/zone prise en charge.

Voici un exemple de définition de back-end :

## YAML

```
---
version: 1
storageDriverName: ontap-san
backendName: san-backend-us-east1
managementLIF: 192.168.27.5
svm: iscsi_svm
username: admin
password: password
supportedTopologies:
- topology.kubernetes.io/region: us-east1
  topology.kubernetes.io/zone: us-east1-a
- topology.kubernetes.io/region: us-east1
  topology.kubernetes.io/zone: us-east1-b
```

## JSON

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "san-backend-us-east1",
  "managementLIF": "192.168.27.5",
  "svm": "iscsi_svm",
  "username": "admin",
  "password": "password",
  "supportedTopologies": [
    {"topology.kubernetes.io/region": "us-east1",
     "topology.kubernetes.io/zone": "us-east1-a"},
    {"topology.kubernetes.io/region": "us-east1",
     "topology.kubernetes.io/zone": "us-east1-b"}
  ]
}
```

 supportedTopologies est utilisé pour fournir une liste de régions et de zones par back-end. Ces régions et ces zones représentent la liste des valeurs admissibles qui peuvent être fournies dans une classe de stockage. Pour les classes de stockage qui contiennent un sous-ensemble de régions et de zones qu'il fournit en back-end, Astra Trident crée un volume en interne.

Vous pouvez également définir supportedTopologies par pool de stockage. Voir l'exemple suivant :

```
---
version: 1
storageDriverName: ontap-nas
backendName: nas-backend-us-central1
managementLIF: 172.16.238.5
svm: nfs_svm
username: admin
password: password
supportedTopologies:
- topology.kubernetes.io/region: us-central1
  topology.kubernetes.io/zone: us-central1-a
- topology.kubernetes.io/region: us-central1
  topology.kubernetes.io/zone: us-central1-b
storage:
- labels:
  workload: production
  supportedTopologies:
  - topology.kubernetes.io/region: us-central1
    topology.kubernetes.io/zone: us-central1-a
- labels:
  workload: dev
  supportedTopologies:
  - topology.kubernetes.io/region: us-central1
    topology.kubernetes.io/zone: us-central1-b
```

Dans cet exemple, les `region` étiquettes et `zone` représentent l'emplacement du pool de stockage. `topology.kubernetes.io/region` et `topology.kubernetes.io/zone` détermine d'où les pools de stockage peuvent être consommés.

## Étape 2 : définissez des classes de stockage qui prennent en compte la topologie

Les classes de stockage peuvent être définies en fonction des labels de topologie fournis aux nœuds du cluster, et contenir des informations de topologie. Cela déterminera les pools de stockage qui servent de candidats aux demandes de volume persistant faites et le sous-ensemble de nœuds qui peuvent utiliser les volumes provisionnés par Trident.

Voir l'exemple suivant :

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: netapp-san-us-east1
  provisioner: csi.trident.netapp.io
  volumeBindingMode: WaitForFirstConsumer
  allowedTopologies:
    - matchLabelExpressions:
    - key: topology.kubernetes.io/zone
      values:
        - us-east1-a
        - us-east1-b
    - key: topology.kubernetes.io/region
      values:
        - us-east1
  parameters:
    fsType: "ext4"

```

Dans la définition de classe de stockage fournie ci-dessus, `volumeBindingMode` est définie sur `WaitForFirstConsumer`. Les demandes de volume persistant demandées pour cette classe de stockage ne seront pas traitées tant qu'elles ne seront pas référencées dans un pod. Et `allowedTopologies` fournit les zones et la région à utiliser. La `netapp-san-us-east1` classe de stockage crée des ESV sur le `san-backend-us-east1` back-end défini ci-dessus.

### Étape 3 : création et utilisation d'une demande de volume persistant

Une fois la classe de stockage créée et mappée à un back-end, vous pouvez désormais créer des demandes de volume persistant.

Voir l'exemple `spec` ci-dessous :

```

---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 300Mi
  storageClassName: netapp-san-us-east1

```

La création d'une demande de volume persistant à l'aide de ce manifeste se traduit par les éléments suivants :

```

kubectl create -f pvc.yaml
persistentvolumeclaim/pvc-san created
kubectl get pvc
NAME      STATUS      VOLUME      CAPACITY      ACCESS MODES      STORAGECLASS
AGE
pvc-san   Pending          2s          netapp-san-us-east1

kubectl describe pvc
Name:            pvc-san
Namespace:       default
StorageClass:    netapp-san-us-east1
Status:          Pending
Volume:
Labels:          <none>
Annotations:    <none>
Finalizers:     [kubernetes.io/pvc-protection]
Capacity:
Access Modes:
VolumeMode:     Filesystem
Mounted By:    <none>
Events:
  Type  Reason          Age      From          Message
  ----  ----          ----      ----          -----
  Normal  WaitForFirstConsumer  6s      persistentvolume-controller  waiting
for first consumer to be created before binding

```

Pour que Trident puisse créer un volume et le lier à la demande de volume persistant, utilisez la demande de volume persistant dans un pod. Voir l'exemple suivant :

```

apiVersion: v1
kind: Pod
metadata:
  name: app-pod-1
spec:
  affinity:
    nodeAffinity:
      requiredDuringSchedulingIgnoredDuringExecution:
        nodeSelectorTerms:
        - matchExpressions:
          - key: topology.kubernetes.io/region
            operator: In
            values:
            - us-east1
      preferredDuringSchedulingIgnoredDuringExecution:
      - weight: 1
        preference:
          matchExpressions:
          - key: topology.kubernetes.io/zone
            operator: In
            values:
            - us-east1-a
            - us-east1-b
  securityContext:
    runAsUser: 1000
    runAsGroup: 3000
    fsGroup: 2000
  volumes:
  - name: vol1
    persistentVolumeClaim:
      claimName: pvc-san
  containers:
  - name: sec-ctx-demo
    image: busybox
    command: [ "sh", "-c", "sleep 1h" ]
    volumeMounts:
    - name: vol1
      mountPath: /data/demo
    securityContext:
      allowPrivilegeEscalation: false

```

Ce podSpec demande à Kubernetes de planifier le pod sur les nœuds présents dans `us-east1` la région, puis de choisir parmi le nœud présent dans les `us-east1-a` zones ou `us-east1-b`.

Voir le résultat suivant :

```

kubectl get pods -o wide
NAME        READY   STATUS    RESTARTS   AGE   IP           NODE
NOMINATED NODE   READINESS GATES
app-pod-1   1/1     Running   0          19s   192.168.25.131   node2
<none>           <none>
kubectl get pvc -o wide
NAME        STATUS    VOLUME
ACCESS MODES   STORAGECLASS   AGE   VOLUMEMODE   CAPACITY
pvc-san     Bound     pvc-ecb1e1a0-840c-463b-8b65-b3d033e2e62b   300Mi
RWO          netapp-san-us-east1   48s   Filesystem

```

## Mettez à jour les systèmes back-end pour inclure `supportedTopologies`

Les systèmes back-end préexistants peuvent être mis à jour pour inclure une liste d'`supportedTopologies` `utilisation `tridentctl backend update. Cela n'affecte pas les volumes qui ont déjà été provisionnés et ne sera utilisé que pour les demandes de volume virtuel suivantes.

## Trouvez plus d'informations

- ["Gestion des ressources pour les conteneurs"](#)
- ["Outil de sélection de nœud"](#)
- ["Affinité et anti-affinité"](#)
- ["Teintes et tolérances"](#)

## Travailler avec des instantanés

Les copies Snapshot de volume Kubernetes de volumes persistants (PVS) permettent d'effectuer des copies instantanées de volumes. Vous pouvez créer une copie Snapshot d'un volume créé à l'aide d'Astra Trident, importer un snapshot créé hors d'Astra Trident, créer un nouveau volume à partir d'un snapshot existant et restaurer les données de volume à partir de snapshots.

### Présentation

Le snapshot de volume est pris en charge par `ontap-nas`, `ontap-nas-flexgroup` `ontap-san` , `ontap-san-economy` , , `solidfire-san` `gcp-cvs`, et `azure-netapp-files` pilotes.

### Avant de commencer

Vous devez disposer d'un contrôleur de snapshot externe et de définitions de ressources personnalisées (CRD) pour pouvoir utiliser les snapshots. Cela relève de la responsabilité de l'orchestrateur Kubernetes (par exemple : Kubeadm, GKE, OpenShift).

Si votre distribution Kubernetes n'inclut pas le contrôleur de snapshot et les CRD, reportez-vous à la [Déployer un contrôleur de snapshot de volume](#).



Ne créez pas de contrôleur de snapshot si vous créez des snapshots de volume à la demande dans un environnement GKE. GKE utilise un contrôleur de snapshot caché intégré.

## Créer un snapshot de volume

### Étapes

1. Créez un `VolumeSnapshotClass`. Pour plus d'informations, reportez-vous à "["VolumeSnapshotClass"](#)" la section .
  - Le indique le `driver` conducteur de l'Astra Trident CSI.
  - `deletionPolicy` peut être `Delete` ou `Retain`. Lorsqu'il est défini sur `Retain`, le snapshot physique sous-jacent du cluster de stockage est conservé même lorsque l' `'VolumeSnapshot'` objet est supprimé.

### Exemple

```
cat snap-sc.yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: csi-snapclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

2. Créer un snapshot d'une demande de volume persistant existante.

### Exemples

- Dans cet exemple, nous allons créer un snapshot d'un volume persistant existant.

```
cat snap.yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshot
metadata:
  name: pvc1-snap
spec:
  volumeSnapshotClassName: csi-snapclass
  source:
    persistentVolumeClaimName: pvc1
```

- Cet exemple crée un objet de snapshot de volume pour une demande de volume persistant nommée `pvc1` et le nom de l'instantané est défini sur `pvc1-snap`. Un `VolumeSnapshot` est similaire à une demande de volume persistant et est associé à un `VolumeSnapshotContent` objet qui représente le snapshot réel.

```

kubectl create -f snap.yaml
volumesnapshot.snapshot.storage.k8s.io/pvc1-snap created

kubectl get volumesnapshots
NAME          AGE
pvc1-snap    50s

```

- Vous pouvez identifier `VolumeSnapshotContent` l'objet du `pvc1-snap` `VolumeSnapshot` en le décrivant. Le système `Snapshot Content Name` identifie l'objet `VolumeSnapshotContent` qui sert ce snapshot. Le `Ready To Use` paramètre indique que l'instantané peut être utilisé pour créer une nouvelle demande de volume persistant.

```

kubectl describe volumesnapshots pvc1-snap
Name:          pvc1-snap
Namespace:     default
.
.
.
Spec:
  Snapshot Class Name:  pvc1-snap
  Snapshot Content Name: snapcontent-e8d8a0ca-9826-11e9-9807-
  525400f3f660
  Source:
    API Group: 
    Kind:       PersistentVolumeClaim
    Name:       pvc1
Status:
  Creation Time:  2019-06-26T15:27:29Z
  Ready To Use:   true
  Restore Size:   3Gi
.
.
.

```

## Créer une demande de volume persistant à partir d'un snapshot de volume

Vous pouvez utiliser `dataSource` pour créer une demande de volume persistant à l'aide d'un `VolumeSnapshot` nommé `<pvc-name>` source des données. Une fois la demande de volume persistant créée, elle peut être connectée à un pod et utilisée comme n'importe quel autre PVC.

 La demande de volume sera créée dans le même back-end que le volume source. Reportez-vous à la "["Base de connaissances : la création d'une demande de volume persistant à partir d'un Snapshot de volume persistant Trident ne peut pas être créée dans un autre back-end"](#)".

L'exemple suivant crée la demande de volume persistant en utilisant `pvc1-snap` comme source de données.

```

cat pvc-from-snap.yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc-from-snap
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: golden
  resources:
    requests:
      storage: 3Gi
  dataSource:
    name: pvcl-snap
    kind: VolumeSnapshot
    apiGroup: snapshot.storage.k8s.io

```

## Importer un instantané de volume

ASTRA Trident prend en charge "[Processus Snapshot prévisionné Kubernetes](#)" pour permettre à l'administrateur du cluster de créer un `VolumeSnapshotContent` objet et d'importer des snapshots créés en dehors d'Astra Trident.

### Avant de commencer

ASTRA Trident doit avoir créé ou importé le volume parent du snapshot.

### Étapes

1. **Cluster admin:** Créez un `VolumeSnapshotContent` objet qui fait référence au snapshot back-end. Cela lance le workflow de snapshot dans Astra Trident.
  - Spécifiez le nom du snapshot back-end dans annotations comme `trident.netapp.io/internalSnapshotName: <"backend-snapshot-name">`.
  - Spécifiez `<name-of-parent-volume-in-trident>/<volume-snapshot-content-name>` dans `snapshotHandle`. Il s'agit de la seule information fournie à Astra Trident par le snapshotter externe dans l' ``ListSnapshots`` appel.



Le système `<volumeSnapshotContentName>` ne peut pas toujours correspondre au nom du snapshot back-end en raison des contraintes de dénomination CR.

### Exemple

L'exemple suivant crée un `VolumeSnapshotContent` objet qui référence le snapshot back-end `snap-01`.

```

apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotContent
metadata:
  name: import-snap-content
  annotations:
    trident.netapp.io/internalSnapshotName: "snap-01" # This is the
    name of the snapshot on the backend
spec:
  deletionPolicy: Retain
  driver: csi.trident.netapp.io
  source:
    snapshotHandle: pvc-f71223b5-23b9-4235-bbfe-e269ac7b84b0/import-
    snap-content # <import PV name or source PV name>/<volume-snapshot-
    content-name>

```

2. **Cluster admin:** Créez la VolumeSnapshot CR qui fait référence à l' VolumeSnapshotContent `objet. Cette opération demande l'accès à pour utiliser `VolumeSnapshot dans un espace de noms donné.

#### Exemple

L'exemple suivant crée une VolumeSnapshot demande de modification nommée qui fait référence à l' VolumeSnapshotContent nommée import-snap import-snap-content .

```

apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshot
metadata:
  name: import-snap
spec:
  # volumeSnapshotClassName: csi-snapclass (not required for pre-
  # provisioned or imported snapshots)
  source:
    volumeSnapshotContentName: import-snap-content

```

3. **Traitement interne (aucune action requise):** le snapshotter externe reconnaît le nouveau créé VolumeSnapshotContent et exécute l' ListSnapshots `appel. ASTRA Trident crée le `TridentSnapshot.

- Le snapshotter externe définit le VolumeSnapshotContent sur readyToUse et le VolumeSnapshot sur true.
- Trident renvoie readyToUse=true.

4. **Tout utilisateur :** Créez un PersistentVolumeClaim pour référencer le nouveau VolumeSnapshot, où le spec.dataSource nom (ou spec.dataSourceRef) est le VolumeSnapshot nom.

#### Exemple

L'exemple suivant crée un PVC faisant référence au VolumeSnapshot import-snap .

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: pvc-from-snap
spec:
  accessModes:
    - ReadWriteOnce
  storageClassName: simple-sc
  resources:
    requests:
      storage: 1Gi
  dataSource:
    name: import-snap
    kind: VolumeSnapshot
    apiGroup: snapshot.storage.k8s.io
```

## Restaurez les données de volume à l'aide de snapshots

Le répertoire des snapshots est masqué par défaut pour faciliter la compatibilité maximale des volumes provisionnés à l'aide des `ontap-nas` pilotes et `ontap-nas-economy`. Activez le `.snapshot` répertoire pour restaurer directement les données à partir de snapshots.

Utilisez l'interface de ligne de commandes ONTAP de restauration de snapshot de volume pour restaurer un volume à un état enregistré dans un snapshot précédent.

```
cluster1::>*> volume snapshot restore -vserver vs0 -volume vol3 -snapshot
vol3_snap_archive
```

 Lorsque vous restaurez une copie Snapshot, la configuration de volume existante est écrasée. Les modifications apportées aux données de volume après la création de la copie Snapshot sont perdues.

Le répertoire des snapshots est masqué par défaut pour faciliter la compatibilité maximale des volumes provisionnés à l'aide des `ontap-nas` pilotes et `ontap-nas-economy`. Activez le `.snapshot` répertoire pour restaurer directement les données à partir de snapshots.

 Lorsque vous restaurez une copie Snapshot, la configuration de volume existante est écrasée. Les modifications apportées aux données de volume après la création de la copie Snapshot sont perdues.

## Restauration de volumes sur place à partir d'un snapshot

ASTRA Control Provisioner assure une restauration rapide de volume sur place à partir d'un snapshot à l'aide du `TridentActionSnapshotRestore` système CR (TASR). Cette CR fonctionne comme une action Kubernetes impérative et ne persiste pas une fois l'opération terminée.

ASTRA Control Provisioner prend en charge la restauration Snapshot sur ontap-san, ontap-san-economy ontap-nas, , ontap-nas-flexgroup, , , azure-netapp-files gcp-cvs, et solidfire-san pilotes.

## Avant de commencer

Vous devez disposer d'une demande de volume liée et d'un instantané de volume disponible.

- Vérifiez que l'état de la demande de volume persistant est lié.

```
kubectl get pvc
```

- Vérifiez que le snapshot du volume est prêt à être utilisé.

```
kubectl get vs
```

## Étapes

1. Créez la CR TASR. Cet exemple crée une CR pour la PVC pvc1 et l'instantané de volume pvc1-snapshot.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Appliquez la CR pour effectuer une restauration à partir de l'instantané. Cet exemple permet de restaurer des données à partir d'un snapshot pvc1.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

## Résultats

ASTRA Control Provisioner restaure les données à partir du snapshot. Vous pouvez vérifier l'état de la restauration des snapshots.

```

kubectl get tasr -o yaml

apiVersion: v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""

```

- i**
- Dans la plupart des cas, Astra Control Provisioner ne réessaiera pas automatiquement l'opération en cas de panne. Vous devrez effectuer à nouveau l'opération.
  - Les utilisateurs Kubernetes sans accès administrateur peuvent avoir à obtenir l'autorisation de l'administrateur pour créer une CR ASR dans l'espace de noms de leur application.

## Supprimez un volume persistant avec les snapshots associés

Lors de la suppression d'un volume persistant avec les snapshots associés, le volume Trident correspondant est mis à jour et passe à un état « Suppression ». Supprimez les snapshots de volume pour supprimer le volume Astra Trident.

## Déployer un contrôleur de snapshot de volume

Si votre distribution Kubernetes n'inclut pas le contrôleur de snapshot et les CRD, vous pouvez les déployer comme suit.

### Étapes

1. Création de CRD de snapshot de volume.

```
cat snapshot-setup.sh
#!/bin/bash
# Create volume snapshot CRDs
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yaml
1
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-
6.1/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

## 2. Créer le contrôleur de snapshot.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-6.1/deploy/kubernetes/snapshot-
controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-
csi/external-snapshotter/release-6.1/deploy/kubernetes/snapshot-
controller/setup-snapshot-controller.yaml
```



Si nécessaire, ouvrez `deploy/kubernetes/snapshot-controller/rbac-
snapshot-controller.yaml` et mettez à jour namespace votre espace de noms.

## Liens connexes

- ["Snapshots de volume"](#)
- ["VolumeSnapshotClass"](#)

# Gestion et contrôle d'Astra Trident

## Mettez à niveau Astra Trident

### Mettez à niveau Astra Trident

À partir de la version 24.02, Astra Trident suit une publication tous les quatre mois, livrant trois versions majeures chaque année. Chaque nouvelle version exploite les versions précédentes et fournit de nouvelles fonctionnalités, des améliorations de performances, des correctifs et des améliorations. Nous vous encourageons à effectuer une mise à niveau au moins une fois par an pour profiter des nouvelles fonctionnalités d'Astra Trident.

#### Considérations avant la mise à niveau

Lorsque vous mettez à niveau vers la dernière version d'Astra Trident, prenez en compte les points suivants :

- Il ne doit y avoir qu'une seule instance Astra Trident installée sur tous les namespaces d'un cluster Kubernetes donné.
- ASTRA Trident 23.07 et les versions ultérieures requièrent des snapshots de volume v1 et ne prennent plus en charge les snapshots alpha ou bêta.
- Si vous avez créé Cloud Volumes Service pour Google Cloud dans le ["Type de service CVS"](#), vous devez mettre à jour la configuration back-end pour utiliser le `standardsw` niveau de service ou `zoneredundantstandardsw` lors de la mise à niveau à partir d'Astra Trident 23.01. L'échec de la mise à jour du système `serviceLevel` dans le back-end peut entraîner l'échec des volumes. Voir ["Exemples de type de service CVS"](#) pour plus de détails.
- Lors de la mise à niveau, il est important que vous fournissez `parameter.fsType` dans `StorageClasses` utilisé par Astra Trident. Vous pouvez supprimer et recréer des données `StorageClasses` sans interrompre les volumes préexistants.
  - Il s'agit d'une **exigence** pour l'application ["contextes de sécurité"](#) pour les volumes SAN.
  - Le répertoire `sample input` contient des exemples, tels que <https://github.com/NetApp/Trident/blob/master/Trident-installer/sample-input/Storage-class-samples/Storage-class-Basic.yaml.template> et [link:https://github.com/NetApp/Trident/blob/master/Trident-input-default-class-samples/Storage-sample-than-class-than-default-\[storage-class-bronze-default.yaml.class\[storage-class-basic.yaml.template](https://github.com/NetApp/Trident/blob/master/Trident-input-default-class-samples/Storage-sample-than-class-than-default-[storage-class-bronze-default.yaml.class[storage-class-basic.yaml.template).
  - Pour plus d'informations, reportez-vous ["Problèmes connus"](#) à .

#### Étape 1 : sélectionnez une version

Les versions Astra Trident suivent une convention de dénomination basée sur la date `YY.MM`, où « `YY` » correspond aux deux derniers chiffres de l'année et « `MM` » au mois. Les versions de points suivent une `YY.MM.X` convention, où « `X` » est le niveau de patch. Vous allez sélectionner la version à mettre à niveau en fonction de la version à partir de laquelle vous effectuez la mise à niveau.

- Vous pouvez effectuer une mise à niveau directe vers n'importe quelle version cible située dans une fenêtre à quatre versions de la version installée. Par exemple, vous pouvez effectuer une mise à niveau directe de la version 23.04 (ou de toute version 23.04 points) vers la version 24.06.

- Si vous effectuez une mise à niveau à partir d'une version en dehors de la fenêtre à quatre versions, effectuez une mise à niveau en plusieurs étapes. Suivez les instructions de mise à "version antérieure" niveau de pour effectuer la mise à niveau vers la version la plus récente qui s'adapte à la fenêtre à quatre versions. Par exemple, si vous exécutez 22.01 et que vous souhaitez effectuer une mise à niveau vers 24.06 :
  - a. Première mise à niveau de 22.07 à 23.04.
  - b. Puis passez de 23.04 à 24.06.

 Lorsque vous effectuez une mise à niveau avec l'opérateur Trident sur OpenShift Container Platform, vous devez effectuer une mise à niveau vers Trident 21.01.1 ou une version ultérieure. L'opérateur Trident sorti avec 21.01.0 contient un problème connu qui a été résolu en 21.01.1. Pour plus de détails, reportez-vous au "["Consultez le document GitHub pour plus d'informations"](#).

## Étape 2 : déterminer la méthode d'installation d'origine

Pour déterminer quelle version vous avez utilisée pour l'installation initiale d'Astra Trident :

1. Utilisez `kubectl get pods -n trident` pour examiner les modules.
  - S'il n'y a pas de module opérateur, Astra Trident a été installée à l'aide de `tridentctl`.
  - S'il existe un pod opérateur, Astra Trident a été installé à l'aide de l'opérateur Trident soit manuellement, soit à l'aide d'Helm.
2. S'il existe un module opérateur, utilisez `kubectl describe torc` pour déterminer si Astra Trident a été installée à l'aide de Helm.
  - S'il y a une étiquette Helm, Astra Trident a été installée à l'aide d'Helm.
  - S'il n'y a pas d'étiquette Helm, Astra Trident a été installé manuellement à l'aide de l'opérateur Trident.

## Étape 3 : sélectionnez une méthode de mise à niveau

En général, vous devez "[passer d'une méthode d'installation à l'autre](#)" effectuer une mise à niveau en utilisant la même méthode que celle utilisée pour l'installation initiale, mais vous pouvez . Il existe deux options de mise à niveau d'Astra Trident.

- "["Mise à niveau à l'aide de l'opérateur Trident"](#)



Nous vous conseillons de passer en revue "["Comprendre le workflow de mise à niveau de l'opérateur"](#) avant de procéder à la mise à niveau avec l'opérateur.

\*

## Mise à niveau avec l'opérateur

### Comprendre le workflow de mise à niveau de l'opérateur

Avant d'utiliser l'opérateur Trident pour mettre à niveau Astra Trident, vous devez comprendre les processus en arrière-plan qui se produisent pendant la mise à niveau. Cela inclut les modifications apportées au contrôleur Trident, au pod du contrôleur et aux pods des nœuds, ainsi qu'au jeu de démonstration des nœuds qui activent les mises à jour en continu.

## Gestion des mises à niveau par l'opérateur Trident

L'une des nombreuses ["Avantages de l'utilisation de l'opérateur Trident"](#) à installer et à mettre à niveau Astra Trident est la gestion automatique des objets Astra Trident et Kubernetes sans interrompre les volumes montés existants. De cette façon, Astra Trident peut prendre en charge les mises à niveau sans interruption, ou ["mises à jour en continu"](#). En particulier, l'opérateur Trident communique avec le cluster Kubernetes pour :

- Supprimez et recréez le déploiement du contrôleur Trident et le nœud DemonSet.
- Remplacez l'afficheur de contrôleur Trident et les pods de nœud Trident par de nouvelles versions.
  - Si un nœud n'est pas mis à jour, il n'empêche pas la mise à jour des nœuds restants.
  - Seuls les nœuds exécutant Trident Node Pod peuvent monter des volumes.



Pour plus d'informations sur l'architecture d'Astra Trident sur le cluster Kubernetes, consultez ["Architecture d'Astra Trident"](#).

## Workflow de mise à niveau de l'opérateur

Lorsque vous lancez une mise à niveau avec l'opérateur Trident :

1. **L'opérateur Trident :**
  - a. Détecte la version d'Astra Trident actuellement installée (version  $n$ ).
  - b. Mise à jour de tous les objets Kubernetes, y compris les CRD, RBAC et le service Trident.
  - c. Supprime le déploiement du contrôleur Trident pour la version  $n$ .
  - d. Crée le déploiement du contrôleur Trident pour la version  $n+1$ .
2. **Kubernetes** crée le pod du contrôleur Trident pour  $n+1$ .
3. **L'opérateur Trident :**
  - a. Supprime le jeu de démonstration du nœud Trident pour  $n$ . L'opérateur n'attend pas la fin de Node Pod.
  - b. Crée le déclenchement du nœud Trident pour  $n+1$ .
4. **Kubernetes** crée des pods de nœuds Trident sur les nœuds qui n'exécutent pas Trident Node Pod  $n$ . Cela permet de garantir qu'il n'y a jamais plus d'un pod de nœuds Trident, quelle que soit la version, sur un nœud.

## Mettez à niveau une installation d'Astra Trident avec l'opérateur Trident ou Helm

Vous pouvez mettre à niveau Astra Trident à l'aide de l'opérateur Trident manuellement ou à l'aide d'Helm. Vous pouvez effectuer une mise à niveau d'une installation opérateur Trident vers une autre installation opérateur Trident ou passer d'une `tridentctl` installation à une version opérateur Trident. Révision ["Sélectionnez une méthode de mise à niveau"](#) avant la mise à niveau d'une installation de l'opérateur Trident.

### Mettre à niveau une installation manuelle

Vous pouvez effectuer une mise à niveau d'une installation d'opérateur Trident dont le périmètre est défini dans le cluster vers une autre installation d'opérateur Trident dont le périmètre est défini dans le cluster. Toutes les versions 21.01 et supérieures d'Astra Trident utilisent un opérateur à périmètre de cluster.



Pour effectuer la mise à niveau à partir d'Astra Trident qui a été installée à l'aide de l'opérateur dont le périmètre d'espace de noms est compris entre les versions 20.07 et 20.10, utilisez les instructions de mise à niveau "[votre version installée](#)" d'Astra Trident.

## Description de la tâche

Trident fournit un fichier bundle que vous pouvez utiliser pour installer l'opérateur et créer les objets associés pour votre version Kubernetes.

- Pour les clusters exécutant Kubernetes 1.24, utilisez "[bundle\\_pre\\_1\\_25.yaml](#)".
- Pour les clusters exécutant Kubernetes 1.25 ou version ultérieure, utilisez "[bundle\\_post\\_1\\_25.yaml](#)".

## Avant de commencer

Assurez-vous d'utiliser un cluster Kubernetes en cours d'exécution "[Version Kubernetes prise en charge](#)".

## Étapes

1. Vérifiez votre version d'Astra Trident :

```
./tridentctl -n trident version
```

2. Supprimez l'opérateur Trident qui a été utilisé pour installer l'instance Astra Trident actuelle. Par exemple, si vous mettez à niveau depuis 23.07, exécutez la commande suivante :

```
kubectl delete -f 23.07.0/trident-installer/deploy/<bundle.yaml> -n trident
```

3. Si vous avez personnalisé votre installation initiale à l'aide d' `TridentOrchestrator` attributs, vous pouvez modifier l' `TridentOrchestrator` objet pour modifier les paramètres d'installation. Cela peut inclure des modifications visant à spécifier les registres d'images en miroir Trident et CSI pour le mode hors ligne, à activer les journaux de débogage ou à spécifier les secrets d'extraction d'images.
4. Installez Astra Trident en utilisant le fichier YAML de bundle approprié pour votre environnement, où `<bundle.yaml>` est `bundle_pre_1_25.yaml` ou `bundle_post_1_25.yaml` basé sur votre version de Kubernetes. Par exemple, si vous installez Astra Trident 24.06, exécutez la commande suivante :

```
kubectl create -f 24.06.0/trident-installer/deploy/<bundle.yaml> -n trident
```

## Mettre à niveau une installation Helm

Vous pouvez mettre à niveau une installation d'Astra Trident Helm.



Lors de la mise à niveau d'un cluster Kubernetes de la version 1.24 vers la version 1.25 ou ultérieure sur lequel Astra Trident est installé, vous devez mettre à jour `Values.yaml` pour définir `excludePodSecurityPolicy` sur `true` ou ajouter la `--set excludePodSecurityPolicy=true` `helm upgrade` commande avant de pouvoir mettre à niveau le cluster.

## Étapes

1. Si vous ["Installez Astra Trident à l'aide d'Helm - effectué"](#), vous pouvez utiliser `helm upgrade trident netapp-trident/trident-operator --version 100.2406.0` pour effectuer une mise à niveau en une seule étape. Si vous n'avez pas ajouté le Helm repo ou si vous ne pouvez pas l'utiliser pour mettre à niveau :

- a. Téléchargez la dernière version d'Astra Trident sur ["La section Assets sur GitHub"](#).
- b. Utilisez `helm upgrade` la commande où reflète la version vers laquelle `trident-operator-24.06.0.tgz` vous souhaitez effectuer la mise à niveau.

```
helm upgrade <name> trident-operator-24.06.0.tgz
```



Si vous définissez des options personnalisées lors de l'installation initiale (par exemple, spécification de registres privés, en miroir pour les images Trident et CSI), ajoutez la commande à l'aide de `--set` pour vous assurer que ces options sont incluses dans la commande de mise à niveau, sinon les valeurs seront réinitialisées `helm upgrade` à leur valeur par défaut.

2. Exécutez `helm list` pour vérifier que le graphique et la version de l'application ont tous deux été mis à niveau. Exécutez `tridentctl logs` pour consulter tous les messages de débogage.

### Mise à niveau d'une `tridentctl` installation vers un opérateur Trident

Vous pouvez effectuer une mise à niveau vers la dernière version de l'opérateur Trident à partir d'une `tridentctl` installation. Les systèmes back-end et ESV existants seront automatiquement disponibles.



Avant de passer d'une méthode d'installation à l'autre, consultez ["Passage d'une méthode d'installation à l'autre"](#).

## Étapes

1. Téléchargez la dernière version d'Astra Trident.

```
# Download the release required [24.060.0]
mkdir 24.06.0
cd 24.06.0
wget
https://github.com/NetApp/trident/releases/download/v24.06.0/trident-
installer-24.06.0.tar.gz
tar -xf trident-installer-24.06.0.tar.gz
cd trident-installer
```

2. Créez le `tridentorchestrator` CRD à partir du manifeste.

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

3. Déployer l'opérateur cluster-scoped dans le même namespace.

```
kubectl create -f deploy/<bundle-name.yaml>

serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created

#Examine the pods in the Trident namespace
NAME READY STATUS RESTARTS AGE
trident-controller-79df798bdc-m79dc 6/6 Running 0 150d
trident-node-linux-xrst8 2/2 Running 0 150d
trident-operator-5574dbbc68-nthjv 1/1 Running 0 1m30s
```

4. Créez une TridentOrchestrator demande de modification pour installer Astra Trident.

```
cat deploy/crds/tridentorchestrator_cr.yaml
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident

kubectl create -f deploy/crds/tridentorchestrator_cr.yaml

#Examine the pods in the Trident namespace
NAME READY STATUS RESTARTS AGE
trident-csi-79df798bdc-m79dc 6/6 Running 0 1m
trident-csi-xrst8 2/2 Running 0 1m
trident-operator-5574dbbc68-nthjv 1/1 Running 0 5m41s
```

5. Vérifiez que Trident a été mis à niveau vers la version prévue.

```
kubectl describe torc trident | grep Message -A 3

Message: Trident installed
Namespace: trident
Status: Installed
Version: v24.06.0
```

## Mise à niveau avec tridentctl

Vous pouvez facilement mettre à niveau une installation Astra Trident existante à l'aide de `tridentctl`.

### Description de la tâche

La désinstallation et la réinstallation d'Astra Trident fait office de mise à niveau. Lorsque vous désinstallez Trident, la demande de volume persistant et le volume persistant utilisés par l'Astra Trident. Les volumes persistants ayant déjà été provisionnés restent disponibles pendant la mise hors ligne d'Astra Trident, et Astra Trident provisionne les volumes pour les demandes de volume persistant créées dans l'intervalle une fois de nouveau en ligne.

### Avant de commencer

Révision ["Sélectionnez une méthode de mise à niveau"](#) avant la mise à niveau à l'aide de `tridentctl`.

### Étapes

1. Exécutez la commande de désinstallation dans `tridentctl` pour supprimer toutes les ressources associées à Astra Trident, à l'exception des CRD et des objets associés.

```
./tridentctl uninstall -n <namespace>
```

2. Réinstallez Astra Trident. Reportez-vous à la ["Installation d'Astra Trident à l'aide de tridentctl"](#).



N'interrompez pas le processus de mise à niveau. Assurez-vous que le programme d'installation s'exécute jusqu'à la fin.

## Gérez Astra Trident à l'aide de tridentctl

Le système ["Pack d'installation Trident"](#) inclut l' `tridentctl` utilitaire de ligne de commande qui permet un accès simple à Astra Trident. Les utilisateurs Kubernetes disposant de priviléges suffisants peuvent l'utiliser pour installer Astra Trident ou gérer le namespace qui contient le pod Astra Trident.

### Commandes et indicateurs globaux

Vous pouvez exécuter `tridentctl help` pour obtenir une liste des commandes disponibles pour `tridentctl` ou ajouter l' `--help` indicateur à n'importe quelle commande afin d'obtenir une liste d'options et d'indicateurs pour cette commande spécifique.

```
tridentctl [command] [--optional-flag]
```

L'utilitaire Astra Trident `tridentctl` prend en charge les commandes et indicateurs globaux suivants.

## Commandes

### **create**

Ajoutez une ressource à Astra Trident.

### **delete**

Supprimez une ou plusieurs ressources d'Astra Trident.

### **get**

Obtenez une ou plusieurs ressources d'Astra Trident.

### **help**

Aide sur n'importe quelle commande.

### **images**

Imprimez un tableau des images de conteneur dont Astra Trident a besoin.

### **import**

Importez une ressource existante dans Astra Trident.

### **install**

Installer Astra Trident.

### **logs**

Imprimez les journaux depuis Astra Trident.

### **send**

Envoyer une ressource depuis Astra Trident.

### **uninstall**

Désinstallez Astra Trident.

### **update**

Modifier une ressource dans Astra Trident.

### **update backend state**

Suspendre temporairement les opérations back-end.

### **upgrade**

Mise à niveau d'une ressource dans Astra Trident

### **version**

Imprimez la version d'Astra Trident.

## Alarmes globales

### **-d, --debug**

Sortie de débogage.

### **-h, --help**

Aide pour tridentctl.

### **-k, --kubeconfig string**

Spécifiez le KUBECONFIG chemin d'exécution des commandes en local ou d'un cluster Kubernetes vers un autre.



Vous pouvez également exporter la KUBECONFIG variable pour pointer vers un cluster Kubernetes spécifique et lancer des tridentctl commandes vers ce cluster.

### **-n, --namespace string**

Espace de noms du déploiement d'Astra Trident.

### **-o, --output string**

Format de sortie. Un de json|yaml|nom|large|ps (par défaut).

### **-s, --server string**

Adresse/port de l'interface REST d'Astra Trident.



Vous pouvez configurer l'interface REST de Trident pour écouter et utiliser l'interface 127.0.0.1 (pour IPv4) ou [::1] (pour IPv6) uniquement.

## Options et indicateurs de commande

### création

Utilisez create la commande pour ajouter une ressource à Astra Trident.

```
tridentctl create [option]
```

### Options

backend: Ajouter un back-end à Astra Trident.

### supprimer

Utilisez delete la commande pour supprimer une ou plusieurs ressources d'Astra Trident.

```
tridentctl delete [option]
```

### Options

backend: Supprimez un ou plusieurs systèmes back-end de stockage d'Astra Trident.

snapshot: Supprimez un ou plusieurs snapshots de volume d'Astra Trident.

storageclass: Supprimez une ou plusieurs classes de stockage d'Astra Trident.

**volume:** Supprimez un ou plusieurs volumes de stockage d'Astra Trident.

## obtenez

Utilisez `get` la commande pour obtenir une ou plusieurs ressources d'Astra Trident.

```
tridentctl get [option]
```

## Options

`backend`: Obtenez un ou plusieurs systèmes back-end de stockage d'Astra Trident.

`snapshot`: Obtenez un ou plusieurs snapshots d'Astra Trident.

`storageclass`: Obtenez une ou plusieurs classes de stockage d'Astra Trident.

`volume`: Obtenez un ou plusieurs volumes d'Astra Trident.

## Alarmes

`-h, --help`: Aide pour les volumes.

`--parentOfSubordinate string`: Limiter la requête au volume source subordonné.

`--subordinateOf string`: Limiter la requête aux subordonnés de volume.

## images

Utilisez `images` des indicateurs pour imprimer un tableau des images de conteneur requises par Astra Trident.

```
tridentctl images [flags]
```

## Alarmes

`-h, --help`: Aide pour les images.

`-v, --k8s-version string`: Version sémantique du cluster Kubernetes.

## importer le volume

Utiliser `import volume` la commande pour importer un volume existant dans Astra Trident.

```
tridentctl import volume <backendName> <volumeName> [flags]
```

## Alias

`volume, v`

## Alarmes

`-f, --filename string`: Chemin d'accès au fichier ESV YAML ou JSON.

`-h, --help`: Aide pour le volume.

`--no-manage`: Créer PV/PVC uniquement. Ne supposez pas la gestion du cycle de vie des volumes.

## installer

Utilisez les `install` drapeaux pour installer Astra Trident.

```
tridentctl install [flags]
```

## Alarmes

```
--autosupport-image string: L'image conteneur pour la télémétrie AutoSupport (par défaut "NetApp/Trident AutoSupport:<current-version>").  
--autosupport-proxy string: Adresse/port d'un proxy pour l'envoi de la télémétrie AutoSupport.  
--enable-node-prep: Tentative d'installation des modules requis sur les nœuds.  
--generate-custom-yaml: Générer des fichiers YAML sans rien installer.  
-h, --help: Aide pour l'installation.  
--http-request-timeout: Remplacer le délai d'expiration de la requête HTTP pour l'API REST du contrôleur Trident (1m30s par défaut).  
--image-registry string: Adresse/port d'un registre d'images interne.  
--k8s-timeout duration: Délai d'expiration pour toutes les opérations Kubernetes (3m0s par défaut).  
--kubelet-dir string: Emplacement de l'hôte de l'état interne de kubelet (par défaut "/var/lib/kubelet").  
--log-format string: Le format de consignation Astra Trident (texte, json) (par défaut "texte").  
--pv string: Le nom de l'ancien PV utilisé par Astra Trident, s'assure que ce n'est pas le cas (par défaut "Trident").  
--pvc string: Le nom de l'ancien PVC utilisé par Astra Trident, s'assure que ce n'est pas le cas (par défaut "Trident").  
--silence-autosupport: N'envoyez pas automatiquement de paquets AutoSupport à NetApp (valeur par défaut true).  
--silent: Désactivez la plupart des sorties pendant l'installation.  
--trident-image string: L'image Astra Trident à installer.  
--use-custom-yaml: Utilisez tous les fichiers YAML existants qui existent dans le répertoire d'installation.  
--use-ipv6: Utilisez IPv6 pour la communication d'Astra Trident.
```

## journaux

Utilisez logs des indicateurs pour imprimer les journaux à partir d'Astra Trident.

```
tridentctl logs [flags]
```

## Alarmes

```
-a, --archive: Créez une archive de support avec tous les journaux, sauf indication contraire.  
-h, --help: Aide pour les journaux.  
-l, --log string: Astra Trident log à afficher. L'une des options Trident|auto|Trident-operator|All (par défaut, « auto »).  
--node string: Nom du nœud Kubernetes à partir duquel collecter les journaux du pod du nœud.  
-p, --previous: Si elle existe, obtenez les journaux de l'instance de conteneur précédente.  
--sidecars: Obtenir les billes pour les conteneurs sidecar.
```

## envoyer

Utiliser send la commande pour envoyer une ressource à partir d'Astra Trident.

```
tridentctl send [option]
```

## Options

autosupport: Envoyer une archive AutoSupport à NetApp.

## désinstaller

Utilisez `uninstall` des indicateurs pour désinstaller Astra Trident.

```
tridentctl uninstall [flags]
```

## Alarmes

- `-h, --help`: Aide pour la désinstallation.
- `--silent`: Désactivez la plupart des sorties lors de la désinstallation.

## mise à jour

Utiliser `update` la commande pour modifier une ressource dans Astra Trident.

```
tridentctl update [option]
```

## Options

- `backend`: Mettre à jour un backend dans Astra Trident.

## mettre à jour l'état back-end

Utiliser `update backend state` la commande pour suspendre ou reprendre les opérations back-end.

```
tridentctl update backend state <backend-name> [flag]
```

## Points à prendre en compte

- Si un backend est créé à l'aide d'une `TridentBackendConfig` (tbc), le backend ne peut pas être mis à jour à l'aide d'un `backend.json` fichier.
- Si le `userState` a été défini dans un tbc, il ne peut pas être modifié à l'aide de la `tridentctl update backend state <backend-name> --user-state suspended/normal` commande.
- Pour rétablir la possibilité de définir le `userState` via `tridentctl` une fois qu'il a été défini via tbc, le `userState` champ doit être supprimé du tbc. Cela peut être fait à l'aide de la `kubectl edit tbc` commande. Une fois le `userState` champ supprimé, vous pouvez utiliser `tridentctl update backend state` la commande pour modifier le `userState` d'un back-end.
- Utilisez les `tridentctl update backend state` pour modifier le `userState`. Vous pouvez également mettre à jour le `userState` fichier en utilisant `TridentBackendConfig` ou `backend.json` ; ceci déclenche une réinitialisation complète du back-end et peut prendre du temps.

## Alarmes

- `-h, --help`: Aide pour l'état back-end.
- `--user-state`: Défini sur `suspended` pour interrompre les opérations back-end. Défini sur `normal` pour reprendre les opérations back-end. Si réglé sur `suspended`:

- `AddVolume` et `Import Volume` sont en pause.
- `CloneVolume`, `ResizeVolume` `PublishVolume`, , `UnPublishVolume`, `CreateSnapshot` `GetSnapshot` `RestoreSnapshot`, `DeleteSnapshot`, , `RemoveVolume`, `GetVolumeExternal` `ReconcileNodeAccess` et restent disponibles.

Vous pouvez également mettre à jour l'état du back-end à l'aide du `userState` champ dans le fichier de configuration du back-end `TridentBackendConfig` ou `backend.json`. Pour plus d'informations, reportez-

vous à "Options de gestion des systèmes back-end" et "Effectuer la gestion back-end avec kubectl".

**Exemple:**

## JSON

Procédez comme suit pour mettre à jour `userState` à l'aide du `backend.json` fichier :

1. Modifiez le `backend.json` fichier pour inclure le `userState` champ avec sa valeur définie sur « terminé ».
2. Mettez à jour le backend à l'aide de la `tridentctl backend update` commande et du chemin d'accès au fichier mis à jour `backend.json`.

**Exemple :** `tridentctl backend update -f /<path to backend JSON file>/backend.json`

```
{  
  "version": 1,  
  "storageDriverName": "ontap-nas",  
  "managementLIF": "<redacted>",  
  "svm": "nas-svm",  
  "backendName": "customBackend",  
  "username": "<redacted>",  
  "password": "<redacted>",  
  "userState": "suspended",  
}
```

## YAML

Vous pouvez modifier la commande `tbc` une fois qu'elle a été appliquée à l'aide de la `kubectl edit <tbc-name> -n <namespace>` commande. L'exemple suivant met à jour l'état back-end pour qu'il soit suspendu à l'aide de l' `userState: suspended` option :

```
apiVersion: trident.netapp.io/v1  
kind: TridentBackendConfig  
metadata:  
  name: backend-ontap-nas  
spec:  
  version: 1  
  backendName: customBackend  
  storageDriverName: ontap-nas  
  managementLIF: <redacted>  
  svm: nas-svm  
  userState: suspended  
  credentials:  
    name: backend-tbc-ontap-nas-secret
```

## version

Utilisez `version` des indicateurs pour imprimer la version de `tridentctl` et le service Trident en cours d'exécution.

```
tridentctl version [flags]
```

## Alarmes

`--client`: Version client uniquement (pas de serveur requis).  
`-h, --help`: Aide pour la version.

# Contrôle d'Astra Trident

ASTRA Trident fournit un ensemble de terminaux de metrics Prometheus que vous pouvez utiliser pour contrôler les performances d'Astra Trident.

## Présentation

Avec les metrics d'Astra Trident, vous pouvez :

- Surveillez l'état et la configuration d'Astra Trident. Vous avez la possibilité d'examiner la réussite des opérations et de savoir si elles peuvent communiquer avec les systèmes back-end comme prévu.
- Examiner les informations d'utilisation du système back-end et comprendre le nombre de volumes provisionnés sur un système back-end, ainsi que la quantité d'espace consommé, etc.
- Conservez un mappage de la quantité de volumes provisionnés sur les systèmes back-end disponibles.
- Suivi des performances. Découvrez le temps nécessaire pour communiquer avec Astra Trident aux systèmes back-end et effectuer les opérations.



Par défaut, les mesures de Trident sont exposées sur le port cible 8001 au niveau du `/metrics` noeud final. Ces mesures sont **activées par défaut** lors de l'installation de Trident.

## Ce dont vous avez besoin

- Cluster Kubernetes avec Astra Trident installé.
- Instance Prometheus. Ce peut être un "[Déploiement conteneurisé par Prometheus](#)" ou vous pouvez choisir d'exécuter Prometheus comme un "[application native](#)".

## Étape 1 : définir une cible Prometheus

Vous devez définir une cible Prometheus pour collecter les metrics et obtenir des informations sur les systèmes back-end gérés par Trident, les volumes qu'elle crée, etc. ["Blog"](#) Vous apprendrez ainsi à utiliser Prometheus et Grafana avec Astra Trident pour récupérer des metrics. Découvrez sur ce blog comment exécuter Prometheus en tant qu'opérateur dans votre cluster Kubernetes et comment créer un ServiceMonitor pour obtenir des metrics Astra Trident.

## Étape 2 : créer un ServiceMonitor Prometheus

Pour consommer les metrics Trident, vous devez créer un ServiceMonitor Prometheus qui surveille le `trident-csi` service et écoute sur le `metrics` port. Un exemple de ServiceMonitor se présente comme suit :

```

apiVersion: monitoring.coreos.com/v1
kind: ServiceMonitor
metadata:
  name: trident-sm
  namespace: monitoring
  labels:
    release: prom-operator
spec:
  jobLabel: trident
  selector:
    matchLabels:
      app: controller.csi.trident.netapp.io
  namespaceSelector:
    matchNames:
    - trident
  endpoints:
  - port: metrics
    interval: 15s

```

Cette définition de ServiceMonitor récupère les mesures renvoyées par le `trident-csi` service et recherche spécifiquement le `metrics` point final du service. Par conséquent, Prometheus est désormais configuré pour être en mesure de comprendre les metrics d'Astra Trident.

En plus des metrics disponibles directement depuis Astra Trident, kubelet expose de nombreux `kubelet_volume_* metrics` via son propre terminal de metrics. Kubelet peut fournir des informations sur les volumes reliés, ainsi que sur les pods et autres opérations internes qu'elle gère. Reportez-vous à la ["ici"](#).

### Étape 3 : interroger les mesures Trident avec PromQL

PromQL est bon pour la création d'expressions qui renvoient des séries chronologiques ou des données tabulaires.

Voici quelques questions PromQL que vous pouvez utiliser :

#### Accédez aux informations sur l'état de santé de Trident

- Pourcentage de réponses HTTP 2XX d'Astra Trident

```
(sum (trident_rest_ops_seconds_total_count{status_code=~"2.."}) OR on()
vector(0)) / sum (trident_rest_ops_seconds_total_count)) * 100
```

- Pourcentage de réponses REST d'Astra Trident par le code d'état

```
(sum (trident_rest_ops_seconds_total_count) by (status_code) / scalar
(sum (trident_rest_ops_seconds_total_count))) * 100
```

- Durée moyenne en ms des opérations effectuées par Astra Trident

```
sum by (operation)
(trident_operation_duration_milliseconds_sum{success="true"}) / sum by
(operation)
(trident_operation_duration_milliseconds_count{success="true"})
```

## Découvrez les informations d'utilisation d'Astra Trident

- Taille moyenne du volume

```
trident_volume_allocated_bytes/trident_volume_count
```

- Espace volume total provisionné par chaque back-end

```
sum (trident_volume_allocated_bytes) by (backend_uuid)
```

## Utiliser individuellement le volume



Cette activation est uniquement possible si les indicateurs kubelet sont également collectés.

- Pourcentage d'espace utilisé pour chaque volume

```
kubelet_volume_stats_used_bytes / kubelet_volume_stats_capacity_bytes * 100
```

## Découvrez la télémétrie AutoSupport d'Astra Trident

Par défaut, Astra Trident envoie des metrics de Prometheus et des informations de base back-end à NetApp dans un rythme quotidien.

- Pour empêcher Astra Trident d'envoyer des metrics Prometheus et des informations back-end de base à NetApp, transmettez le `--silence-autosupport` drapeau lors de l'installation d'Astra Trident.
- ASTRA Trident peut également envoyer des journaux de conteneur à NetApp support à la demande via `tridentctl send autosupport`. Vous devrez déclencher Astra Trident pour télécharger ses journaux. Avant de soumettre des journaux, vous devez accepter les fichiers NetApp "[politique de confidentialité](#)".
- Sauf mention contraire, Astra Trident extrait les journaux des 24 dernières heures.
- Vous pouvez spécifier la durée de conservation du journal avec l' `--since` indicateur. Par exemple : `tridentctl send autosupport --since=1h`. Ces informations sont collectées et envoyées via un `trident-autosupport` conteneur installé avec Astra Trident. Vous pouvez obtenir l'image du conteneur à l'adresse "[AutoSupport Trident](#)".
- Le AutoSupport Trident ne collecte pas et ne transmet pas d'informations à caractère personnel (PII) ou de données personnelles. Il est fourni avec un "[CLUF](#)" qui ne s'applique pas à l'image du conteneur Trident. Pour en savoir plus sur l'engagement de NetApp en faveur de la sécurité et de la confiance des données

"ici".

Voici un exemple de charge utile envoyée par Astra Trident :

```
---
items:
- backendUUID: ff3852e1-18a5-4df4-b2d3-f59f829627ed
  protocol: file
  config:
    version: 1
    storageDriverName: ontap-nas
    debug: false
    debugTraceFlags:
    disableDelete: false
    serialNumbers:
    - nwkvzfanek_SN
    limitVolumeSize: ''
  state: online
  online: true
```

- Les messages AutoSupport sont envoyés au terminal AutoSupport de NetApp. Si vous utilisez un registre privé pour stocker des images de conteneur, vous pouvez utiliser l' `--image-registry` indicateur.
- Vous pouvez également configurer des URL proxy en générant les fichiers YAML d'installation. Ceci peut être fait en utilisant `tridentctl install --generate-custom-yaml` pour créer les fichiers YAML et en ajoutant l' `--proxy-url` argument pour le `trident-autosupport` conteneur dans `trident-deployment.yaml`.

## Désactivation des metrics d'Astra Trident

Pour que **disable** metrics ne soient pas signalés, vous devez générer des YAML personnalisés (à l'aide de `--generate-custom-yaml` l'indicateur) et les modifier pour supprimer l' `--metrics` `indicateur d'appel pour le `trident-main` conteneur.

## Désinstaller Astra Trident

Vous devez utiliser la même méthode pour désinstaller Astra Trident que pour installer Astra Trident.

### Description de la tâche

- Si vous avez besoin d'un correctif pour les bugs observés après une mise à niveau, des problèmes de dépendance ou une mise à niveau non réussie ou incomplète, désinstallez Astra Trident et réinstallez la version précédente en suivant les instructions spécifiques à cette mise à niveau "[version](#)". Il s'agit de la seule méthode recommandée pour *rétrograder* vers une version antérieure.
- Pour faciliter la mise à niveau et la réinstallation, la désinstallation d'Astra Trident ne supprime pas les CRD ou les objets associés créés par Astra Trident. Si vous devez supprimer complètement Astra Trident et toutes ses données, reportez-vous à la "[Retirez complètement Astra Trident et les CRD](#)".

### Avant de commencer

Si vous désaffectez des clusters Kubernetes, vous devez supprimer toutes les applications qui utilisent des volumes créés par Astra Trident avant de procéder à la désinstallation. Cela permet de s'assurer que les ESV ne sont pas publiées sur les nœuds Kubernetes avant d'être supprimées.

## Déterminez la méthode d'installation d'origine

Vous devez utiliser la même méthode pour désinstaller Astra Trident que vous avez utilisée pour l'installer. Avant de procéder à la désinstallation, vérifiez quelle version vous avez utilisée pour installer Astra Trident à l'origine.

1. Utilisez `kubectl get pods -n trident` pour examiner les modules.
  - S'il n'y a pas de module opérateur, Astra Trident a été installée à l'aide de `tridentctl`.
  - S'il existe un pod opérateur, Astra Trident a été installé à l'aide de l'opérateur Trident soit manuellement, soit à l'aide d'Helm.
2. S'il existe un module opérateur, utilisez `kubectl describe tproc trident` pour déterminer si Astra Trident a été installée à l'aide de Helm.
  - S'il y a une étiquette Helm, Astra Trident a été installée à l'aide d'Helm.
  - S'il n'y a pas d'étiquette Helm, Astra Trident a été installé manuellement à l'aide de l'opérateur Trident.

## Désinstallez l'installation d'un opérateur Trident

Vous pouvez désinstaller manuellement l'installation d'un opérateur trident ou à l'aide d'Helm.

### Désinstallez l'installation manuelle

Si vous avez installé Astra Trident à l'aide de l'opérateur, vous pouvez le désinstaller en effectuant l'une des opérations suivantes :

1. **Modifiez `TridentOrchestrator` CR et définissez l'indicateur de désinstallation :**

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

Lorsque l'`uninstall` `indicateur est défini sur `true, l'opérateur Trident désinstalle Trident, mais ne supprime pas l'orchestrateur TridentOrchestrator lui-même. Vous devez nettoyer TridentOrchestrator et en créer un nouveau si vous souhaitez réinstaller Trident.

2. **Supprimer `TridentOrchestrator`** : en supprimant le `TridentOrchestrator` CR utilisé pour déployer Astra Trident, vous demandez à l'opérateur de désinstaller Trident. L'opérateur traite la suppression `TridentOrchestrator` et procède à la suppression du déploiement et du démonset Astra Trident, en supprimant les pods Trident qu'il avait créés dans le cadre de l'installation.

```
kubectl delete -f deploy/<bundle.yaml> -n <namespace>
```

## Désinstallez l'installation d'Helm

Si vous avez installé Astra Trident en utilisant Helm, vous pouvez le désinstaller en utilisant `helm uninstall`.

```
#List the Helm release corresponding to the Astra Trident install.
helm ls -n trident
NAME          NAMESPACE      REVISION      UPDATED
STATUS        CHART
trident      trident        1            2021-04-20
00:26:42.417764794 +0000 UTC deployed      trident-operator-21.07.1
21.07.1

#Uninstall Helm release to remove Trident
helm uninstall trident -n trident
release "trident" uninstalled
```

## Désinstallez une `tridentctl` installation

Utilisez `uninstall` la commande dans `tridentctl` pour supprimer toutes les ressources associées à Astra Trident, à l'exception des CRD et des objets associés :

```
./tridentctl uninstall -n <namespace>
```

# Astra Trident pour Docker

## Conditions préalables au déploiement

Vous devez installer et configurer les protocoles requis sur votre hôte avant de déployer Astra Trident.

### Vérifier les exigences

- Vérifiez que votre déploiement correspond à tous les "[de formation](#)".
- Vérifiez que vous disposez d'une version prise en charge de Docker installée. Si votre version de Docker n'est pas à jour, "[installez-le ou mettez-le à jour](#)".

```
docker --version
```

- Vérifiez que les prérequis de protocole sont installés et configurés sur votre hôte.

### Outils NFS

Installez les outils NFS à l'aide des commandes de votre système d'exploitation.

#### RHEL 8+

```
sudo yum install -y nfs-utils
```

#### Ubuntu

```
sudo apt-get install -y nfs-common
```



Redémarrez les nœuds workers après l'installation des outils NFS afin d'éviter toute défaillance lors de la connexion des volumes aux conteneurs.

### Outils iSCSI

Installez les outils iSCSI à l'aide des commandes de votre système d'exploitation.

## RHEL 8+

1. Installez les packages système suivants :

```
sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils device-mapper-multipath
```

2. Vérifiez que la version iscsi-initiator-utils est 6.2.0.874-2.el7 ou ultérieure :

```
rpm -q iscsi-initiator-utils
```

3. Définir la numérisation sur manuelle :

```
sudo sed -i 's/^\\(node.session.scan\\) .*\\1 = manual/' /etc/iscsi/iscsid.conf
```

4. Activer les chemins d'accès multiples :

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```



Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de defaults.

5. Assurez-vous que `iscsid` et `multipathd` sont en cours d'exécution :

```
sudo systemctl enable --now iscsid multipathd
```

6. Activer et démarrer `iscsi`:

```
sudo systemctl enable --now iscsi
```

## Ubuntu

1. Installez les packages système suivants :

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools scsitools
```

2. Vérifiez que la version Open-iscsi est 2.0.874-5ubuntu2.10 ou ultérieure (pour bionic) ou 2.0.874-7.1ubuntu6.1 ou ultérieure (pour focal) :

```
dpkg -l open-iscsi
```

### 3. Définir la numérisation sur manuelle :

```
sudo sed -i 's/^\\(node.session.scan\\) .*\\1 = manual/'  
/etc/iscsi/iscsid.conf
```

### 4. Activer les chemins d'accès multiples :

```
sudo tee /etc/multipath.conf <<-'EOF'  
defaults {  
    user_friendly_names yes  
    find_multipaths no  
}  
EOF  
sudo systemctl enable --now multipath-tools.service  
sudo service multipath-tools restart
```



Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

### 5. Assurez-vous que `open-iscsi` et `multipath-tools` sont activés et en cours d'exécution :

```
sudo systemctl status multipath-tools  
sudo systemctl enable --now open-iscsi.service  
sudo systemctl status open-iscsi
```

## Outils NVMe

Installez les outils NVMe à l'aide des commandes correspondant à votre système d'exploitation.

- NVMe requiert RHEL 9 ou version ultérieure.
- Si la version du noyau de votre nœud Kubernetes est trop ancienne ou si le package NVMe n'est pas disponible pour votre version du noyau, vous devrez peut-être mettre à jour la version du noyau de votre nœud avec le package NVMe.

## RHEL 9

```
sudo yum install nvme-cli
sudo yum install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

## Ubuntu

```
sudo apt install nvme-cli
sudo apt -y install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

# Déployez Astra Trident

ASTRA Trident pour Docker offre une intégration directe avec l'écosystème Docker pour les plateformes de stockage NetApp. Il prend en charge le provisionnement et la gestion des ressources de stockage, depuis la plateforme de stockage jusqu'aux hôtes Docker, par exemple, l'ajout de plateformes supplémentaires à l'avenir.

Plusieurs instances d'Astra Trident peuvent être exécutées simultanément sur le même hôte. Vous pouvez ainsi établir des connexions simultanées à plusieurs systèmes et types de stockage, et personnaliser le stockage utilisé pour les volumes Docker.

### Ce dont vous avez besoin

Voir la "["conditions préalables au déploiement"](#)". Une fois que vous avez rempli les conditions préalables, vous êtes prêt à déployer Astra Trident.

## Méthode de plug-in géré Docker (version 1.13/17.03 et ultérieure)

### Avant de commencer



Si vous avez utilisé Astra Trident pré Docker 1.13/17.03 dans la méthode du démon traditionnel, veillez à arrêter le processus Astra Trident et à redémarrer votre démon Docker avant d'utiliser la méthode du plug-in géré.

1. Arrêter toutes les instances en cours d'exécution :

```
pkill /usr/local/bin/netappdvp
pkill /usr/local/bin/trident
```

2. Redémarrez Docker.

```
systemctl restart docker
```

3. Vérifiez que Docker Engine 17.03 (nouveau modèle 1.13) ou ultérieur est installé.

```
docker --version
```

Si votre version est obsolète, ["installez ou mettez à jour votre installation"](#).

## Étapes

1. Créez un fichier de configuration et spécifiez les options comme suit :

- config: Le nom de fichier par défaut est config.json, mais vous pouvez utiliser n'importe quel nom en spécifiant l' config`option avec le nom de fichier. Le fichier de configuration doit se trouver dans le `/etc/netappdvp répertoire du système hôte.
- log-level: Spécifiez le niveau de journalisation (debug info, , warn, , error fatal ). La valeur par défaut est info.
- debug: Spécifiez si la journalisation de débogage est activée. La valeur par défaut est FALSE. Remplace le niveau de journalisation si vrai.

i. Créez un emplacement pour le fichier de configuration :

```
sudo mkdir -p /etc/netappdvp
```

ii. Créez le fichier de configuration :

```
cat << EOF > /etc/netappdvp/config.json
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "managementLIF": "10.0.0.1",
    "dataLIF": "10.0.0.2",
    "svm": "svm_nfs",
    "username": "vsadmin",
    "password": "password",
    "aggregate": "aggr1"
}
EOF
```

2. Démarrez Astra Trident à l'aide du système de plug-in géré. Remplacez <version>-le par la version du plug-in (xxx.xx.x) que vous utilisez.

```
docker plugin install --grant-all-permissions --alias netapp
netapp/trident-plugin:<version> config=myConfigFile.json
```

3. Commencez à utiliser Astra Trident pour consommer le stockage à partir du système configuré.

- a. Créez un volume nommé « firstVolume » :

```
docker volume create -d netapp --name firstVolume
```

- b. Créez un volume par défaut au démarrage du conteneur :

```
docker run --rm -it --volume-driver netapp --volume secondVolume:/my_vol alpine ash
```

- c. Supprimez le volume « firstVolume » :

```
docker volume rm firstVolume
```

## Méthode traditionnelle (version 1.12 ou antérieure)

### Avant de commencer

1. Vérifiez que Docker version 1.10 ou ultérieure est installé.

```
docker --version
```

Si votre version est obsolète, mettez à jour votre installation.

```
curl -fsSL https://get.docker.com/ | sh
```

Ou, "suivez les instructions relatives à votre distribution".

2. Vérifiez que NFS et/ou iSCSI sont configurés pour votre système.

### Étapes

1. Installez et configurez le plug-in de volume NetApp Docker :

- a. Téléchargez et déballez l'application :

```
wget  
https://github.com/NetApp/trident/releases/download/v24.10.0/trident-  
installer-24.06.0.tar.gz  
tar zxf trident-installer-24.06.0.tar.gz
```

- b. Déplacer vers un emplacement dans le chemin du bac :

```
sudo mv trident-installer/extras/bin/trident /usr/local/bin/  
sudo chown root:root /usr/local/bin/trident  
sudo chmod 755 /usr/local/bin/trident
```

c. Créez un emplacement pour le fichier de configuration :

```
sudo mkdir -p /etc/netappdvp
```

d. Créez le fichier de configuration :

```
cat << EOF > /etc/netappdvp/ontap-nas.json  
{  
    "version": 1,  
    "storageDriverName": "ontap-nas",  
    "managementLIF": "10.0.0.1",  
    "dataLIF": "10.0.0.2",  
    "svm": "svm_nfs",  
    "username": "vsadmin",  
    "password": "password",  
    "aggregate": "agg1"  
}  
EOF
```

2. Après avoir placé le fichier binaire et créé le fichier de configuration, démarrez le démon Trident en utilisant le fichier de configuration souhaité.

```
sudo trident --config=/etc/netappdvp/ontap-nas.json
```



Sauf indication contraire, le nom par défaut du pilote de volume est « NetApp ».

Une fois le démon démarré, vous pouvez créer et gérer des volumes à l'aide de l'interface de ligne de commande de Docker

3. Créer un volume :

```
docker volume create -d netapp --name trident_1
```

4. Provisionnement d'un volume Docker lors du démarrage d'un conteneur :

```
docker run --rm -it --volume-driver netapp --volume trident_2:/my_vol  
alpine ash
```

5. Supprimer un volume Docker :

```
docker volume rm trident_1
docker volume rm trident_2
```

## Commencez avec Astra Trident au démarrage du système

Un exemple de fichier d'unité pour les systèmes basés sur le système se trouve `contrib/trident.service.example` dans le Git repo. Pour utiliser le fichier avec RHEL, procédez comme suit :

1. Copiez le fichier à l'emplacement correct.

Vous devez utiliser des noms uniques pour les fichiers d'unité si plusieurs instances sont en cours d'exécution.

```
cp contrib/trident.service.example
/usr/lib/systemd/system/trident.service
```

2. Modifiez le fichier, modifiez la description (ligne 2) pour qu'elle corresponde au nom du pilote et au chemin du fichier de configuration (ligne 9) pour qu'elle corresponde à votre environnement.
3. Recharger le système pour qu'il ingère les modifications :

```
systemctl daemon-reload
```

4. Activer le service.

Ce nom varie en fonction de ce que vous avez appelé le fichier dans le `/usr/lib/systemd/system` répertoire.

```
systemctl enable trident
```

5. Démarrer le service.

```
systemctl start trident
```

6. Afficher l'état.

```
systemctl status trident
```



Chaque fois que vous modifiez le fichier d'unité, exécutez la `systemctl daemon-reload` commande pour qu'il soit informé des modifications.

## Mise à niveau ou désinstallation d'Astra Trident

Vous pouvez mettre à niveau Astra Trident pour Docker en toute sécurité, sans impact sur les volumes en cours d'utilisation. Au cours du processus de mise à niveau, les `docker volume` commandes dirigées vers le plug-in ne réussiront pas et les applications ne pourront pas monter les volumes tant que le plug-in ne sera pas exécuté à nouveau. Dans la plupart des cas, c'est une question de secondes.

### Mise à niveau

Suivez les étapes ci-dessous pour mettre à niveau Astra Trident pour Docker.

#### Étapes

1. Lister les volumes existants :

```
docker volume ls
DRIVER          VOLUME NAME
netapp:latest    my_volume
```

2. Désactivez le plug-in :

```
docker plugin disable -f netapp:latest
docker plugin ls
ID                  NAME          DESCRIPTION
ENABLED
7067f39a5df5      netapp:latest  nDVP - NetApp Docker Volume
Plugin    false
```

3. Mettez à niveau le plug-in :

```
docker plugin upgrade --skip-remote-check --grant-all-permissions
netapp:latest netapp/trident-plugin:21.07
```



La version 18.01 d'Astra Trident remplace le nDVP. Vous devez effectuer une mise à niveau directe de l' `netapp/ndvp-plugin` image vers l' `netapp/trident-plugin` image.

4. Activer le plug-in :

```
docker plugin enable netapp:latest
```

## 5. Vérifiez que le plug-in est activé :

```
docker plugin ls
ID          NAME          DESCRIPTION
ENABLED
7067f39a5df5  netapp:latest  Trident - NetApp Docker Volume
Plugin      true
```

## 6. Vérifier que les volumes sont visibles :

```
docker volume ls
DRIVER          VOLUME NAME
netapp:latest    my_volume
```

 Si vous effectuez la mise à niveau d'une ancienne version d'Astra Trident (pré-20.10) vers Astra Trident 20.10 ou version ultérieure, vous risquez de vous produire une erreur. Pour plus d'informations, reportez-vous "[Problèmes connus](#)" à . Si vous entrez dans l'erreur, vous devez d'abord désactiver le plug-in, puis supprimer le plug-in, puis installer la version d'Astra Trident requise en passant un paramètre de configuration supplémentaire : `docker plugin install netapp/trident-plugin:20.10 --alias netapp --grant-all-permissions config=config.json`

## Désinstaller

Effectuez les opérations suivantes pour désinstaller Astra Trident pour Docker.

### Étapes

1. Supprimez tous les volumes créés par le plug-in.
2. Désactivez le plug-in :

```
docker plugin disable netapp:latest
docker plugin ls
ID          NAME          DESCRIPTION
ENABLED
7067f39a5df5  netapp:latest  nDVP - NetApp Docker Volume
Plugin      false
```

3. Retirez le plug-in :

```
docker plugin rm netapp:latest
```

# Utilisation de volumes

Vous pouvez facilement créer, cloner et supprimer des volumes à l'aide des commandes standard `docker volume` avec le nom de pilote Astra Trident spécifié si nécessaire.

## Créer un volume

- Créez un volume avec un pilote à l'aide du nom par défaut :

```
docker volume create -d netapp --name firstVolume
```

- Créez un volume avec une instance Astra Trident spécifique :

```
docker volume create -d ntap_bronze --name bronzeVolume
```



Si vous ne spécifiez aucune "options", les valeurs par défaut du pilote sont utilisées.

- Remplacer la taille du volume par défaut. Voir l'exemple suivant pour créer un volume de 20 Gio avec un pilote :

```
docker volume create -d netapp --name my_vol --opt size=20G
```



Les tailles de volume sont exprimées en chaînes contenant une valeur entière avec des unités facultatives (par exemple : 10G, 20 Go, Tio). Si aucune unité n'est spécifiée, la valeur par défaut est G. les unités de taille peuvent être exprimées en puissances de 2 (B, KiB, MiB, Gio, Tio) ou en puissances de 10 (B, Ko, Mo, Go, To). Les unités de raccourci utilisent des puissances de 2 (G = Gio, T = Tio, ...).

## Supprimer un volume

- Supprimez le volume comme n'importe quel autre volume Docker :

```
docker volume rm firstVolume
```



Lorsque vous utilisez le `solidfire-san` pilote, l'exemple ci-dessus supprime et purge le volume.

Suivez les étapes ci-dessous pour mettre à niveau Astra Trident pour Docker.

## Clonez un volume

Lorsque vous utilisez les `ontap-nas`, `ontap-san`, `solidfire-san` et `gcp-cvs` storage drivers, Astra Trident peut cloner des volumes. Lorsque vous utilisez les `ontap-nas-flexgroup` pilotes ou `ontap-`

nas-economy, le clonage n'est pas pris en charge. La création d'un nouveau volume à partir d'un volume existant entraîne la création d'un nouveau snapshot.

- Inspectez le volume pour énumérer les instantanés :

```
docker volume inspect <volume_name>
```

- Créer un nouveau volume à partir d'un volume existant. Cela entraîne la création d'un nouvel instantané :

```
docker volume create -d <driver_name> --name <new_name> -o  
from=<source_docker_volume>
```

- Créer un nouveau volume à partir d'un snapshot existant sur un volume. Cette opération ne crée pas de nouvel instantané :

```
docker volume create -d <driver_name> --name <new_name> -o  
from=<source_docker_volume> -o fromSnapshot=<source_snap_name>
```

## Exemple

```
docker volume inspect firstVolume
```

```
[  
  {  
    "Driver": "ontap-nas",  
    "Labels": null,  
    "Mountpoint": "/var/lib/docker-volumes/ontap-  
nas/netappdvp_firstVolume",  
    "Name": "firstVolume",  
    "Options": {},  
    "Scope": "global",  
    "Status": {  
      "Snapshots": [  
        {  
          "Created": "2017-02-10T19:05:00Z",  
          "Name": "hourly.2017-02-10_1505"  
        }  
      ]  
    }  
  }  
]
```

```
docker volume create -d ontap-nas --name clonedVolume -o from=firstVolume  
clonedVolume
```

```
docker volume rm clonedVolume  
docker volume create -d ontap-nas --name volFromSnap -o from=firstVolume  
-o fromSnapshot=hourly.2017-02-10_1505  
volFromSnap
```

```
docker volume rm volFromSnap
```

## Accéder aux volumes créés en externe

Vous pouvez accéder aux dispositifs de blocs créés en externe (ou à leurs clones) par des conteneurs à l'aide de Trident **uniquement** s'ils n'ont pas de partitions et si leur système de fichiers est pris en charge par Astra Trident (par exemple, un fichier `ext4` formaté `/dev/sdc1` ne sera pas accessible via Astra Trident).

## Options de volume spécifiques au conducteur

Chaque pilote de stockage dispose d'un ensemble d'options différent, que vous pouvez spécifier au moment de la création du volume pour personnaliser le résultat. Vous trouverez ci-dessous les options qui s'appliquent à votre système de stockage configuré.

Ces options sont simples à utiliser lors de l'opération de création de volume. Indiquez l'option et la valeur à l'aide de l'`-o` opérateur pendant le fonctionnement de l'interface de ligne de commande. Ces valeurs

remplacent toute valeur équivalente du fichier de configuration JSON.

## Options de volume ONTAP

Les options de création de volumes pour NFS et iSCSI sont les suivantes :

Option	Description
size	La taille du volume est définie par défaut sur 1 Gio.
spaceReserve	Provisionnement fin ou non fin du volume, conversion par défaut en fin. Les valeurs valides sont <code>none</code> (provisionnement fin) et (provisionnement lourd) volume.
snapshotPolicy	La règle de snapshot sera alors définie sur la valeur souhaitée. La valeur par défaut est <code>none</code> , ce qui signifie qu'aucun instantané ne sera automatiquement créé pour le volume. Sauf modification de la part de votre administrateur de stockage, une règle nommée « par défaut » existe sur tous les systèmes ONTAP qui créent et conserve six snapshots toutes les heures, deux par jour et deux fois par semaine. Les données conservées dans un snapshot peuvent être restaurées en naviguant vers le <code>.snapshot</code> répertoire de n'importe quel répertoire du volume.
snapshotReserve	La réserve d'instantanés sera alors définie sur le pourcentage souhaité. La valeur par défaut n'est pas définie. Cela signifie que ONTAP sélectionne la fonction de copie instantanée (généralement 5 %) si vous avez sélectionné une stratégie de snapshots, ou 0 % si la stratégie de snapshots n'est pas définie. Vous pouvez définir la valeur par défaut des snapshots dans le fichier de configuration pour tous les systèmes back-end ONTAP. Vous pouvez l'utiliser comme option de création de volumes pour tous les systèmes back-end ONTAP, à l'exception des économies ontap-nas.
splitOnClone	Lors du clonage d'un volume, ONTAP va immédiatement séparer le clone de son volume parent. La valeur par défaut est <code>false</code> . Pour optimiser l'efficacité du stockage, il est préférable de séparer le clone de son parent dès sa création, car il est peu probable que cette utilisation soit utile. Par exemple, le clonage d'une base de données vide permet de gagner beaucoup de temps mais réduit les économies de stockage. Il est donc préférable de séparer immédiatement le clone.

Option	Description
encryption	<p>Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume. La valeur par défaut est <code>false</code>. Pour utiliser cette option, NVE doit être sous licence et activé sur le cluster.</p> <p>Si NAE est activé sur le back-end, tous les volumes provisionnés dans Astra Trident seront activés par NAE.</p> <p>Pour plus d'informations, reportez-vous à la section : <a href="#">"Fonctionnement d'Astra Trident avec NVE et NAE"</a>.</p>
tieringPolicy	<p>Définit la règle de hiérarchisation à utiliser pour le volume. Cette décision détermine si les données sont déplacées vers le Tier cloud lorsqu'elles deviennent inactives.</p>

Les options supplémentaires suivantes concernent NFS **uniquement** :

Option	Description
unixPermissions	<p>Cette option contrôle les autorisations définies pour le volume lui-même. Par défaut, les autorisations seront définies sur <code>---rwxr-xr-x</code>, ou en notation numérique 0755, et <code>root</code> sera le propriétaire. Le format texte ou numérique fonctionnera.</p>
snapshotDir	<p>Si vous définissez cette option sur <code>true</code>, le répertoire sera <code>.snapshot</code> visible pour les clients accédant au volume. La valeur par défaut est <code>false</code>, ce qui signifie que la visibilité du <code>.snapshot</code> répertoire est désactivée par défaut. Certaines images, par exemple l'image MySQL officielle, ne fonctionnent pas comme prévu lorsque le <code>.snapshot</code> répertoire est visible.</p>
exportPolicy	<p>Définit l'export policy à utiliser pour le volume. La valeur par défaut est <code>default</code>.</p>
securityStyle	<p>Définit le style de sécurité à utiliser pour accéder au volume. La valeur par défaut est <code>unix</code>. Les valeurs valides sont <code>unix</code> et <code>mixed</code>.</p>

Les options supplémentaires suivantes sont disponibles pour iSCSI **uniquement** :

Option	Description
fileSystemType	Définit le système de fichiers utilisé pour formater les volumes iSCSI. La valeur par défaut est <code>ext4</code> . Les valeurs valides sont <code>ext3</code> , <code>ext4</code> et <code>xfs</code> .
spaceAllocation	Si vous définissez cette option sur <code>false</code> , la fonctionnalité d'allocation d'espace de la LUN sera désactivée. La valeur par défaut est <code>true</code> , ce qui signifie que ONTAP avertit l'hôte lorsque le volume est à court d'espace et que la LUN du volume ne peut pas accepter les écritures. Cette option permet également à ONTAP de récupérer automatiquement de l'espace lorsque votre hôte supprime des données.

## Exemples

Voir les exemples ci-dessous :

- Création d'un volume de 10 Gio :

```
docker volume create -d netapp --name demo -o size=10G -o
encryption=true
```

- Créez un volume de 100 Gio avec les snapshots :

```
docker volume create -d netapp --name demo -o size=100G -o
snapshotPolicy=default -o snapshotReserve=10
```

- Créez un volume dont le bit setuid est activé :

```
docker volume create -d netapp --name demo -o unixPermissions=4755
```

La taille minimale du volume est de 20MiB.

Si la réserve d'instantanés n'est pas spécifiée et que la règle d'instantanés est `none`, Trident utilise une réserve d'instantanés de 0 %.

- Créer un volume sans policy de snapshots et sans réserve de snapshots :

```
docker volume create -d netapp --name my_vol --opt snapshotPolicy=none
```

- Créer un volume sans policy snapshot et une réserve Snapshot personnalisée de 10 % :

```
docker volume create -d netapp --name my_vol --opt snapshotPolicy=none  
--opt snapshotReserve=10
```

- Créer un volume avec une règle Snapshot et une réserve Snapshot personnalisée de 10 % :

```
docker volume create -d netapp --name my_vol --opt  
snapshotPolicy=myPolicy --opt snapshotReserve=10
```

- Créer un volume avec une règle Snapshot et accepter la réserve Snapshot par défaut d'ONTAP (généralement 5 %) :

```
docker volume create -d netapp --name my_vol --opt  
snapshotPolicy=myPolicy
```

## Options de volumes du logiciel Element

Les options du logiciel Element présentent les règles de taille et de qualité de services associées au volume. Lors de la création du volume, la politique de QoS associée est spécifiée à l'aide de la `-o type=service_level` nomenclature.

La première étape pour définir un niveau de service QoS avec le pilote Element consiste à créer au moins un type et à spécifier les IOPS minimum, maximum et en rafale associées à un nom dans le fichier de configuration.

Les autres options de création de volumes du logiciel Element sont les suivantes :

Option	Description
size	La taille du volume, par défaut à 1 Gio ou entrée de configuration ... « Valeurs par défaut » : {« taille » : « 5G »}.
blocksize	Utilisez 512 ou 4096, par défaut 512 ou l'entrée de configuration DefaultBlockSize.

### Exemple

Voir l'exemple de fichier de configuration suivant avec les définitions QoS :

```
{
  "...": "...",
  "Types": [
    {
      "Type": "Bronze",
      "Qos": {
        "minIOPS": 1000,
        "maxIOPS": 2000,
        "burstIOPS": 4000
      }
    },
    {
      "Type": "Silver",
      "Qos": {
        "minIOPS": 4000,
        "maxIOPS": 6000,
        "burstIOPS": 8000
      }
    },
    {
      "Type": "Gold",
      "Qos": {
        "minIOPS": 6000,
        "maxIOPS": 8000,
        "burstIOPS": 10000
      }
    }
  ]
}
```

Dans la configuration ci-dessus, nous avons trois définitions de règles : bronze, Silver et Gold. Ces noms sont arbitraires.

- Crédit d'un volume Gold de 10 Gio :

```
docker volume create -d solidfire --name sfGold -o type=Gold -o size=10G
```

- Créez un volume Bronze de 100 Gio :

```
docker volume create -d solidfire --name sfBronze -o type=Bronze -o size=100G
```

# Collecte des journaux

Vous pouvez recueillir des journaux pour obtenir de l'aide en matière de dépannage. La méthode que vous utilisez pour collecter les journaux varie en fonction de l'exécution du plug-in Docker.

## Collecte des journaux pour le dépannage

### Étapes

1. Si vous exécutez Astra Trident à l'aide de la méthode de plug-in généré recommandée (à l'aide de `docker plugin` commandes), affichez-les comme suit :

```
docker plugin ls
ID          NAME          DESCRIPTION
ENABLED
4fb97d2b956b    netapp:latest    nDVP - NetApp Docker Volume
Plugin    false
journalctl -u docker | grep 4fb97d2b956b
```

Le niveau d'enregistrement standard devrait vous permettre de diagnostiquer la plupart des problèmes. Si vous trouvez que ce n'est pas suffisant, vous pouvez activer la journalisation de débogage.

2. Pour activer la journalisation de débogage, installez le plug-in avec la journalisation de débogage activée :

```
docker plugin install netapp/trident-plugin:<version> --alias <alias>
debug=true
```

Ou activez la journalisation de débogage lorsque le plug-in est déjà installé :

```
docker plugin disable <plugin>
docker plugin set <plugin> debug=true
docker plugin enable <plugin>
```

3. Si vous exécutez le fichier binaire lui-même sur l'hôte, les journaux sont disponibles dans le répertoire de l'hôte `/var/log/netappdvp`. Pour activer la journalisation de débogage, spécifiez `--debug` lorsque vous exécutez le plug-in.

## Conseils généraux de dépannage

- Le problème le plus courant auquel les nouveaux utilisateurs se sont exécutés est une mauvaise configuration qui empêche le plug-in de s'initialiser. Lorsque cela se produit, vous verrez probablement un message tel que celui-ci lorsque vous essayez d'installer ou d'activer le plug-in :

```
Error response from daemon: dial unix /run/docker/plugins/<id>/netapp.sock:
connect: no such file or directory
```

Cela signifie que le plug-in n'a pas démarré. Heureusement, le plug-in a été conçu avec une fonctionnalité de journalisation complète qui devrait vous aider à diagnostiquer la plupart des problèmes que vous êtes susceptible de venir.

- 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 service `rpcbind` en exécutant un `systemctl status rpcbind` ou son équivalent.

## Gérez plusieurs instances Trident d'Astra

Vous avez besoin de plusieurs instances de Trident lorsque vous souhaitez disposer de plusieurs configurations de stockage simultanément. La clé de plusieurs instances consiste à leur donner différents noms à l'aide de l'`--alias` option avec le plug-in conteneurisé, ou `--volume-driver` de l'option lors de l'instanciation de Trident sur l'hôte.

### Étapes du plug-in géré par Docker (version 1.13/17.03 ou ultérieure)

1. Lancez la première instance en spécifiant un alias et un fichier de configuration.

```
docker plugin install --grant-all-permissions --alias silver
netapp/trident-plugin:21.07 config=silver.json
```

2. Lancez la deuxième instance, en spécifiant un autre alias et un fichier de configuration.

```
docker plugin install --grant-all-permissions --alias gold
netapp/trident-plugin:21.07 config=gold.json
```

3. Créez des volumes spécifiant l'alias comme nom de pilote.

Par exemple, pour le volume Gold :

```
docker volume create -d gold --name ntapGold
```

Par exemple, pour le volume Silver :

```
docker volume create -d silver --name ntapSilver
```

### Étapes pour les versions traditionnelles (version 1.12 ou antérieure)

1. Lancez le plug-in avec une configuration NFS à l'aide d'un ID de pilote personnalisé :

```
sudo trident --volume-driver=netapp-nas --config=/path/to/config  
-nfs.json
```

2. Lancez le plug-in avec une configuration iSCSI à l'aide d'un ID de pilote personnalisé :

```
sudo trident --volume-driver=netapp-san --config=/path/to/config  
-iscsi.json
```

3. Provisionnement de volumes Docker pour chaque instance de pilote :

Par exemple pour NFS :

```
docker volume create -d netapp-nas --name my_nfs_vol
```

Par exemple pour iSCSI :

```
docker volume create -d netapp-san --name my_iscsi_vol
```

## Options de configuration du stockage

Découvrez les options de configuration disponibles pour vos configurations Astra Trident.

### Options de configuration globale

Ces options de configuration s'appliquent à toutes les configurations Astra Trident, quelle que soit la plateforme de stockage utilisée.

Option	Description	Exemple
version	Numéro de version du fichier de configuration	1
storageDriverName	Nom du pilote de stockage	ontap-nas ontap-san, ontap-nas-economy, , , ontap-nas-flexgroup solidfire-san
storagePrefix	Préfixe facultatif pour les noms de volumes. Valeur par défaut : netappdvp_.	staging_

Option	Description	Exemple
limitVolumeSize	Restriction facultative sur les tailles de volume. Par défaut : « » (non appliqué)	10g



N'utilisez pas `storagePrefix` (y compris la valeur par défaut) les systèmes back-end Element. Par défaut, le `solidfire-san` pilote ignore ce paramètre et n'utilise pas de préfixe. Nous vous recommandons d'utiliser un ID de `tentID` spécifique pour le mappage de volume Docker ou les données d'attributs renseignées par la version de Docker, les informations relatives au pilote et le nom brut de Docker dans les cas où il est possible d'utiliser une `mundening` de nom.

Les options par défaut sont disponibles pour éviter d'avoir à les spécifier sur chaque volume que vous créez. L'`'size'` option est disponible pour tous les types de contrôleurs. Pour un exemple de définition de la taille de volume par défaut, reportez-vous à la section ONTAP configuration.

Option	Description	Exemple
size	Taille par défaut facultative pour les nouveaux volumes. Par défaut : 1G	10G

## Configuration DE L'INFRASTRUCTURE ONTAP

Outre les valeurs de configuration globale ci-dessus, lorsque vous utilisez ONTAP, les options de premier niveau suivantes sont disponibles.

Option	Description	Exemple
managementLIF	Adresse IP de la LIF de management ONTAP. Vous pouvez spécifier un nom de domaine complet (FQDN).	10.0.0.1

Option	Description	Exemple
dataLIF	<p>Adresse IP de la LIF de protocole.</p> <p><b>Pilotes NAS ONTAP:</b> Nous vous recommandons de spécifier dataLIF. Si elle n'est pas fournie, Astra Trident extrait les LIF 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.</p> <p><b>Pilotes SAN ONTAP :</b> ne pas spécifier pour iSCSI. ASTRA Trident utilise "<a href="#">Mappage de LUN sélectif ONTAP</a>" pour découvrir les LIF iSCI nécessaires pour établir une session à chemins multiples. Un avertissement est généré si dataLIF est explicitement défini.</p>	10.0.0.2
svm	Storage Virtual machine à utiliser (requis, si la LIF de gestion est une LIF de cluster)	svm_nfs
username	Nom d'utilisateur pour la connexion au périphérique de stockage	vsadmin
password	Mot de passe pour se connecter au périphérique de stockage	secret
aggregate	Agrégat pour le provisionnement (facultatif ; si défini, doit être attribué au SVM) Pour le <code>ontap-nas-flexgroup</code> pilote, cette option est ignorée. Tous les agrégats affectés à un SVM sont utilisés pour provisionner un volume FlexGroup.	aggr1
limitAggregateUsage	Facultatif, le provisionnement échoue si l'utilisation est supérieure à ce pourcentage	75%

Option	Description	Exemple
nfsMountOptions	Contrôle granulaire des options de montage NFS ; par défaut : «-o nfssvers=3 ». <b>Disponible uniquement pour les ontap-nas pilotes et ontap-nas-economy.</b> "Pour plus d'informations sur la configuration de l'hôte NFS, consultez ici".	-o nfsvers=4
igroupName	ASTRA Trident crée et gère par nœud igroups en tant que netappdvp.  Cette valeur ne peut pas être modifiée ou omise.  <b>Disponible uniquement pour le ontap-san pilote.</b>	netappdvp
limitVolumeSize	Taille maximale du volume éligible.	300g
qtreesPerFlexvol	Le nombre maximal de qtrees par FlexVol doit être compris dans la plage [50, 300], la valeur par défaut est 200.  <b>Pour le ontap-nas-economy pilote, cette option permet de personnaliser le nombre maximal de qtrees par FlexVol.</b>	300
sanType	<b>Pris en charge pour le ontap-san pilote uniquement.</b> Utilisez pour sélectionner iscsi pour iSCSI ou nvme pour NVMe/TCP.	iscsi si vide
limitVolumePoolSize	<b>Pris en charge pour ontap-san-economy les ontap-san-economy pilotes et uniquement.</b> Limite la taille des FlexVol pour les modèles économiques ONTAP ONTAP-nas et ONTAP-SAN.	300g

Les options par défaut sont disponibles pour éviter d'avoir à les spécifier sur chaque volume que vous créez :

Option	Description	Exemple
spaceReserve	Mode de réservation d'espace ; none (provisionnement fin) ou volume (lourd)	none

Option	Description	Exemple
snapshotPolicy	Règle Snapshot à utiliser ; la valeur par défaut est <code>none</code>	<code>none</code>
snapshotReserve	Pourcentage de réserve de snapshot. La valeur par défaut est « » pour accepter la valeur par défaut de ONTAP	10
splitOnClone	Séparer un clone de son parent lors de sa création. Par défaut, la valeur est <code>false</code>	<code>false</code>
encryption	<p>Active le chiffrement de volume NetApp (NVE) sur le nouveau volume ; par défaut sur <code>false</code>. Pour utiliser cette option, NVE doit être sous licence et activé sur le cluster.</p> <p>Si NAE est activé sur le back-end, tous les volumes provisionnés dans Astra Trident seront activés par NAE.</p> <p>Pour plus d'informations, reportez-vous à la section : <a href="#">"Fonctionnement d'Astra Trident avec NVE et NAE"</a>.</p>	<code>vrai</code>
unixPermissions	L'option NAS pour les volumes NFS provisionnés est définie par défaut sur <code>777</code>	777
snapshotDir	Option NAS pour l'accès au <code>.snapshot</code> répertoire, par défaut à <code>false</code>	<code>true</code>
exportPolicy	L'option NAS pour la <code>export policy</code> NFS à utiliser est définie par défaut sur <code>default</code>	<code>default</code>
securityStyle	Option NAS pour l'accès au volume NFS provisionné. Prise en charge et <code>unix</code> styles de sécurité par NFS <code>mixed</code> . La valeur par défaut est <code>unix</code> .	<code>unix</code>
fileSystemType	Option SAN pour sélectionner le type de système de fichiers, par défaut sur <code>ext4</code>	<code>xfs</code>
tieringPolicy	Règle de Tiering à utiliser ; la valeur par défaut est <code>none</code> ; <code>snapshot-only</code> pour la configuration SVM-DR antérieure à ONTAP 9.5	<code>none</code>

## Options d'évolutivité

Les `ontap-nas` pilotes et `ontap-san` créent un ONTAP FlexVol pour chaque volume Docker. ONTAP prend en charge jusqu'à 1000 volumes FlexVol par nœud de cluster avec un cluster maximum de 12,000 volumes

FlexVol. Si vos exigences de volume Docker correspondent à cette limitation, le `ontap-nas` pilote est la solution NAS préférée en raison des fonctionnalités supplémentaires proposées par FlexVols, telles que les copies Snapshot granulaires de volume Docker et le clonage.

Si vous avez besoin de plus de volumes Docker que les limites de FlexVol, choisissez le `ontap-nas-economy` ou le `ontap-san-economy` pilote.

Le `ontap-nas-economy` pilote crée des volumes Docker sous forme de qtrees ONTAP au sein d'un pool de volumes FlexVol automatiquement gérés. Les qtrees offrent une évolutivité largement supérieure, jusqu'à 100,000 par nœud de cluster et 2,400,000 par cluster, au détriment de certaines fonctionnalités. Le `ontap-nas-economy` pilote ne prend pas en charge les snapshots granulaires au niveau des volumes Docker ni le clonage.



Le `ontap-nas-economy` pilote n'est pas pris en charge dans Docker Swarm, car Swarm n'orchestre pas la création de volumes sur plusieurs nœuds.

Le `ontap-san-economy` pilote crée des volumes Docker en tant que LUN ONTAP au sein d'un pool partagé de volumes FlexVol automatiquement gérés. De cette façon, chaque FlexVol n'est pas limité à un seul LUN et offre une meilleure évolutivité pour les charges de travail SAN. Selon les baies de stockage, ONTAP prend en charge jusqu'à 16384 LUN par cluster. Comme les volumes sont sous-LUN, ce pilote prend en charge les snapshots et le clonage granulaires par volume Docker.

Choisissez le `ontap-nas-flexgroup` pilote pour augmenter le parallélisme vers un volume unique pouvant atteindre plusieurs pétaoctets avec des milliards de fichiers. Les utilisations idéales de FlexGroups sont l'IA, LE ML, le Big Data et l'analytique, les logiciels, le streaming, les référentiels de fichiers, etc. Trident utilise tous les agrégats attribués à un SVM lors du provisionnement d'un volume FlexGroup. La prise en charge d'FlexGroup dans Trident comporte également plusieurs considérations :

- Requiert ONTAP version 9.2 ou supérieure
- À ce jour, FlexGroups prend uniquement en charge NFS v3.
- Recommandé pour activer les identifiants NFSv3 64 bits pour la SVM.
- La taille minimale recommandée du membre/volume FlexGroup est de 100 Gio.
- Le clonage n'est pas pris en charge pour FlexGroup volumes.

Pour plus d'informations sur les FlexGroups et les charges de travail appropriées pour FlexGroups, reportez-vous au "[NetApp FlexGroup Volume Guide des meilleures pratiques et de mise en œuvre](#)" .

Pour bénéficier de fonctionnalités avancées et d'une grande évolutivité dans un même environnement, vous pouvez exécuter plusieurs instances du plug-in de volume Docker, l'une utilisant et l'autre avec `ontap-nas-economy`.

## Exemples de fichiers de configuration ONTAP

### Exemple NFS pour le pilote `ONTAP`

```
{  
  "version": 1,  
  "storageDriverName": "ontap-nas",  
  "managementLIF": "10.0.0.1",  
  "dataLIF": "10.0.0.2",  
  "svm": "svm_nfs",  
  "username": "vsadmin",  
  "password": "password",  
  "aggregate": "aggr1",  
  "defaults": {  
    "size": "10G",  
    "spaceReserve": "none",  
    "exportPolicy": "default"  
  }  
}
```

### Exemple NFS pour le pilote `ONTAP-nas-FlexGroup`

```
{  
  "version": 1,  
  "storageDriverName": "ontap-nas-flexgroup",  
  "managementLIF": "10.0.0.1",  
  "dataLIF": "10.0.0.2",  
  "svm": "svm_nfs",  
  "username": "vsadmin",  
  "password": "password",  
  "defaults": {  
    "size": "100G",  
    "spaceReserve": "none",  
    "exportPolicy": "default"  
  }  
}
```

### Exemple NFS pour le pilote </code> `ONTAP-nas-economy`

```
{  
  "version": 1,  
  "storageDriverName": "ontap-nas-economy",  
  "managementLIF": "10.0.0.1",  
  "dataLIF": "10.0.0.2",  
  "svm": "svm_nfs",  
  "username": "vsadmin",  
  "password": "password",  
  "aggregate": "aggr1"  
}
```

### Exemple iSCSI pour le pilote </code> `ONTAP- </code>`

```
{  
  "version": 1,  
  "storageDriverName": "ontap-san",  
  "managementLIF": "10.0.0.1",  
  "dataLIF": "10.0.0.3",  
  "svm": "svm_iscsi",  
  "username": "vsadmin",  
  "password": "password",  
  "aggregate": "aggr1",  
  "igroupName": "netappdvp"  
}
```

### Exemple NFS pour le pilote </code> `ONTAP-san-economy`

```
{  
  "version": 1,  
  "storageDriverName": "ontap-san-economy",  
  "managementLIF": "10.0.0.1",  
  "dataLIF": "10.0.0.3",  
  "svm": "svm_iscsi_eco",  
  "username": "vsadmin",  
  "password": "password",  
  "aggregate": "aggr1",  
  "igroupName": "netappdvp"  
}
```

## Exemple NVMe/TCP pour le pilote <code>ONTAP</code>

```
{  
  "version": 1,  
  "backendName": "NVMeBackend",  
  "storageDriverName": "ontap-san",  
  "managementLIF": "10.0.0.1",  
  "svm": "svm_nvme",  
  "username": "vsadmin",  
  "password": "password",  
  "sanType": "nvme",  
  "useREST": true  
}
```

## Configuration logicielle Element

Outre les valeurs de configuration globale, lorsque le logiciel Element (NetApp HCI/SolidFire) est utilisé, ces options sont disponibles.

Option	Description	Exemple
Endpoint	<code>https://&lt;login&gt;:&lt;password&gt;@&lt;mvip&gt;/json-rpc/&lt;element-version&gt;</code>	<code>https://admin:admin@192.168.160.3/json-rpc/8.0</code>
SVIP	Port et adresse IP iSCSI	10.0.0.7:3260
TenantName	Locataire SolidFireF à utiliser (créé s'il n'est pas trouvé)	docker
InitiatorIFace	Spécifiez l'interface lors de la restriction du trafic iSCSI à une interface non-par défaut	default
Types	Spécifications de QoS	Voir l'exemple ci-dessous
LegacyNamePrefix	Préfixe des installations Trident mises à niveau. Si vous avez utilisé une version de Trident antérieure à la version 1.3.2 et effectué une mise à niveau avec des volumes existants, vous devez définir cette valeur pour accéder aux anciens volumes mappés avec la méthode nom-volume.	<code>netappdvp-</code>

Le solidfire-san pilote ne prend pas en charge Docker Swarm.

## Exemple de fichier de configuration du logiciel Element

```
{  
  "version": 1,  
  "storageDriverName": "solidfire-san",  
  "Endpoint": "https://admin:admin@192.168.160.3/json-rpc/8.0",  
  "SVIP": "10.0.0.7:3260",  
  "TenantName": "docker",  
  "InitiatorIFace": "default",  
  "Types": [  
    {  
      "Type": "Bronze",  
      "Qos": {  
        "minIOPS": 1000,  
        "maxIOPS": 2000,  
        "burstIOPS": 4000  
      }  
    },  
    {  
      "Type": "Silver",  
      "Qos": {  
        "minIOPS": 4000,  
        "maxIOPS": 6000,  
        "burstIOPS": 8000  
      }  
    },  
    {  
      "Type": "Gold",  
      "Qos": {  
        "minIOPS": 6000,  
        "maxIOPS": 8000,  
        "burstIOPS": 10000  
      }  
    }  
  ]  
}
```

## Problèmes et limites connus

Découvrez des informations sur les problèmes et les limites connus avec Astra Trident avec Docker.

**La mise à niveau de Trident Docker Volume Plug-in vers la version 20.10 et ultérieure à partir des versions plus anciennes entraîne un échec de mise à niveau, sans erreur de fichier ou de répertoire de ce type.**

#### Solution de contournement

1. Désactivez le plug-in.

```
docker plugin disable -f netapp:latest
```

2. Retirez le plug-in.

```
docker plugin rm -f netapp:latest
```

3. Réinstallez le plug-in en fournissant le paramètre supplémentaire config.

```
docker plugin install netapp/trident-plugin:20.10 --alias netapp --grant -all-permissions config=config.json
```

#### Les noms de volumes doivent comporter au moins 2 caractères.



Il s'agit d'une limitation client Docker. Le client interprète un nom de caractère unique comme étant un chemin Windows. ["Voir bug 25773"](#).

**Docker Swarm dispose de certains comportements qui empêchent Astra Trident de les prendre en charge avec chaque combinaison de stockage et de pilote.**

- Docker Swarm utilise actuellement le nom du volume, mais pas l'ID de volume, comme identifiant de volume unique.
- Les requêtes de volume sont envoyées simultanément à chaque noeud d'un cluster Swarm.
- Les plug-ins de volumes (y compris Astra Trident) doivent être exécutés de manière indépendante sur chaque noeud d'un cluster Swarm. En raison du fonctionnement de ONTAP et du ontap-nas fonctionnement des pilotes et ontap-san, ce sont eux qui sont les seuls à pouvoir fonctionner dans ces limites.

Les autres conducteurs sont sujets à des problèmes tels que les conditions de course qui peuvent entraîner la création d'un grand nombre de volumes pour une seule demande sans un « gagnant » clair ; par exemple, l'élément possède une fonctionnalité qui permet aux volumes d'avoir le même nom mais des ID différents.

NetApp a fourni des commentaires à l'équipe Docker, mais ne fournit aucune indication de recours futur.

**Si un FlexGroup est provisionné, ONTAP ne provisionne pas un deuxième FlexGroup si le deuxième FlexGroup dispose d'un ou de plusieurs agrégats en commun avec la FlexGroup provisionnée.**

# Meilleures pratiques et recommandations

## Déploiement

Utilisez les recommandations indiquées ici pour déployer Astra Trident.

### Déploiement dans un namespace dédié

"[Espaces de noms](#)" séparation administrative entre les différentes applications et obstacle au partage des ressources. Par exemple, un volume persistant ne peut pas être consommé depuis un autre espace de noms. Astra Trident fournit des ressources PV à tous les namespaces du cluster Kubernetes et exploite par conséquent un compte de service avec des priviléges élevés.

L'accès au pod Trident peut également permettre à un utilisateur d'accéder aux identifiants du système de stockage et à d'autres informations sensibles. Il est important de s'assurer que les utilisateurs d'applications et les applications de gestion ne peuvent pas accéder aux définitions d'objets Trident ou aux pods eux-mêmes.

### Utilisez les quotas et les limites des plages pour contrôler la consommation du stockage

Kubernetes dispose de deux fonctionnalités qui, lorsqu'elles sont combinées, fournissent un mécanisme puissant pour limiter la consommation des ressources par les applications. "[mécanisme de quotas de stockage](#)" Permet à l'administrateur de mettre en œuvre des limites de consommation de capacité et de nombre d'objets globales et spécifiques à chaque classe de stockage, par espace de noms. En outre, l'utilisation d'un "[limite de plage](#)" garantit que les demandes de volume persistant sont à la fois dans les limites minimum et maximum avant que la demande ne soit transmise au provisionneur.

Ces valeurs sont définies par espace de noms, ce qui signifie que chaque espace de noms doit avoir des valeurs définies qui correspondent à leurs besoins en ressources. Voir ici pour plus d'informations sur "[comment exploiter les quotas](#)".

## Configuration de stockage sous-jacente

Chaque plateforme de stockage du portefeuille NetApp dispose de fonctionnalités uniques qui bénéficient aux applications, conteneurisées ou non.

### Présentation de la plateforme

Trident fonctionne avec ONTAP et Element. Il n'existe pas de plate-forme mieux adaptée à toutes les applications et tous les scénarios qu'une autre. Cependant, les besoins de l'application et l'équipe chargée de l'administration du périphérique doivent être pris en compte lors du choix d'une plate-forme.

Vous devez suivre les meilleures pratiques de base du système d'exploitation hôte avec le protocole utilisé. Vous pouvez éventuellement envisager d'intégrer les meilleures pratiques des applications, le cas échéant, avec des paramètres de back-end, de classe de stockage et de volume persistant afin d'optimiser le stockage pour certaines applications.

### Meilleures pratiques pour ONTAP et Cloud Volumes ONTAP

Découvrez les bonnes pratiques pour la configuration d'ONTAP et de Cloud Volumes ONTAP pour Trident.

Les recommandations suivantes sont des instructions de configuration de ONTAP pour les workloads conteneurisés, qui consomment des volumes provisionnés dynamiquement par Trident. Chaque élément doit être pris en compte et évalué en fonction de la pertinence dans votre environnement.

## Utilisation de SVM(s) dédié(s) à Trident

Les machines virtuelles de stockage (SVM) assurent l'isolation et la séparation administrative entre les locataires sur un système ONTAP. La dédier un SVM aux applications permet de déléguer des priviléges et d'appliquer les meilleures pratiques en matière de limitation de la consommation des ressources.

Plusieurs options sont disponibles pour la gestion de la SVM :

- Fournir l'interface de gestion du cluster en configuration back-end avec les identifiants appropriés et spécifier le nom du SVM
- Créer une interface de gestion dédiée pour le SVM via ONTAP System Manager ou l'interface de ligne de commande.
- Partage du rôle de gestion avec une interface de données NFS

Dans chaque cas, l'interface doit être dans DNS et le nom DNS doit être utilisé lors de la configuration de Trident. Ainsi, certaines scénarios de reprise après incident, par exemple SVM-DR, sans conservation des identités de réseau.

Il n'existe aucune préférence entre une LIF de gestion dédiée ou partagée pour le SVM, cependant, vous devez vous assurer que vos stratégies de sécurité réseau sont en adéquation avec l'approche de votre choix. Quoi qu'il en soit, la LIF de gestion doit être accessible via DNS afin de faciliter une flexibilité maximale doit "[SVM-DR](#)" être utilisée conjointement avec Trident.

## Limitez le nombre maximal de volumes

Les systèmes de stockage ONTAP disposent d'un nombre maximal de volumes, qui varie selon la version logicielle et la plateforme matérielle. Reportez-vous "[NetApp Hardware Universe](#)" à la pour connaître votre plate-forme spécifique et la version de ONTAP pour déterminer les limites exactes. Lorsque le nombre de volumes est épuisé, les opérations de provisionnement échouent non seulement pour Trident, mais pour l'ensemble des requêtes de stockage.

Les Trident `ontap-nas` et leurs `ontap-san` pilotes provisionnent un FlexVolume pour chaque volume persistant Kubernetes créé. Le `ontap-nas-economy` pilote crée environ un FlexVolume pour 200 PVS (configurable entre 50 et 300). Le `ontap-san-economy` pilote crée environ un FlexVolume pour 100 PVS (configurable entre 50 et 200). Pour empêcher Trident de consommer tous les volumes disponibles sur le système de stockage, vous devez définir une limite sur la SVM. Vous pouvez le faire à partir de la ligne de commande :

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

La valeur de varie en fonction de `max-volumes` plusieurs critères spécifiques à votre environnement :

- Le nombre de volumes existants dans le cluster ONTAP
- Le nombre de volumes que vous prévoyez de provisionner en dehors de Trident pour d'autres applications
- Nombre de volumes persistants que les applications Kubernetes devraient consommer

`max-volumes` La valeur correspond au total des volumes provisionnés sur tous les nœuds du cluster ONTAP et non sur un nœud ONTAP individuel. Par conséquent, vous pouvez rencontrer des situations où un nœud de cluster ONTAP peut avoir plus ou moins de volumes provisionnés Trident qu'un autre nœud.

Par exemple, un cluster ONTAP à deux nœuds peut héberger un maximum de 2000 volumes flexibles. Avoir le volume maximum réglé sur 1250 semble très raisonnable. Toutefois, si seul un nœud est attribué au SVM ou si "64 bits" les agrégats attribués à partir d'un nœud ne peuvent pas être provisionnés sur (par exemple, en raison de la capacité), l'autre nœud devient la cible de tous les volumes provisionnés Trident. Cela signifie que la limite de volume peut être atteinte pour ce nœud avant que la valeur ne max-volumes soit atteinte, ce qui a un impact sur les opérations de volume Trident et autres qui utilisent ce nœud. **Vous pouvez éviter cette situation en vous assurant que les agrégats de chaque nœud du cluster sont attribués à la SVM utilisée par Trident en chiffres égaux.**

### **Limitez la taille maximale des volumes créés par Trident**

Pour configurer la taille maximale des volumes pouvant être créés par Trident, utilisez le `limitVolumeSize` paramètre de votre `backend.json` définition.

Vous devez aussi exploiter les fonctionnalités Kubernetes pour contrôler la taille du volume au niveau de la baie de stockage.

### **Limitez la taille maximale des volumes FlexVol créés par Trident**

Pour configurer la taille maximale des volumes FlexVol utilisés comme pools pour les pilotes ONTAP-san-Economy et ONTAP-nas-Economy, utilisez le `limitVolumePoolSize` paramètre dans votre `backend.json` définition.

### **Configurez Trident pour utiliser le protocole CHAP bidirectionnel**

Vous pouvez spécifier l'initiateur CHAP et les noms d'utilisateur et mots de passe cibles dans votre définition du système back-end et activer Trident sur la SVM. En utilisant `useCHAP` le paramètre de votre configuration back-end, Trident authentifie les connexions iSCSI pour les systèmes back-end ONTAP avec le protocole CHAP.

### **Création et utilisation d'une politique de QoS de SVM**

L'utilisation d'une politique de QoS de ONTAP appliquée au SVM limite le nombre de consommables d'IOPS par les volumes provisionnés par Trident. Cela permet à "évitez un tyran" ou à un conteneur hors contrôle d'affecter les charges de travail en dehors de la SVM Trident.

Vous pouvez créer une politique de QoS pour la SVM en quelques étapes. Consultez la documentation de votre version de ONTAP pour obtenir des informations précises. L'exemple ci-dessous crée une politique de QoS qui limite le nombre total d'IOPS disponibles pour la SVM à 5000.

```

# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>

```

Si votre version d'ONTAP la prend en charge, il est également possible d'utiliser un minimum de QoS pour garantir un débit minimum pour les workloads conteneurisés. La QoS adaptative n'est pas compatible avec une règle de niveau SVM.

Le nombre d'IOPS dédiées aux workloads conteneurisés dépend de plusieurs aspects. Entre autres choses :

- Autres charges de travail qui utilisent la baie de stockage. Si certaines charges de travail, autres que celles liées au déploiement Kubernetes avec les ressources de stockage, veillez à ne pas affecter accidentellement ces charges de travail.
- Workloads attendus s'exécutant dans des conteneurs. Si des charges de travail qui exigent des IOPS élevées s'exécutent dans des conteneurs, une faible politique de QoS entraîne une mauvaise expérience.

Il est important de rappeler qu'une politique de QoS attribuée au niveau du SVM entraîne tous les volumes provisionnés sur la SVM et partageant le même pool d'IOPS. Si l'une des applications conteneurisées a une exigence d'IOPS élevées, elle pourrait devenir une force dominante pour les autres workloads conteneurisés. Dans ce cas, vous pourriez envisager d'utiliser l'automatisation externe pour attribuer des règles de QoS par volume.



Vous devez affecter la « policy group » QoS à la SVM **Only** si la version de votre ONTAP est antérieure à 9.8.

## Création de groupes de règles de QoS pour Trident

La qualité de service (QoS) garantit que les performances des workloads stratégiques ne sont pas dégradées par des charges de travail concurrentes. Les groupes de règles de QoS de ONTAP proposent des options de QoS pour les volumes et permettent aux utilisateurs de définir le plafond de débit pour une ou plusieurs charges de travail. Pour plus d'informations sur QoS, reportez-vous à ["Débit garanti avec la QoS"](#). Vous pouvez spécifier des groupes de règles de QoS dans le back-end ou dans un pool de stockage, et ils sont appliqués à chaque volume créé dans ce pool ou back-end.

ONTAP propose deux types de groupes de règles de QoS : classiques et évolutifs. Les groupes de règles classiques fournissent un débit minimal (ou minimal, dans les versions ultérieures) plat en IOPS. La QoS adaptative ajuste automatiquement le débit en fonction de la taille du workload. Elle maintient le rapport entre les IOPS et les To|Go en fonction de l'évolution de la taille du workload. Vous pouvez ainsi gérer des centaines, voire des milliers de charges de travail dans le cadre d'un déploiement à grande échelle.

Avant de créer des groupes de règles de QoS, tenez compte des points suivants :

- Vous devez définir la `qosPolicy` clé dans le `defaults` bloc de la configuration back-end. Voir l'exemple de configuration back-end suivant :

```

---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
storage:
- labels:
  performance: extreme
  defaults:
    adaptiveQosPolicy: extremely-adaptive-pg
- labels:
  performance: premium
  defaults:
    qosPolicy: premium-pg

```

- Vous devez appliquer les « policy groups » par volume pour que chaque volume bénéficie de l'intégralité du débit spécifié par le « policy group ». Les groupes de stratégies partagés ne sont pas pris en charge.

Pour plus d'informations sur les groupes de règles QoS, reportez-vous ["Commandes QoS de ONTAP 9.8"](#) à la section .

### Limitez l'accès aux ressources de stockage aux membres du cluster Kubernetes

La limitation de l'accès aux volumes NFS et aux LUN iSCSI créés par Trident est un composant stratégique du niveau de sécurité pour votre déploiement Kubernetes. En effet, les hôtes qui ne font pas partie du cluster Kubernetes n'accèdent pas aux volumes et peuvent modifier les données de façon inattendue.

Il est important de comprendre que les espaces de noms sont la limite logique des ressources dans Kubernetes. L'hypothèse est que les ressources dans un même espace de noms peuvent être partagées, mais, surtout, il n'existe aucune fonctionnalité de multi-espace de noms. Même si les volumes persistants sont des objets globaux, lorsqu'ils sont liés à une demande de volume persistant, ils ne sont accessibles que par des pods qui se trouvent dans le même espace de noms. **Il est essentiel de s'assurer que les espaces de noms sont utilisés pour fournir la séparation, le cas échéant.**

La préoccupation principale de la plupart des entreprises en ce qui concerne la sécurité des données dans un contexte Kubernetes est qu'un processus dans un conteneur peut accéder au stockage monté sur l'hôte, mais qui n'est pas destiné au conteneur. ["Espaces de noms"](#) sont conçus pour empêcher ce type de compromis. Toutefois, il y a une exception : les conteneurs privilégiés.

Un conteneur privilégié est un conteneur exécuté avec beaucoup plus d'autorisations au niveau de l'hôte que la normale. Ils ne sont pas refusés par défaut. Assurez-vous donc de désactiver cette fonctionnalité à l'aide de ["stratégies de sécurité des pods"](#).

Pour les volumes pour lesquels l'accès est demandé depuis Kubernetes et des hôtes externes, le stockage doit être géré de manière classique, avec le volume persistant introduit par l'administrateur et non géré par

Trident. Cela garantit que le volume de stockage est détruit uniquement lorsque les hôtes Kubernetes et externes sont déconnectés et qu'ils n'utilisent plus le volume. En outre, il est possible d'appliquer une export policy personnalisée qui permet l'accès depuis les nœuds de cluster Kubernetes et les serveurs ciblés à l'extérieur du cluster Kubernetes.

Pour les déploiements avec des nœuds d'infrastructure dédiés (par exemple OpenShift) ou d'autres nœuds ne pouvant pas planifier les applications utilisateur, des règles d'exportation distinctes doivent être utilisées pour limiter davantage l'accès aux ressources de stockage. Cela inclut la création d'une export policy pour les services qui sont déployés sur ces nœuds d'infrastructure (par exemple les services OpenShift Metrics et Logging Services), ainsi que pour les applications standard déployées sur des nœuds non liés à l'infrastructure.

## Utiliser une export policy dédiée

Vous devez vous assurer qu'il existe une export policy pour chaque backend qui autorise uniquement l'accès aux nœuds présents dans le cluster Kubernetes. Trident peut créer et gérer automatiquement des règles d'export. Trident limite ainsi l'accès aux volumes qu'il provisionne aux nœuds du cluster Kubernetes et simplifie l'ajout et la suppression des nœuds.

Vous pouvez également créer une export policy manuellement et la remplir à l'aide d'une ou plusieurs règles d'exportation qui traitent chaque demande d'accès de nœud :

- Utiliser `vserver export-policy create` la commande de l'interface de ligne de commandes ONTAP pour créer les export policy.
- Ajoutez des règles à la export policy à l'aide de la `vserver export-policy rule create` commande de l'interface de ligne de commandes ONTAP.

L'exécution de ces commandes vous permet de limiter l'accès aux données aux nœuds Kubernetes.

## Désactivez showmount pour le SVM d'application

La showmount fonctionnalité permet à un client NFS d'interroger le SVM sur la liste des exports NFS disponibles. Un pod déployé dans le cluster Kubernetes peut émettre la `showmount -e` commande contre la LIF de données et recevoir une liste des montages disponibles, y compris ceux auxquels il n'a pas accès. Bien qu'il ne s'agisse pas d'un compromis sur la sécurité, cette solution fournit des informations inutiles susceptibles d'aider un utilisateur non autorisé à se connecter à une exportation NFS.

Pour la désactiver showmount, utiliser la commande CLI ONTAP au niveau du SVM :

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

## Les meilleures pratiques pour SolidFire

Découvrez les bonnes pratiques pour la configuration du stockage SolidFire pour Trident.

### Créer un compte SolidFire

Chaque compte SolidFire représente un propriétaire de volume unique et reçoit ses propres informations d'identification CHAP (Challenge-Handshake Authentication Protocol). Vous pouvez accéder aux volumes affectés à un compte en utilisant le nom du compte et les informations d'identification CHAP relatives ou par le biais d'un groupe d'accès de volume. Un compte peut comporter jusqu'à deux milliers de volumes qui lui sont attribués, mais un volume ne peut appartenir qu'à un seul compte.

## Création d'une règle de QoS

Utilisez les règles de QoS SolidFire pour créer et enregistrer des paramètres de qualité de service standardisés qui peuvent être appliqués à de nombreux volumes.

Vous pouvez définir des paramètres de QoS par volume. Les performances de chaque volume peuvent être garanties en définissant trois paramètres configurables pour définir les QoS : IOPS min, IOPS max et IOPS en rafale.

Voici les valeurs d'IOPS minimales, maximales et en rafale possibles pour la taille de bloc de 4 Ko.

Paramètre IOPS	Définition	Valeur min	Valeur par défaut	Valeur max. (4 Ko)
IOPS min	Niveau de performance garanti pour un volume.	50	50	15000
IOPS max	La performance ne dépassera pas cette limite.	50	15000	200 000
IOPS en rafale	IOPS maximales autorisées en rafale,	50	15000	200 000



Même si les IOPS maximales et en rafale peuvent être définies jusqu'à 200,000, les performances maximales réelles d'un volume sont limitées par l'utilisation du cluster et les performances par noeud.

La taille et la bande passante des blocs influencent directement le nombre d'opérations d'entrée/sortie par seconde. Lorsque la taille de bloc augmente, le système augmente la bande passante jusqu'au niveau nécessaire pour traiter les tailles de bloc de taille supérieure. Lorsque la bande passante augmente, le nombre d'IOPS augmente, le système peut atteindre une baisse. Pour plus d'informations sur la qualité de service et les performances, reportez-vous à la section "["Qualité de service SolidFire"](#)".

## Authentification SolidFire

Element prend en charge deux méthodes d'authentification : CHAP et VAG (Volume Access Groups). CHAP utilise le protocole CHAP pour authentifier l'hôte au back-end. Les groupes d'accès de volume contrôlent l'accès aux volumes qu'ils provisionne. NetApp recommande d'utiliser le protocole CHAP pour l'authentification, car il est plus simple et ne comporte pas de limites d'évolutivité.



Trident avec le mécanisme de provisionnement CSI amélioré prend en charge l'authentification CHAP. Les VAGs ne doivent être utilisés que dans le mode de fonctionnement traditionnel non CSI.

L'authentification CHAP (vérification que l'initiateur est l'utilisateur de volume prévu) n'est prise en charge qu'avec un contrôle d'accès basé sur le compte. Si vous utilisez CHAP pour l'authentification, deux options sont disponibles : CHAP unidirectionnel et CHAP bidirectionnel. L'authentification CHAP unidirectionnelle authentifie l'accès au volume à l'aide du nom du compte SolidFire et du secret de l'initiateur. L'option CHAP bidirectionnelle fournit le moyen le plus sûr d'authentifier le volume car le volume authentifie l'hôte via le nom du compte et le secret de l'initiateur, puis l'hôte authentifie le volume via le nom du compte et le secret cible.

Toutefois, si CHAP ne peut pas être activé et que VAGs sont requis, créez le groupe d'accès et ajoutez les initiateurs hôtes et les volumes au groupe d'accès. Chaque IQN que vous ajoutez à un groupe d'accès peut accéder à chaque volume du groupe avec ou sans authentification CHAP. Si l'initiateur iSCSI est configuré pour utiliser l'authentification CHAP, un contrôle d'accès basé sur les comptes est utilisé. Si l'initiateur iSCSI n'est pas configuré pour utiliser l'authentification CHAP, le contrôle d'accès au groupe d'accès de volume est utilisé.

## Où trouver plus d'informations ?

Une partie de la documentation sur les meilleures pratiques est présentée ci-dessous. Recherchez les versions les plus récentes dans le ["Bibliothèque NetApp"](#).

### ONTAP

- ["Guide des meilleures pratiques et de mise en œuvre de NFS"](#)
- ["Guide d'administration SAN"](#) (Pour iSCSI)
- ["Configuration iSCSI Express pour RHEL"](#)

### Logiciel Element

- ["Configuration de SolidFire pour Linux"](#)

### NetApp HCI

- ["Conditions préalables au déploiement de NetApp HCI"](#)
- ["Accès au moteur de déploiement NetApp"](#)

### Information sur les pratiques exemplaires des applications

- ["Bonnes pratiques pour MySQL sur ONTAP"](#)
- ["Bonnes pratiques pour MySQL sur SolidFire"](#)
- ["NetApp SolidFire et Cassandra"](#)
- ["Meilleures pratiques pour Oracle sur SolidFire"](#)
- ["Meilleures pratiques PostgreSQL sur SolidFire"](#)

Toutes les applications ne disposent pas de directives spécifiques, il est important de travailler avec votre équipe NetApp et d'utiliser le ["Bibliothèque NetApp"](#) pour trouver la documentation la plus récente.

## Intégrez Astra Trident

Pour intégrer Astra Trident, les éléments de conception et d'architecture suivants nécessitent l'intégration : sélection des pilotes et déploiement, conception de la classe de stockage, conception de pool virtuel, impact de la demande de volume persistant sur le provisionnement du stockage, les opérations des volumes et le déploiement de services OpenShift avec Astra Trident.

## Choix et déploiement du conducteur

Sélectionnez et déployez un pilote backend pour votre système de stockage.

## Pilotes ONTAP backend

Les pilotes back-end ONTAP sont différenciés par le protocole utilisé et le mode de provisionnement des volumes sur le système de stockage. Par conséquent, réfléchissez bien au choix du conducteur à déployer.

À un niveau plus élevé, si votre application dispose de composants qui nécessitent un stockage partagé (plusieurs modules accédant au même volume de demande de volume persistant), les pilotes NAS seraient la solution par défaut, tandis que les pilotes iSCSI basés sur les blocs répondent aux besoins d'un stockage non partagé. Choisir le protocole en fonction des besoins de l'application et du niveau de confort des équipes chargées du stockage et de l'infrastructure. En règle générale, ces différences sont peu nombreuses pour la plupart des applications. La décision dépend donc souvent de la nécessité d'un stockage partagé (dans lequel plusieurs pods auront besoin d'un accès simultané).

Les pilotes ONTAP backend disponibles sont les suivants :

- `ontap-nas`: Chaque volume persistant provisionné est un volume flexible ONTAP complet.
- `ontap-nas-economy`: Chaque volume persistant provisionné est un qtree, avec un nombre configurable de qtree par FlexVolume (la valeur par défaut est 200).
- `ontap-nas-flexgroup`: Chaque volume persistant provisionné en tant que ONTAP FlexGroup complet, et tous les agrégats affectés à un SVM sont utilisés.
- `ontap-san`: Chaque volume persistant provisionné est une LUN au sein de son propre volume FlexVolume.
- `ontap-san-economy`: Chaque PV provisionné est une LUN, avec un nombre configurable de LUN par FlexVolume (la valeur par défaut est 100).

Le choix entre les trois pilotes NAS a des ramifications sur les fonctionnalités mises à disposition de l'application.

Il est à noter que dans les tableaux ci-dessous, toutes les fonctionnalités ne sont pas exposées par Astra Trident. L'administrateur du stockage doit appliquer une partie après le provisionnement si cette fonctionnalité est souhaitée. Les notes de bas de page en exposant distinguent les fonctionnalités par fonction et pilote.

Pilotes NAS de ONTAP	Snapshot s	Clones	Règles d'exportation dynamiques	Multi-attacher	La QoS	Redimensionner	La réplication
<code>ontap-nas</code>	Oui	Oui	Note de bas de page : 5[]	Oui	Note de bas de page : 1[]	Oui	Note de bas de page : 1[]
<code>ontap-nas-economy</code>	Note de bas de page : 3[]	Note de bas de page : 3[]	Note de bas de page : 5[]	Oui	Note de bas de page : 3[]	Oui	Note de bas de page : 3[]
<code>ontap-nas-flexgroup</code>	Note de bas de page : 1[]	Non	Note de bas de page : 5[]	Oui	Note de bas de page : 1[]	Oui	Note de bas de page : 1[]

Astra Trident propose 2 pilotes SAN pour ONTAP dont les fonctionnalités sont présentées ci-dessous.

Pilotes SAN de ONTAP	Snapshot s	Clones	Multi-attacher	Chap bi-directionnel	La QoS	Redimensionner	La réplication
ontap-san	Oui	Oui	Note de bas de page : 4[]	Oui	Note de bas de page : 1[]	Oui	Note de bas de page : 1[]
ontap-san-economy	Oui	Oui	Note de bas de page : 4[]	Oui	Note de bas de page : 3[]	Oui	Note de bas de page : 3[]

Note de bas de page pour les tableaux ci-dessus : Yes [1]: Non géré par Astra Trident Yes [2]: Géré par Astra Trident, mais non par PV granulaire Yes [3]: Non géré par Astra Trident et non par PV granulaire Yes [4]: Pris en charge pour les volumes de bloc brut Yesnote:5[]: Pris en charge par Astra Trident

Les fonctionnalités qui ne sont pas granulaires volume persistant sont appliquées à l'ensemble du volume flexible et tous les volumes persistants (qtrees ou LUN inclus dans les volumes FlexVol partagés) partageront une planification commune.

Comme nous le voyons dans les tableaux ci-dessus, la plupart des fonctionnalités entre ontap-nas et ontap-nas-economy sont identiques. Toutefois, comme ontap-nas-economy le pilote limite la capacité à contrôler la planification au niveau de la granularité par volume persistant, cela peut avoir un impact particulier sur la planification de la reprise d'activité et de la sauvegarde. Pour les équipes de développement qui souhaitent exploiter la fonctionnalité de clonage PVC sur le stockage ONTAP, cette fonctionnalité n'est possible que lorsque des pilotes , ontap-san ou ontap-san-economy sont utilisés ontap-nas.



Le solidfire-san pilote peut également cloner des ESV.

## Pilotes Cloud Volumes ONTAP backend

Cloud Volumes ONTAP assure le contrôle des données et des fonctionnalités de stockage haute performance dans divers cas d'utilisation, notamment pour les partages de fichiers et le stockage de niveau bloc qui servent les protocoles NAS et SAN (NFS, SMB/CIFS et iSCSI). Les pilotes compatibles avec Cloud Volume ONTAP sont ontap-nas, ontap-nas-economy ontap-san et ontap-san-economy. Applicable à Cloud Volume ONTAP pour Azure, Cloud Volume ONTAP pour GCP.

## Pilotes backend Amazon FSX pour ONTAP

Avec Amazon FSX pour NetApp ONTAP, vous exploitez les fonctionnalités, les performances et les capacités d'administration d'NetApp que vous connaissez déjà, tout en profitant de la simplicité, de l'agilité, de la sécurité et de l'évolutivité du stockage des données sur AWS. FSX pour ONTAP prend en charge de nombreuses fonctionnalités de système de fichiers ONTAP et API d'administration. Les pilotes compatibles avec Cloud Volume ONTAP sont ontap-nas, , ontap-nas-economy ontap-nas-flexgroup ontap-san et ontap-san-economy.

## Pilotes back-end NetApp HCI/SolidFire

Le solidfire-san pilote utilisé avec les plateformes NetApp HCI/SolidFire permet à l'administrateur de configurer un back-end Element pour Trident en fonction des limites de QoS. Si vous souhaitez concevoir votre back-end de façon à définir les limites de QoS spécifiques sur les volumes provisionnés par Trident, utilisez le

type paramètre dans le fichier back-end. L'administrateur peut également limiter la taille du volume qui pourrait être créé sur le stockage à l'aide du `limitVolumeSize` paramètre. Actuellement, les fonctionnalités de stockage Element comme le redimensionnement de volume et la réPLICATION de volume ne sont pas prises en charge par le `solidfire-san` pilote. Ces opérations doivent être effectuées manuellement via l'interface utilisateur Web du logiciel Element.

Pilote SolidFire	Snapshot s	Clones	Multi-attacher	CHAP	La QoS	Redimensionner	La réPLICATION
<code>solidfire-san</code>	Oui	Oui	Note de bas de page : 2[]	Oui	Oui	Oui	Note de bas de page : 1[]

Note de bas de page: Yes [1]: Non géré par Astra Trident Yes [2]: Pris en charge pour les volumes en blocs bruts

### Pilotes Azure NetApp Files backend

ASTRA Trident utilise le `azure-netapp-files` pilote pour gérer le "[Azure NetApp Files](#)" service.

Pour plus d'informations sur ce pilote et sur sa configuration "[Configuration back-end d'Astra Trident pour Azure NetApp Files](#)", reportez-vous à la section .

Pilote Azure NetApp Files	Snapshots	Clones	Multi-attacher	La QoS	Développement	La réPLICATION
<code>azure-netapp-files</code>	Oui	Oui	Oui	Oui	Oui	Note de bas de page : 1[]

Note de bas de page: Yes [1]: Non géré par Astra Trident

### Cloud Volumes Service sur le pilote back-end Google Cloud

ASTRA Trident utilise `gcp-cvs` le pilote pour établir un lien avec Cloud Volumes Service sur Google Cloud.

Le `gcp-cvs` pilote utilise des pools virtuels pour extraire le back-end et permettre à Astra Trident de déterminer le placement des volumes. L'administrateur définit les pools virtuels dans les `backend.json` fichiers. Les classes de stockage utilisent des sélecteurs pour identifier les pools virtuels par étiquette.

- Si des pools virtuels sont définis au niveau du système back-end, Astra Trident essaie de créer un volume dans les pools de stockage Google Cloud auxquels ces pools virtuels sont limités.
- Si des pools virtuels ne sont pas définis dans le système back-end, Astra Trident sélectionne un pool de stockage Google Cloud à partir des pools de stockage disponibles dans la région.

Pour configurer le back-end Google Cloud sur Astra Trident, vous devez spécifier `projectNumber`, `apiRegion` et `apiKey` dans le fichier back-end. Le numéro de projet est indiqué dans la console Google Cloud. La clé API est utilisée depuis le fichier de clé privée du compte de service que vous avez créé lors de la configuration de l'accès API pour Cloud Volumes Service sur Google Cloud.

Pour plus d'informations sur Cloud Volumes Service sur les types de services et les niveaux de service Google Cloud, reportez-vous à "[En savoir plus sur la prise en charge d'Astra Trident pour CVS pour GCP](#)" la section .

Pilote Cloud Volumes Service pour Google Cloud	Snapshots	Clones	Multi-attacher	La QoS	Développement	La réplication
gcp-cvs	Oui	Oui	Oui	Oui	Oui	Disponible uniquement sur le type de service CVS-Performance.

#### Notes de réplication



- La réplication n'est pas gérée par Astra Trident.
- Le clone sera créé dans le même pool de stockage que le volume source.

## Conception de classe de stockage

Chaque classe de stockage doit être configurée et appliquée pour créer un objet de classe de stockage Kubernetes. Cette section décrit comment concevoir un système de stockage pour votre application.

### Utilisation du système back-end spécifique

Le filtrage peut être utilisé au sein d'un objet de classe de stockage spécifique pour déterminer le pool de stockage ou l'ensemble de pools à utiliser avec cette classe de stockage spécifique. Trois jeux de filtres peuvent être définis dans la classe de stockage : `storagePools`, `additionalStoragePools` et/ou `excludeStoragePools`.

Le `storagePools` paramètre permet de limiter le stockage à l'ensemble de pools correspondant à n'importe quel attribut spécifié. Le `additionalStoragePools` paramètre est utilisé pour étendre l'ensemble de pools qu'Astra Trident utilisera pour le provisionnement, ainsi que l'ensemble de pools sélectionné par les attributs et les `storagePools` paramètres. Vous pouvez utiliser l'un ou l'autre paramètre seul ou les deux ensemble pour vous assurer que l'ensemble approprié de pools de stockage est sélectionné.

Le `excludeStoragePools` paramètre est utilisé pour exclure spécifiquement l'ensemble de pools répertoriés qui correspondent aux attributs.

### Émuler les règles de QoS

Si vous souhaitez concevoir des classes de stockage pour émuler des stratégies de qualité de service, créez une classe de stockage avec `media` l'attribut comme `hdd` ou `ssd`. En fonction de l' `media`` attribut mentionné dans la classe de stockage, Trident sélectionne le back-end approprié qui sert `hdd` ou `ssd` regroupe les agrégats pour correspondre à l'attribut de support, puis dirige le provisionnement des volumes vers l'agrégat spécifique. Nous pouvons donc créer une PRIME DE classe de stockage dont l'attribut aurait `media` été défini et `ssd` qui pourrait être classé comme la politique de QoS PREMIUM. Nous pouvons créer une autre NORME de classe de stockage dont l'attribut de support est défini comme `'hdd'`, qui pourrait être classé comme règle de QoS STANDARD. Nous pourrions également utiliser l'attribut « IOPS » de la classe de stockage pour rediriger le provisionnement vers une appliance Element qui peut être définie comme une règle de QoS.

## Utilisation du système back-end en fonction de fonctionnalités spécifiques

Les classes de stockage peuvent être conçues pour diriger le provisionnement des volumes sur un système back-end spécifique, où des fonctionnalités telles que le provisionnement fin et lourd, les copies Snapshot, les clones et le chiffrement sont activées. Pour spécifier le stockage à utiliser, créez des classes de stockage qui spécifient le back-end approprié avec la fonction requise activée.

### Pools virtuels

Des pools virtuels sont disponibles pour tous les systèmes back-end Astra Trident. Vous pouvez définir des pools virtuels pour tout système back-end, à l'aide de n'importe quel pilote fourni par Astra Trident.

Les pools virtuels permettent à un administrateur de créer un niveau d'abstraction sur les systèmes back-end, qui peut être référencé via des classes de stockage, pour une plus grande flexibilité et un placement efficace des volumes dans les systèmes back-end. Différents systèmes back-end peuvent être définis avec la même classe de service. En outre, il est possible de créer plusieurs pools de stockage sur le même back-end, mais avec des caractéristiques différentes. Lorsqu'une classe de stockage est configurée avec un sélecteur portant les étiquettes spécifiques, Astra Trident choisit un système back-end correspondant à toutes les étiquettes de sélection pour placer le volume. Si les étiquettes de sélection de classe de stockage correspondent à plusieurs pools de stockage, Astra Trident choisira l'un d'entre eux pour provisionner le volume.

### Conception de pool virtuel

Lors de la création d'un backend, vous pouvez généralement spécifier un ensemble de paramètres. Il était impossible pour l'administrateur de créer un autre système back-end avec les mêmes identifiants de stockage et avec un ensemble de paramètres différent. Grâce à l'introduction de pools virtuels, ce problème a été résolu. Les pools virtuels sont une abstraction de niveau introduite entre le back-end et la classe de stockage Kubernetes. L'administrateur peut ainsi définir des paramètres et des étiquettes que l'on peut référencer via les classes de stockage Kubernetes comme un sélecteur, de façon indépendante du back-end. Il est possible de définir des pools virtuels pour tous les systèmes back-end NetApp pris en charge avec Astra Trident. Il s'agit notamment des systèmes SolidFire/NetApp HCI, ONTAP, Cloud Volumes Service sur GCP et Azure NetApp Files.

 Lors de la définition de pools virtuels, il est recommandé de ne pas tenter de réorganiser l'ordre des pools virtuels existants dans une définition backend. Il est également conseillé de ne pas modifier/modifier les attributs d'un pool virtuel existant et de définir un nouveau pool virtuel à la place.

### Émulation de différents niveaux de service/QoS

Il est possible de concevoir des pools virtuels pour émuler des classes de service. Grâce à l'implémentation du pool virtuel pour Cloud volumes Service pour Azure NetApp Files, examinons comment nous pouvons configurer différentes classes de service. Configurer le back-end Azure NetApp Files avec plusieurs étiquettes représentant différents niveaux de performances. Définissez `servicelevel` l'aspect sur le niveau de performance approprié et ajoutez d'autres aspects requis sous chaque étiquette. Créez désormais différentes classes de stockage Kubernetes qui seraient mappées sur différents pools virtuels. En utilisant ce `parameters.selector` champ, chaque classe de stockage indique quels pools virtuels peuvent être utilisés pour héberger un volume.

### Attribution d'un ensemble spécifique d'aspects

Il est possible de concevoir plusieurs pools virtuels, dont les aspects sont spécifiques, à partir d'un système back-end unique. Pour ce faire, configurez le back-end avec plusieurs étiquettes et définissez les aspects requis sous chaque étiquette. Créez maintenant différentes classes de stockage Kubernetes à l'aide du

parameters.selector champ qui serait mappé sur différents pools virtuels. Les volumes provisionnés sur le back-end possèdent les aspects définis dans le pool virtuel choisi.

## Caractéristiques des PVC qui affectent le provisionnement du stockage

Certains paramètres au-delà de la classe de stockage requise peuvent affecter le processus de décision de provisionnement Astra Trident lors de la création d'un volume persistant.

### Mode d'accès

Lors de la demande de stockage via un PVC, l'un des champs obligatoires est le mode d'accès. Le mode désiré peut affecter le back-end sélectionné pour héberger la demande de stockage.

Astra Trident tentera de correspondre au protocole de stockage utilisé avec la méthode d'accès spécifiée dans la matrice suivante. Cette technologie est indépendante de la plateforme de stockage sous-jacente.

	<b>ReadWriteOnce</b>	<b>ReadOnlyMany</b>	<b>ReadWriteMany</b>
ISCSI	Oui	Oui	Oui (bloc brut)
NFS	Oui	Oui	Oui

Toute demande de volume persistant **ReadWriteMany** soumise à un déploiement Trident sans système back-end NFS configuré entraînera le provisionnement d'un volume. Pour cette raison, le demandeur doit utiliser le mode d'accès qui convient à son application.

## Opérations de volume

### Modifier les volumes persistants

Les volumes persistants sont, à deux exceptions près, des objets immuables dans Kubernetes. Une fois créée, la règle de récupération et la taille peuvent être modifiées. Toutefois, certains aspects du volume ne peuvent pas être modifiés en dehors de Kubernetes. Vous pouvez ainsi personnaliser le volume pour des applications spécifiques, en veillant à ce que la capacité ne soit pas accidentellement consommée ou tout simplement pour déplacer le volume vers un autre contrôleur de stockage pour n'importe quelle raison.



Les actuellement sur provisionnement des arborescences Kubernetes ne prennent pas en charge les opérations de redimensionnement des volumes pour les volumes NFS ou iSCSI PVS. Astra Trident prend en charge l'extension des volumes NFS et iSCSI.

Les détails de connexion du PV ne peuvent pas être modifiés après sa création.

### Création de copies Snapshot de volume à la demande

Astra Trident prend en charge la création de copies Snapshot de volume à la demande et la création de demandes de volume persistant à partir de copies Snapshot via le framework CSI. Les snapshots constituent une méthode pratique de conservation des copies ponctuelles des données et ont un cycle de vie indépendant du volume persistant source dans Kubernetes. Ces snapshots peuvent être utilisés pour cloner des demandes de volume persistant.

### Créer des volumes à partir de copies Snapshot

Astra Trident prend également en charge la création de volumes persistant à partir des snapshots de volume. Pour ce faire, il suffit de créer une demande de volume persistant et de mentionner l' datasource comme

instantané requis à partir duquel le volume doit être créé. Astra Trident va gérer ce volume de volume persistant en créant un volume dont les données sont présentes sur le snapshot. Grâce à cette fonctionnalité, il est possible de dupliquer des données entre régions, de créer des environnements de test, de remplacer un volume de production endommagé ou corrompu dans son intégralité, ou de récupérer des fichiers et des répertoires spécifiques et de les transférer vers un autre volume attaché.

## Déplacement des volumes dans le cluster

Les administrateurs du stockage peuvent déplacer des volumes entre les agrégats et les contrôleurs du cluster ONTAP sans interruption pour l'utilisateur du stockage. Cette opération n'affecte pas Astra Trident ou le cluster Kubernetes, tant que l'agrégat de destination est un auquel le SVM utilisé par Astra Trident a accès. Important : si l'agrégat a été récemment ajouté au SVM, le système back-end devra être actualisé en le ajoutant à Astra Trident. Cela déclenchera l'Astra Trident afin de réinventorier la SVM afin que le nouvel agrégat soit reconnu.

Néanmoins, Astra Trident ne prend pas automatiquement en charge le déplacement des volumes entre les systèmes back-end. Il s'agit notamment d'étendre les SVM au sein d'un même cluster, entre plusieurs clusters ou sur une autre plateforme de stockage (même si ce système est un SVM connecté à Astra Trident).

Si un volume est copié à un autre emplacement, la fonctionnalité d'importation de volume peut être utilisée pour importer les volumes actuels dans Astra Trident.

## Développement des volumes

Astra Trident prend en charge le redimensionnement des volumes NFS et iSCSI PVS. Les utilisateurs peuvent ainsi redimensionner leurs volumes directement via la couche Kubernetes. L'extension de volume est possible pour toutes les principales plateformes de stockage NetApp, y compris ONTAP, SolidFire/NetApp HCI et les systèmes back-end Cloud Volumes Service. Pour autoriser une éventuelle extension ultérieurement, définissez `allowVolumeExpansion` sur `true` dans votre classe de stockage associée au volume. Lorsque le volume persistant doit être redimensionné, modifiez l'``spec.resources.requests.storage`` annotation de la demande de volume persistant en fonction de la taille de volume requise. Trident s'occupe automatiquement du redimensionnement du volume sur le cluster de stockage.

## Importer un volume existant dans Kubernetes

L'importation de volumes permet d'importer un volume de stockage existant dans un environnement Kubernetes. Ceci est actuellement pris en charge par les `ontap-nas` pilotes, `ontap-nas-flexgroup`, `solidfire-san`, `azure-netapp-files` et `gcp-cvs`. Cette fonctionnalité est utile lors du portage d'une application existante sur Kubernetes ou lors de scénarios de reprise après incident.

Lorsque vous utilisez ONTAP et `solidfire-san` des pilotes, utilisez la commande `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` pour importer un volume existant dans Kubernetes et le gérer par Astra Trident. Le fichier PVC YAML ou JSON utilisé dans la commande de volume d'importation pointe vers une classe de stockage qui identifie Astra Trident comme provisionneur. Si vous utilisez un système back-end NetApp HCI/SolidFire, assurez-vous que les noms des volumes sont uniques. Si les noms des volumes sont dupliqués, cloner le volume en un nom unique afin que la fonctionnalité d'importation des volumes puisse les distinguer.

Si le `azure-netapp-files` pilote ou `gcp-cvs` est utilisé, utilisez la commande `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` pour importer le volume dans Kubernetes et le gérer par Astra Trident. Cela garantit une référence de volume unique.

À l'exécution de la commande ci-dessus, Astra Trident trouve le volume sur le back-end et lit sa taille. Il ajoute automatiquement (et écrase si nécessaire) la taille du volume de la demande de volume configurée. Astra Trident crée ensuite le nouveau volume persistant, et Kubernetes lie la demande de volume persistant au

volume persistant.

Lorsqu'un conteneur a été déployé de façon à ce qu'il ait besoin de la demande de volume persistant importée spécifique, il resterait dans un état en attente jusqu'à ce que la paire PVC/PV soit liée via le processus d'importation de volume. Une fois la paire PVC/PV liée, le conteneur doit s'installer, à condition qu'il n'y ait pas d'autres problèmes.

## Le déploiement des services OpenShift

Les services de cluster à valeur ajoutée OpenShift offrent des fonctionnalités importantes aux administrateurs de clusters et aux applications hébergées. Le stockage utilisé par ces services peut être provisionné à l'aide des ressources locales. Toutefois, la capacité, la performance, la récupération et la durabilité du service sont souvent limitées. En tirant parti d'une baie de stockage d'entreprise pour fournir la capacité nécessaire à ces services, nous pouvons obtenir un service considérablement amélioré. Cependant, comme pour toutes les applications, OpenShift et les administrateurs de stockage doivent travailler en étroite collaboration afin de déterminer les options les plus adaptées à chacun d'entre eux. La documentation Red Hat doit être largement exploitée pour déterminer les exigences et s'assurer que les besoins en matière de dimensionnement et de performances sont satisfaits.

### Service de registre

Le déploiement et la gestion du stockage pour le registre ont été documentés "[netapp.io](#)" dans le "[Blog](#)".

### Service de journalisation

Comme les autres services OpenShift, le service de journalisation est déployé à l'aide d'Ansible avec les paramètres de configuration fournis par le fichier d'inventaire, également appelé hôtes, fourni avec le PlayBook. Deux méthodes d'installation sont proposées : le déploiement de la journalisation lors de l'installation initiale d'OpenShift et le déploiement de la journalisation une fois OpenShift installé.

À partir de la version 3.9 de Red Hat OpenShift, la documentation officielle recommande à NFS d'utiliser le service de journalisation en raison de problèmes de corruption des données. Ceci est basé sur les tests Red Hat de leurs produits. Le serveur NFS ONTAP ne présente pas ces problèmes et peut facilement soutenir un déploiement de journalisation. En fin de compte, le choix du protocole pour le service de journalisation constitue un bon choix. Il suffit de savoir que les deux fonctionneront bien avec les plateformes NetApp. Il n'y a aucune raison d'éviter NFS si c'est votre choix.

Si vous choisissez d'utiliser NFS avec le service de journalisation, vous devez définir la variable Ansible `openshift_enable_unsupported_configurations` sur `true` pour empêcher l'échec du programme d'installation.

### Commencez

Le service de journalisation peut, éventuellement, être déployé pour les deux applications ainsi que pour les opérations de base du cluster OpenShift. Si vous choisissez de déployer la journalisation des opérations, en spécifiant la variable `openshift_logging_use_ops` comme `true`, deux instances du service seront créées. Les variables qui contrôlent l'instance de journalisation des opérations contiennent des "OPS", alors que l'instance des applications ne le fait pas.

Il est important de configurer les variables Ansible selon la méthode de déploiement afin de s'assurer que le stockage approprié est utilisé par les services sous-jacents. Examinons les options de chacune des méthodes de déploiement.



Les tableaux ci-dessous contiennent uniquement les variables pertinentes pour la configuration du stockage en ce qui concerne le service de journalisation. Vous trouverez d'autres options ["Documentation de journalisation Red Hat OpenShift"](#) qui doivent être vérifiées, configurées et utilisées en fonction de votre déploiement.

Les variables du tableau ci-dessous entraînent la création d'un volume persistant et de demande de volume persistant pour le service de journalisation à l'aide des informations fournies. Cette méthode est beaucoup moins flexible qu'avec le manuel d'installation des composants après l'installation d'OpenShift. Toutefois, si des volumes sont déjà disponibles, il s'agit d'une option.

Variable	Détails
<code>openshift_logging_storage_kind</code>	Définissez sur <code>nfs</code> pour que le programme d'installation crée un fichier PV NFS pour le service de journalisation.
<code>openshift_logging_storage_host</code>	Le nom d'hôte ou l'adresse IP de l'hôte NFS. Il doit être défini sur la LIF de données pour votre machine virtuelle.
<code>openshift_logging_storage_nfs_directory</code>	Chemin de montage pour l'exportation NFS. Par exemple, si le volume est relié par jonction à <code>/openshift_logging</code> , vous utiliserez ce chemin pour cette variable.
<code>openshift_logging_storage_volume_name</code>	Le nom, par exemple <code>pv_ose_logs</code> , du volume persistant à créer.
<code>openshift_logging_storage_volume_size</code>	La taille de l'exportation NFS, par exemple <code>100Gi</code> .

Si votre cluster OpenShift est déjà en cours d'exécution et que Trident a donc été déployé et configuré, le programme d'installation peut utiliser le provisionnement dynamique pour créer les volumes. Les variables suivantes doivent être configurées.

Variable	Détails
<code>openshift_logging_es_pvc_dynamic</code>	Définis sur <code>true</code> pour l'utilisation de volumes provisionnés dynamiquement.
<code>openshift_logging_es_pvc_storage_class_name</code>	Nom de la classe de stockage qui sera utilisée dans le PVC.
<code>openshift_logging_es_pvc_size</code>	Taille du volume demandé dans la demande de volume persistant.
<code>openshift_logging_es_pvc_prefix</code>	Préfixe pour les ESV utilisés par le service de journalisation.
<code>openshift_logging_es_ops_pvc_dynamic</code>	Définissez sur <code>true</code> pour utiliser les volumes provisionnés dynamiquement pour l'instance de journalisation des opérations.
<code>openshift_logging_es_ops_pvc_storage_class_name</code>	Nom de la classe de stockage de l'instance de journalisation OPS.
<code>openshift_logging_es_ops_pvc_size</code>	Taille de la demande de volume pour l'instance OPS.
<code>openshift_logging_es_ops_pvc_prefix</code>	Préfixe pour les ESV de l'instance OPS.

## Déploiement de la pile de consignation

Si vous déployez la connexion dans le cadre du processus d'installation initiale d'OpenShift, il vous suffit de suivre le processus de déploiement standard. Ansible configure et déploie les services et les objets OpenShift nécessaires, de sorte que le service soit disponible dès qu'Ansible se termine.

Cependant, si vous déployez après l'installation initiale, vous devez utiliser le PlayBook des composants Ansible. Ce processus peut varier légèrement avec les différentes versions d'OpenShift. Assurez-vous de lire et de suivre "[Documentation Red Hat OpenShift Container Platform 3.11](#)" votre version.

## Services de metrics

Le service de metrics fournit à l'administrateur des informations précieuses sur l'état, l'utilisation des ressources et la disponibilité du cluster OpenShift. Il est également nécessaire d'utiliser la fonctionnalité de montée en charge automatique des pods. De nombreuses entreprises utilisent les données issues du service de metrics pour leurs applications de refacturation et/ou de show-back.

Comme pour le service de journalisation, OpenShift dans son ensemble, Ansible est utilisé pour déployer le service de metrics. De même, tout comme le service de journalisation, le service de metrics peut être déployé lors de la configuration initiale du cluster ou après son fonctionnement à l'aide de la méthode d'installation des composants. Les tableaux suivants contiennent les variables importantes lors de la configuration du stockage persistant pour le service de metrics.

 Les tableaux ci-dessous contiennent uniquement les variables pertinentes pour la configuration du stockage car elles concernent le service de metrics. De nombreuses autres options sont disponibles dans la documentation qui doit être examinée, configurée et utilisée en fonction de votre déploiement.

Variable	Détails
openshift_metrics_storage_kind	Définissez sur nfs pour que le programme d'installation crée un fichier PV NFS pour le service de journalisation.
openshift_metrics_storage_host	Le nom d'hôte ou l'adresse IP de l'hôte NFS. Il doit être défini sur la LIF de données pour votre SVM.
openshift_metrics_storage_nfs_directory	Chemin de montage pour l'exportation NFS. Par exemple, si le volume est relié par jonction à /openshift_metrics, vous utiliserez ce chemin pour cette variable.
openshift_metrics_storage_volume_name	Le nom, par exemple pv_ose_metrics, du volume persistant à créer.
openshift_metrics_storage_volume_size	La taille de l'exportation NFS, par exemple 100Gi.

Si votre cluster OpenShift est déjà en cours d'exécution et que Trident a donc été déployé et configuré, le programme d'installation peut utiliser le provisionnement dynamique pour créer les volumes. Les variables suivantes doivent être configurées.

Variable	Détails
openshift_metrics_cassandra_pvc_prefix	Préfixe à utiliser pour les ESV de metrics.
openshift_metrics_cassandra_pvc_size	Taille des volumes à demander.

Variable	Détails
openshift_metrics_cassandra_storage_type	Le type de stockage à utiliser pour les metrics, doit être défini sur dynamique pour qu'Ansible crée des demandes de volume persistant avec la classe de stockage appropriée.
openshift_metrics_cassandra_pvc_storage_class_name	Nom de la classe de stockage à utiliser.

## Déployez le service de metrics

Déployez le service à l'aide des variables Ansible appropriées définies dans votre fichier hôtes/d'inventaire. Si vous déployez au moment de l'installation d'OpenShift, le volume persistant est créé et utilisé automatiquement. Si vous déployez à l'aide des playbooks des composants après l'installation d'OpenShift, Ansible crée les demandes PVCS requises et, une fois qu'Astra Trident a provisionné le stockage pour eux, déploie le service.

Les variables ci-dessus et le processus de déploiement peuvent changer avec chaque version d'OpenShift. Assurez-vous de vérifier et de suivre ["Guide de déploiement OpenShift de Red Hat"](#) votre version afin qu'elle soit configurée pour votre environnement.

## Protection des données et reprise d'activité

Découvrez les options de protection et de restauration d'Astra Trident et des volumes créés à l'aide d'Astra Trident. Vous devez disposer d'une stratégie de protection et de restauration des données pour chaque application ayant des exigences de persistance.

### RéPLICATION ET RESTAURATION D'ASTRA TRIDENT

Vous pouvez créer une sauvegarde pour restaurer Astra Trident en cas d'incident.

#### RéPLICATION ASTRA TRIDENT

ASTRA Trident utilise des CRD Kubernetes pour stocker et gérer son propre état et le cluster Kubernetes etcd pour stocker ses métadonnées.

#### ÉTAPES

1. Sauvegardez le cluster Kubernetes etcd à l'aide de ["Kubernetes : sauvegarde d'un cluster ETCD"](#).
2. Placez les artefacts de sauvegarde sur une FlexVol.



Nous vous recommandons de protéger la SVM où réside la FlexVol avec une relation SnapMirror vers une autre SVM.

#### RESTAURATION D'ASTRA TRIDENT

À l'aide des CRD Kubernetes et du snapshot de groupe Kubernetes, vous pouvez restaurer Astra Trident.

#### ÉTAPES

1. Depuis le SVM de destination, monter le volume qui contient les fichiers de données et les certificats Kubernetes sur l'hôte qui sera configuré en tant que nœud maître.

2. Copiez tous les certificats requis en rapport avec le cluster Kubernetes sous `/etc/kubernetes/pki` et les fichiers membres ETCD sous `/var/lib/etcd`.
3. Restaurez le cluster Kubernetes à partir de la sauvegarde etcd à l'aide de "[Kubernetes : restauration d'un cluster ETCD](#)".
4. Exécutez `kubectl get crd` pour vérifier que toutes les ressources personnalisées Trident sont bien présentes et récupérez les objets Trident pour vérifier que toutes les données sont disponibles.

## Réplication et restauration des SVM

ASTRA Trident ne peut pas configurer les relations de réplication, mais l'administrateur du stockage peut utiliser "[SnapMirror ONTAP](#)" pour répliquer un SVM.

En cas d'incident, vous pouvez activer la SVM de destination SnapMirror pour démarrer le service des données. Vous pouvez revenir au système principal lorsque les systèmes sont restaurés.

### Description de la tâche

Tenir compte des points suivants lors de l'utilisation de la fonction de réplication SVM SnapMirror :

- Vous devez créer un back-end distinct pour chaque SVM lorsque la fonction SVM-DR est activée.
- Configurez les classes de stockage pour sélectionner les systèmes back-end répliqués uniquement en cas de besoin, afin d'éviter que des volumes ne nécessitant pas de réplication provisionnée vers les systèmes back-end qui prennent en charge la SVM-DR.
- Les administrateurs d'applications doivent comprendre les coûts et la complexité supplémentaires associés à la réplication et tenir compte de leur plan de reprise avant de commencer ce processus.

## Réplication SVM

Utiliser "[ONTAP : réplication SVM SnapMirror](#)" pour créer la relation de réplication du SVM.

SnapMirror vous permet de définir des options pour contrôler ce qui doit être répliqué. Vous devez savoir quelles options vous avez sélectionnées lors de la préformation [Restauration d'un SVM avec Astra Trident](#).

- "[-identité-préserver vrai](#)" Réplique l'ensemble de la configuration du SVM.
- "[-discard-configs réseau](#)" Exclut les LIFs et les paramètres réseau associés.
- "[-identity-preserve false](#)" réplique uniquement les volumes et la configuration de sécurité.

## Restauration d'un SVM avec Astra Trident

Astra Trident ne détecte pas automatiquement les défaillances du SVM. En cas d'incident, l'administrateur peut initier manuellement le basculement de Trident vers le nouveau SVM.

### Étapes

1. Annuler les transferts SnapMirror planifiés et en cours, rompre la relation de réplication, arrêter la SVM source, puis activer la SVM de destination SnapMirror.
2. Si vous avez spécifié `-identity-preserve false` ou `-discard-config network` lors de la configuration de la réplication de votre SVM, mettez à jour les `managementLIF` et `dataLIF` dans le fichier de définition du back-end Trident.
3. Vérifiez que `storagePrefix` est présent dans le fichier de définition du back-end Trident. Ce paramètre ne peut pas être modifié. L'omission `storagePrefix` entraînera l'échec de la mise à jour du back-end.

4. Mettre à jour tous les systèmes back-end nécessaires pour indiquer le nom du nouveau SVM de destination à l'aide de :

```
./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>
```

5. Si vous avez spécifié `-identity-preserve false` ou `discard-config network`, vous devez rebondir tous les pods d'application.



Si vous avez spécifié `-identity-preserve true`, tous les volumes provisionnés par Astra Trident commencent à transmettre des données lorsque le SVM de destination est activé.

## Réplication et restauration de volume

ASTRA Trident ne peut pas configurer les relations de réplication SnapMirror, mais l'administrateur du stockage peut utiliser "[Réplication et restauration ONTAP SnapMirror](#)" pour répliquer les volumes créés par Astra Trident.

Vous pouvez ensuite importer les volumes récupérés dans Astra Trident à l'aide de "[Importation de volume tridentctl](#)".



L'importation n'est pas prise en charge sur les `ontap-nas-economy` pilotes, `ontap-san-economy` ou ``ontap-flexgroup-economy``.

## Protection des données Snapshot

Vous pouvez protéger et restaurer les données à l'aide des éléments suivants :

- Un contrôleur de snapshot externe et des CRD pour créer des copies Snapshot de volume Kubernetes de volumes persistants (PVS).

["Snapshots de volume"](#)

- Snapshots ONTAP pour restaurer le contenu complet d'un volume ou pour restaurer des fichiers individuels ou des LUN.

["Snapshots ONTAP"](#)

## Réplication des applications Astra Control Center

Avec Astra Control, vous pouvez répliquer les modifications des données et des applications d'un cluster à un autre à l'aide des fonctionnalités de réplication asynchrone de SnapMirror.

["ASTRA Control : réplication d'applications sur un système distant à l'aide de la technologie SnapMirror"](#)

## Sécurité

## Sécurité

Assurez-vous que l'installation d'Astra Trident est sécurisée à l'aide des recommandations indiquées ici.

### Exécutez Astra Trident dans son propre espace de noms

Il est important d'empêcher les applications, les administrateurs d'applications, les utilisateurs et les applications de gestion d'accéder aux définitions d'objets Astra Trident ou aux pods pour assurer un stockage fiable et bloquer tout risque d'activité malveillante.

Pour séparer les autres applications et utilisateurs d'Astra Trident, installez toujours Astra Trident dans son propre espace de noms Kubernetes (`trident`). L'utilisation d'Astra Trident dans son propre espace de noms garantit que seul le personnel d'administration Kubernetes a accès au pod Trident Astra et aux artefacts (tels que les secrets d'arrière-plan et CHAP le cas échéant) stockés dans les objets CRD devant être namesées. Assurez-vous d'autoriser uniquement les administrateurs à accéder au namespace d'Astra Trident et ainsi à l'`tridentctl` application.

### Utilisez l'authentification CHAP avec les systèmes back-end ONTAP SAN

ASTRA Trident prend en charge l'authentification CHAP pour les workloads SAN ONTAP (à l'aide des `ontap-san` pilotes et `ontap-san-economy`). NetApp recommande d'utiliser le protocole CHAP bidirectionnel avec Astra Trident pour l'authentification entre l'hôte et le système back-end de stockage.

Pour les systèmes back-end ONTAP qui utilisent des pilotes de stockage SAN, Astra Trident peut configurer le protocole CHAP bidirectionnel et gérer les noms d'utilisateur et les secrets CHAP via `tridentctl`. Reportez-vous à la section ["](#) pour savoir comment Astra Trident configure CHAP sur des systèmes back-end ONTAP.

### Utilisez l'authentification CHAP avec les systèmes back-end NetApp HCI et SolidFire

NetApp recommande de déployer le protocole CHAP bidirectionnel pour garantir l'authentification entre l'hôte et les systèmes back-end NetApp HCI et SolidFire. Astra Trident utilise un objet secret qui inclut deux mots de passe CHAP par locataire. Lorsque vous installez Astra Trident, il gère les secrets CHAP et les stocke dans un `tridentvolume` objet CR pour le PV correspondant. Lorsque vous créez un volume persistant, Astra Trident utilise les secrets CHAP pour initier une session iSCSI et communiquer avec le système NetApp HCI et SolidFire sur CHAP.



Les volumes créés par Astra Trident ne sont associés à aucun groupe d'accès de volume.

### Utilisez Astra Trident avec NVE et NAE

NetApp ONTAP assure le chiffrement des données au repos pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque. Pour plus de détails, reportez-vous à ["Configurer la présentation de NetApp Volume Encryption"](#).

- Si NAE est activé sur le back-end, tous les volumes provisionnés dans Astra Trident seront NAE.
- Si NAE n'est pas activé sur le back-end, tout volume provisionné dans Astra Trident sera activé sur NVE, à moins que vous ne définiez l'indicateur de chiffrement NVE sur `false` dans la configuration back-end.

Les volumes créés dans Astra Trident sur un système back-end compatible NAE doivent être chiffrés NVE ou NAE.



- Vous pouvez définir l'indicateur de chiffrement NVE sur `true` dans la configuration back-end Trident pour remplacer le chiffrement NAE et utiliser une clé de chiffrement spécifique par volume.
- La définition de l'indicateur de chiffrement NVE `false` sur un système back-end compatible NAE permet de créer un volume NAE. Vous ne pouvez pas désactiver le chiffrement NAE en configurant l'indicateur de chiffrement NVE sur `false`.
- Vous pouvez créer manuellement un volume NVE dans Astra Trident en configurant explicitement l'indicateur de chiffrement NVE sur `true`.

Pour plus d'informations sur les options de configuration du back-end, reportez-vous à :

- ["Options de configuration du stockage SAN ONTAP"](#)
- ["Options de configuration du stockage NAS ONTAP"](#)

## Configuration de clé unifiée Linux (LUKS)

Vous pouvez activer l'utilitaire Linux Unified Key Setup (LUKS) pour chiffrer les volumes SAN ONTAP et SAN ONTAP ÉCONOMIQUES sur Astra Trident. Astra Trident prend en charge la rotation de phrase secrète et l'extension de volume pour les volumes chiffrés LUKS.

Dans Astra Trident, les volumes chiffrés LUKS utilisent le cypher et le mode aes-xts-mclair 64, comme recommandé par ["NIST"](#).

### Avant de commencer

- Les nœuds worker doivent avoir cryptsetup 2.1 ou supérieur (mais inférieur à 3.0) installé. Pour plus d'informations, visitez ["Gitlab : cryptsetup"](#).
- Pour des raisons de performances, nous recommandons aux nœuds workers de prendre en charge les nouvelles instructions AES-ni (Advanced Encryption Standard New instructions). Pour vérifier la prise en charge AES-ni, exécutez la commande suivante :

```
grep "aes" /proc/cpuinfo
```

Si rien n'est renvoyé, votre processeur ne prend pas en charge AES-ni. Pour plus d'informations sur AES-ni, visitez le site : ["Intel : instructions AES-ni \(Advanced Encryption Standard instructions\)"](#).

### Activez le cryptage LUKS

Vous pouvez activer le chiffrement côté hôte par volume en utilisant Linux Unified Key Setup (LUKS) pour SAN ONTAP et les volumes ÉCONOMIQUES SAN ONTAP.

### Étapes

1. Définissez les attributs de cryptage LUKS dans la configuration back-end. Pour plus d'informations sur les options de configuration back-end pour le SAN ONTAP, reportez-vous à la section ["Options de configuration du stockage SAN ONTAP"](#).

```

"storage": [
  {
    "labels": {"luks": "true"},
    "zone": "us_east_1a",
    "defaults": {
      "luksEncryption": "true"
    }
  },
  {
    "labels": {"luks": "false"},
    "zone": "us_east_1a",
    "defaults": {
      "luksEncryption": "false"
    }
  },
]

```

2. `parameters.selector` Permet de définir les pools de stockage à l'aide du cryptage LUKS. Par exemple :

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}

```

3. Créez un secret qui contient la phrase de passe LUKS. Par exemple :

```

kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA

```

## Limites

Les volumes LUKS-chiffrés ne peuvent pas tirer parti de la déduplication et de la compression ONTAP.

## Configuration back-end pour l'importation de volumes LUKS

Pour importer un volume LUKS, vous devez définir `luksEncryption` sur `true` le back-end. L'`luksEncryption` option indique à Astra Trident si le volume est conforme LUKS (`true`) ou non conforme LUKS (`false`) comme indiqué dans l'exemple suivant.

```
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

## Configuration PVC pour l'importation de volumes LUKS

Pour importer des volumes LUKS de façon dynamique, définissez l'annotation `trident.netapp.io/luksEncryption` sur `true` et incluez une classe de stockage LUKS activée dans la demande de volume virtuel, comme indiqué dans cet exemple.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: luks-sc
```

## Faites pivoter une phrase de passe LUKS

Vous pouvez faire pivoter la phrase de passe LUKS et confirmer la rotation.

 N'oubliez pas une phrase de passe tant que vous n'avez pas vérifié qu'elle n'est plus référencée par un volume, un snapshot ou un secret. En cas de perte d'une phrase secrète référencée, vous risquez de ne pas pouvoir monter le volume et les données resteront cryptées et inaccessibles.

## Description de la tâche

La rotation de la phrase de passe LUKS se produit lorsqu'un pod qui monte le volume est créé après la spécification d'une nouvelle phrase de passe LUKS. Lors de la création d'un pod, Astra Trident compare la phrase de passe LUKS sur le volume à la phrase de passe active dans le secret.

- Si la phrase de passe du volume ne correspond pas à la phrase de passe active dans le secret, la rotation se produit.
- Si la phrase de passe du volume correspond à la phrase de passe active du secret, le `previous-luks-passphrase` paramètre est ignoré.

## Étapes

1. Ajoutez les `node-publish-secret-name` paramètres et `node-publish-secret-namespace` `StorageClass`. Par exemple :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identifier les phrases de passe existantes sur le volume ou l'instantané.

### Volumétrie

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames: ["A"]
```

### Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["A"]
```

3. Mettez à jour le secret LUKS pour le volume afin de spécifier les phrases de passe nouvelles et précédentes. Assurez-vous que `previous-luke-passphrase-name` et `previous-luks-passphrase` la phrase de passe précédente est identique.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Créez un nouveau pod qui monte le volume. Ceci est nécessaire pour lancer la rotation.
5. Vérifiez que la phrase de passe a été pivotée.

### Volumétrie

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames: ["B"]
```

### Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames: ["B"]
```

### Résultats

La phrase de passe a été pivotée lorsque seule la nouvelle phrase de passe est renvoyée sur le volume et le snapshot.



Si deux phrases de passe sont renvoyées, par exemple `luksPassphraseNames: ["B", "A"]`, la rotation est incomplète. Vous pouvez déclencher un nouveau pod pour tenter de terminer la rotation.

### Activer l'extension de volume

Vous pouvez activer l'extension de volume sur un volume chiffré LUKS.

### Étapes

1. Activez la `CSINodeExpandSecret` fonctionnalité Gate (bêta 1.25+). Voir ["Kubernetes 1.25 : utilisez les secrets de l'extension des volumes CSI basée sur des nœuds"](#) pour plus de détails.

2. Ajoutez les `node-expand-secret-name` paramètres et `node-expand-secret-namespace` `StorageClass`. Par exemple :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

## Résultats

Lorsque vous initiez l'extension du stockage en ligne, le kubelet transmet les identifiants appropriés au pilote.

## Configuration du chiffrement Kerberos à la volée

Avec Astra Control Provisioner, vous pouvez améliorer la sécurité d'accès aux données en activant le chiffrement pour le trafic entre votre cluster géré et le back-end de stockage.

ASTRA Control provisionner prend en charge le chiffrement Kerberos sur les connexions NFSv3 et NFSv4 depuis les clusters Red Hat OpenShift et Kubernetes en amont vers les volumes ONTAP sur site.

Vous pouvez créer, supprimer, redimensionner, snapshot, cloner clone en lecture seule et importation des volumes qui utilisent le chiffrement NFS.

### Configurez le chiffrement Kerberos à la volée avec les volumes ONTAP sur site

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un système back-end de stockage ONTAP sur site.



Le chiffrement Kerberos pour le trafic NFS avec les systèmes back-end de stockage ONTAP sur site est uniquement pris en charge à l'aide du `ontap-nas` pilote de stockage.

### Avant de commencer

- Vérifiez que vous disposez de "["Mécanisme de provisionnement Astra Control activé"](#) sur le cluster géré.
- Vérifiez que vous avez accès à l' `tridentctl` utilitaire.
- Assurez-vous de disposer d'un accès administrateur au système back-end de stockage ONTAP.
- Assurez-vous de connaître le nom du ou des volumes que vous allez partager à partir du back-end de stockage ONTAP.
- Assurez-vous d'avoir préparé la machine virtuelle de stockage ONTAP à prendre en charge le chiffrement

Kerberos pour les volumes NFS. Reportez-vous "[Activez Kerberos sur une LIF donnée](#)" à pour obtenir des instructions.

- Vérifiez que tous les volumes NFSv4 utilisés avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section Configuration du domaine NetApp NFSv4 (page 13) du "[Guide des améliorations et des bonnes pratiques de NetApp NFSv4](#)".

#### Ajoutez ou modifiez les règles d'export ONTAP

Vous devez ajouter des règles aux règles d'export ONTAP existantes ou créer de nouvelles règles d'export qui prennent en charge le chiffrement Kerberos pour le volume racine de la VM de stockage ONTAP ainsi que tous les volumes ONTAP partagés avec le cluster Kubernetes en amont. Les règles d'export-policy que vous ajoutez ou les nouvelles règles d'export que vous créez doivent prendre en charge les protocoles d'accès et autorisations d'accès suivants :

#### Protocoles d'accès

Configurez la export policy avec les protocoles d'accès NFS, NFSv3 et NFSv4.

#### Accédez aux informations

Vous pouvez configurer l'une des trois versions différentes du cryptage Kerberos, en fonction de vos besoins pour le volume :

- **Kerberos 5** - (authentification et cryptage)
- **Kerberos 5i** - (authentification et chiffrement avec protection d'identité)
- **Kerberos 5p** - (authentification et chiffrement avec protection de l'identité et de la vie privée)

Configurez la règle d'export ONTAP avec les autorisations d'accès appropriées. Par exemple, si les clusters montant les volumes NFS avec un mélange de cryptage Kerberos 5i et Kerberos 5p, utilisez les paramètres d'accès suivants :

Type	Accès en lecture seule	Accès en lecture/écriture	Accès superutilisateur
UNIX	Activé	Activé	Activé
Kerberos 5i	Activé	Activé	Activé
Kerberos 5p	Activé	Activé	Activé

Pour plus d'informations sur la création de règles d'export ONTAP et de règles d'export-policy, reportez-vous à la documentation suivante :

- "[Créer une export-policy](#)"
- "[Ajouter une règle à une export-policy](#)"

#### Créer un back-end de stockage

Vous pouvez créer une configuration back-end de stockage Astra Control Provisioner qui inclut une fonctionnalité de chiffrement Kerberos.

#### Description de la tâche

Lorsque vous créez un fichier de configuration du back-end de stockage qui configure le chiffrement Kerberos, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du `spec.nfsMountOptions` paramètre :

- spec.nfsMountOptions: sec=krb5 (authentification et chiffrement)
- spec.nfsMountOptions: sec=krb5i (authentification et chiffrement avec protection de l'identité)
- spec.nfsMountOptions: sec=krb5p (authentification et chiffrement avec protection de l'identité et de la confidentialité)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de cryptage Kerberos dans la liste des paramètres, seule la première option est utilisée.

## Étapes

1. Sur le cluster géré, créez un fichier de configuration du back-end de stockage à l'aide de l'exemple suivant. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientId: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret

```

2. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

```
tridentctl create backend -f <backend-configuration-file>
```

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

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

### Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec le chiffrement Kerberos.

#### Description de la tâche

Lorsque vous créez un objet classe de stockage, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du `mountOptions` paramètre :

- `mountOptions: sec=krb5` (authentification et chiffrement)
- `mountOptions: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `mountOptions: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la confidentialité)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de cryptage Kerberos dans la liste des paramètres, seule la première option est utilisée. Si le niveau de chiffrement que vous avez spécifié dans la configuration du back-end de stockage est différent du niveau que vous spécifiez dans l'objet classe de stockage, l'objet classe de stockage a priorité.

#### Étapes

1. Créez un objet StorageClass Kubernetes à l'aide de l'exemple suivant :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Créez la classe de stockage :

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Assurez-vous que la classe de stockage a été créée :

```
kubectl get sc ontap-nas-sc
```

Vous devez voir les résultats similaires à ce qui suit :

NAME	PROVISIONER	AGE
ontap-nas-sc	csi.trident.netapp.io	15h

## Provisionner les volumes

Une fois que vous avez créé un système back-end et une classe de stockage, vous pouvez provisionner un volume. Reportez-vous à ces instructions pour "[le provisionnement d'un volume](#)".

## Configurez le chiffrement Kerberos à la volée avec les volumes Azure NetApp Files

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un seul système back-end de stockage Azure NetApp Files ou un pool virtuel de systèmes back-end de stockage Azure NetApp Files.

### Avant de commencer

- Vérifiez que vous avez activé Astra Control Provisioner sur le cluster Red Hat OpenShift géré. Reportez-vous "[Activez le mécanisme de provisionnement Astra Control](#)" à pour obtenir des instructions.
- Vérifiez que vous avez accès à l' `tridentctl` utilitaire.
- Assurez-vous d'avoir préparé le back-end de stockage Azure NetApp Files pour le chiffrement Kerberos en notant les exigences et en suivant les instructions de la section "[Documentation Azure NetApp Files](#)".
- Vérifiez que tous les volumes NFSv4 utilisés avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section Configuration du domaine NetApp NFSv4 (page 13) du "[Guide des améliorations et des bonnes pratiques de NetApp NFSv4](#)".

### Créer un back-end de stockage

Vous pouvez créer une configuration back-end de stockage Azure NetApp Files qui inclut une fonctionnalité de chiffrement Kerberos.

### Description de la tâche

Lorsque vous créez un fichier de configuration du back-end de stockage qui configure le cryptage Kerberos, vous pouvez le définir de manière à ce qu'il soit appliqué à l'un des deux niveaux possibles :

- **Le niveau du backend de stockage** utilisant le `spec.kerberos` champ
- **Niveau de pool virtuel** utilisant le `spec.storage.kerberos` champ

Lorsque vous définissez la configuration au niveau du pool virtuel, le pool est sélectionné à l'aide du libellé de la classe de stockage.

À chaque niveau, vous pouvez spécifier l'une des trois versions différentes du cryptage Kerberos :

- `kerberos: sec=krb5` (authentification et chiffrement)
- `kerberos: sec=krb5i` (authentification et chiffrement avec protection de l'identité)

- **kerberos**: sec=krb5p (authentification et chiffrement avec protection de l'identité et de la confidentialité)

## Étapes

1. Sur le cluster géré, créez un fichier de configuration back-end de stockage en utilisant l'un des exemples suivants, selon l'endroit où vous devez définir le back-end de stockage (niveau du back-end de stockage ou niveau du pool virtuel). Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

## Exemple au niveau du back-end de stockage

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

## Exemple de pool virtuel

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
        kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret

```

2. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

```
tridentctl create backend -f <backend-configuration-file>
```

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

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

### Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec le chiffrement Kerberos.

#### Étapes

1. Créez un objet `StorageClass` Kubernetes à l'aide de l'exemple suivant :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Créez la classe de stockage :

```
kubectl create -f sample-input/storage-class-sc-nfs.yaml
```

3. Assurez-vous que la classe de stockage a été créée :

```
kubectl get sc sc-nfs
```

Vous devez voir les résultats similaires à ce qui suit :

NAME	PROVISIONER	AGE
sc-nfs	csi.trident.netapp.io	15h

### Provisionner les volumes

Une fois que vous avez créé un système back-end et une classe de stockage, vous pouvez provisionner un volume. Reportez-vous à ces instructions pour "[le provisionnement d'un volume](#)".

# Connaissances et support

## Foire aux questions

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

### Questions générales

#### À quelle fréquence Astra Trident est-il commercialisé ?

À partir de la version 24.02, Astra Trident est sorti tous les quatre mois : février, juin et octobre.

#### Est-ce que l'Astra Trident prend en charge toutes les fonctionnalités publiées dans une version particulière de Kubernetes ?

Astra 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.

#### Est-ce que l'Astra Trident se base sur d'autres produits NetApp pour son fonctionnement ?

Astra Trident ne fonctionne pas sous forme de dépendance vis-à-vis d'autres logiciels NetApp, et il fonctionne comme une application autonome. Toutefois, vous devez disposer d'un système de stockage back-end NetApp.

#### Comment obtenir les informations complètes sur la configuration d'Astra Trident ?

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

#### Puis-je obtenir des metrics sur le provisionnement du stockage par Astra Trident ?

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

#### L'expérience utilisateur change-t-elle lors de l'utilisation d'Astra Trident en tant que 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 d'Astra Trident est recommandée si vous souhaitez utiliser toutes les nouvelles fonctionnalités fournies par les versions actuelles et futures.

### Installez et utilisez Astra Trident sur un cluster Kubernetes

#### Est-ce que Astra Trident prend en charge une installation hors ligne à partir d'un registre privé ?

Oui, Astra Trident peut être installé hors ligne. Reportez-vous à la "[Découvrez l'installation d'Astra Trident](#)".

## **Puis-je installer Astra Trident à distance ?**

Oui. ASTRA 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 Astra Trident ?**

ASTRA Trident est installé en tant que déploiement Kubernetes (ReplicaSet) avec une instance. Il est donc intégré à la haute disponibilité. Vous ne devez pas augmenter le nombre de répliques dans le déploiement. Si le nœud sur lequel Astra Trident est installé ou si le pod est inaccessible, Kubernetes redéploie automatiquement le pod sur un nœud en état de santé dans votre cluster. L'Astra Trident est uniquement du plan de contrôle. Les pods actuellement montés ne sont donc pas affectés en cas de redéploiement de l'Astra Trident.

## **Astra Trident a-t-il besoin d'accéder au namespace du système kube ?**

L'Astra Trident effectue une lecture sur le serveur d'API Kubernetes afin de déterminer le moment où les applications demandent des nouveaux ESV. Il doit donc accéder à `kube-System`.

## **Quels sont les rôles et privilèges utilisés par Astra 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`](#)".

## **Est-il possible de générer localement les fichiers de manifeste exacts qu'Astra Trident utilise pour l'installation ?**

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

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

Bien qu'il ne soit pas conseillé, vous pouvez utiliser le même SVM back-end pour deux instances Astra 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 Astra Trident sous ContainerLinux (anciennement CoreOS) ?**

Astra Trident est un simple pod Kubernetes. Il peut être installé quel que soit l'emplacement de Kubernetes.

## **Puis-je utiliser Astra Trident avec NetApp Cloud Volumes ONTAP ?**

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

## **Astra Trident fonctionne-t-il avec NetApp Cloud volumes Services ?**

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

## Dépannage et support

### NetApp prend-il en charge Astra Trident ?

Bien qu'Astra Trident soit open source et fourni gratuitement, NetApp le prend entièrement en charge à condition que votre système 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 "[Astra Trident Github](#)" et mentionnez **RFE** dans l'objet et la description du problème.

### Où puis-je soulever un défaut ?

Créez un problème sur "[Astra 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 Astra Trident et que j'ai besoin de précisions ? Y a-t-il une communauté ou un forum ?

Pour toute question, problème ou demande, contactez-nous via Astra "[Déroulez le canal](#)" ou GitHub.

### Le mot de passe de mon système de stockage a changé et Astra 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`.

### Astra Trident ne trouve pas le nœud Kubernetes. Comment résoudre ce problème ?

Il existe deux scénarios possibles pour savoir pourquoi Astra Trident ne peut pas trouver un nœud Kubernetes. Elle peut être due à un problème de mise en réseau dans Kubernetes ou DNS. Le demonset 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 ont eu lieu après l'installation d'Astra Trident, ce problème se produit uniquement avec les nouveaux nœuds Kubernetes qui sont 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 Astra 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 d'Astra Trident d'une version majeure à la prochaine version majeure. 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 Astra 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. ASTRA Trident utilise "[Mappage de LUN sélectif ONTAP](#)" pour découvrir les LIF iSCSI nécessaires pour établir 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 elle n'est pas fournie, Astra Trident extrait les LIF 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

**L'Astra Trident peut-il configurer le protocole CHAP pour les systèmes back-end ONTAP ?**

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

**Comment gérer les règles d'exportation avec Astra Trident ?**

Astra 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. Ainsi, Astra Trident gère automatiquement l'ajout et la suppression de règles pour les nœuds dont les adresses IP sont comprises dans les rapports CIDR donnés.

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

Astra 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.

ASTRA Trident doit être installé à l'aide de l'indicateur `--use-ipv6` (pour `tridentctl` l'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 Astra Trident pour Kubernetes ?**

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

### **Comment Astra Trident stocke-t-il les identifiants back-end ?**

Astra Trident stocke les identifiants back-end sous le titre de secrets de Kubernetes.

### **Comment l'Astra Trident sélectionne-t-il un système 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 qu'Astra Trident ne provisionne pas d'un back-end spécifique ?**

Le `excludeStoragePools` paramètre est utilisé pour filtrer l'ensemble de pools qu'Astra Trident utilisera pour le provisionnement et supprimera tous les pools correspondant.

### **Si plusieurs systèmes back-end sont de même type, comment Astra Trident sélectionne-t-il le back-end à utiliser ?**

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

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

Oui.

### **Comment Astra Trident déploie-t-il des 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 Astra Trident en définissant un paramètre dans le fichier de définition backend.

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

Par défaut, Astra Trident ne définit pas d'option de montage sur aucune valeur avec 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 de volume avec Astra Trident et 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 d'Astra Trident avec NVE et NAE"](#)

## Quelle est la meilleure façon d'implémenter la QoS pour ONTAP avec Astra Trident ?

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

## Comment puis-je spécifier le provisionnement fin ou non fin avec Astra 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'`'provisioningType'` attribut 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 demandes de volume persistant NFS créées par Astra Trident ?

Oui. Vous pouvez développer un volume de volume persistant créé par Astra 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 de quota Kubernetes en raison d'un manque de capacité, Astra Trident tente d'effectuer le provisionnement, mais s'y efforce d'erreurs.

## Est-il possible de créer des copies Snapshot de volume avec Astra Trident ?

Oui. La création à la demande de copies Snapshot de volume et de volumes persistants à partir de copies Snapshot est prise en charge par Astra 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 Astra 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 Astra 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 possibilité d'effectuer des snapshots des volumes provisionnés par Astra Trident, définissez l'option du paramètre back-end `snapshotPolicy` sur la règle de snapshot souhaitée, comme définie sur le back-end ONTAP. Tout snapshot effectué par le contrôleur de stockage ne est pas connu d'Astra Trident.

## Puis-je définir un pourcentage de réserve de snapshot pour un volume provisionné via Astra Trident ?

Oui, vous pouvez réserver un pourcentage spécifique d'espace disque pour stocker les copies Snapshot via Astra Trident en définissant l' `snapshotReserve` attribut dans le fichier de définition du 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' `snapshotPolicy` option 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 des volumes avec Astra 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 indiqués ici pour résoudre les problèmes que vous pourriez rencontrer lors de l'installation et de l'utilisation d'Astra 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 Astra Trident 20.07 et 20.10, utilisez `tprov` à la 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 `kubectl 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.

```

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

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` l'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 Astra Trident et les CRD

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



Cette opération ne peut pas être annulée. Ne le faites que si vous souhaitez une toute nouvelle installation d'Astra Trident. Pour désinstaller Astra Trident sans supprimer les CRD, reportez-vous à la "["Désinstaller Astra Trident"](#)".

## Opérateur Trident

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

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

## <code> </code>

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

```
tridentctl oblivate 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 espace de noms géré Astra 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 Astra 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 Astra Trident de différentes manières. 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 de prise en charge d'Astra Trident**

ASTRA Trident offre 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**

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

### **Prise en charge limitée**

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

### **Auto-assistance**

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

<b>Version</b>	<b>Support complet</b>	<b>Prise en charge limitée</b>	<b>Auto-assistance</b>
"24,06"	Juin 2025	Juin 2026	Juin 2027
"24,02"	—	Février 2026	Février 2027
"23,10"	—	Octobre 2025	Octobre 2026
"23,07"	—	Juillet 2025	Juillet 2026

Version	Support complet	Prise en charge limitée	Auto-assistance
"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 . Vous pouvez également trouver des informations sur le dépannage des problèmes liés à Astra "[ici](#)".

## Soutien de la communauté

Notre projet Astra est une communauté publique très vivante d'utilisateurs de conteneurs (y compris les développeurs Astra Trident) "[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 Astra 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

- "[Blogs Astra](#)"
- "[Blogs Trident d'Astra](#)"
- "[Kubernetes Hub](#)"
- "[NetApp.io](#)"

# Référence

## Ports Trident d'Astra

Découvrez les ports qu'Astra Trident utilise pour la communication.

### Ports Trident d'Astra

Astra Trident communique sur les ports suivants :

Port	Objectif
8443	HTTPS backChannel
8001	Terminal des metrics Prometheus
8000	Serveur REST Trident
17546	Port de sonde de liaison/préparation utilisé par les modules de démonset Trident



Le port de la sonde d'état de disponibilité/préparation peut être modifié lors de l'installation à l'aide de `--probe-port` l'indicateur. Il est important de s'assurer que ce port n'est pas utilisé par un autre processus sur les nœuds worker.

## API REST d'Astra Trident

Sont le moyen le plus simple d'interagir avec l'API REST d'Astra Trident, mais ["commandes et options tridentctl"](#) vous pouvez utiliser le terminal REST directement si vous préférez.

### Quand utiliser l'API REST

Il est utile pour les installations avancées qui utilisent Astra Trident en tant que binaire autonome dans les déploiements non Kubernetes.

Pour une meilleure sécurité, Astra Trident REST API est limitée à localhost par défaut lors de l'exécution à l'intérieur d'un pod. Pour modifier ce comportement, vous devez définir l'argument d'Astra Trident `--address` dans sa configuration de pod.

### Avec l'API REST

Pour des exemples de la façon dont ces API sont appelées, passez (`-d` l'indicateur `debug` ). Pour plus d'informations, reportez-vous ["Gérez Astra Trident à l'aide de tridentctl"](#) à .

L'API fonctionne comme suit :

### OBTENEZ

```
GET <trident-address>/trident/v1/<object-type>
```

Répertorie tous les objets de ce type.

```
GET <trident-address>/trident/v1/<object-type>/<object-name>
```

Obtient les détails de l'objet nommé.

## POST

```
POST <trident-address>/trident/v1/<object-type>
```

Crée un objet du type spécifié.

- Nécessite une configuration JSON pour que l'objet soit créé. Pour la spécification de chaque type d'objet, reportez-vous "[Gérez Astra Trident à l'aide de tridentctl](#)" à la .
- Si l'objet existe déjà, le comportement varie : les systèmes back-end mettent à jour l'objet existant, tandis que tous les autres types d'objet échoueront.

## SUPPRIMER

```
DELETE <trident-address>/trident/v1/<object-type>/<object-name>
```

Supprime la ressource nommée.



Les volumes associés aux systèmes back-end ou aux classes de stockage continueront d'exister. Ils doivent être supprimés séparément. Pour plus d'informations, reportez-vous "[Gérez Astra Trident à l'aide de tridentctl](#)" à .

# Options de ligne de commande

Astra Trident expose plusieurs options de ligne de commande pour l'orchestrateur Trident. Vous pouvez utiliser ces options pour modifier votre déploiement.

## Journalisation

**-debug**

Active la sortie de débogage.

**-loglevel <level>**

Définit le niveau de journalisation (débogage, info, avertissement, erreur, fatal). La valeur par défaut est INFO.

## Kubernetes

**-k8s\_pod**

Utilisez cette option ou `-k8s_api_server` pour activer la prise en charge de Kubernetes. La configuration de cette configuration entraîne l'utilisation par Trident des identifiants du compte de service Kubernetes du pod qui y est associé pour contacter le serveur d'API. Cela fonctionne uniquement lorsque Trident s'exécute en tant que pod dans un cluster Kubernetes avec les comptes de service activés.

## **-k8s\_api\_server <insecure-address:insecure-port>**

Utilisez cette option ou `-k8s_pod` pour activer la prise en charge de Kubernetes. Lorsqu'il est spécifié, Trident se connecte au serveur API Kubernetes à l'aide de l'adresse et du port non sécurisés fournis. Trident peut donc être déployé en dehors d'un pod, mais il ne prend uniquement en charge les connexions non sécurisées vers le serveur API. Pour vous connecter en toute sécurité, déployez Trident dans un pod avec l' `-k8s_pod` option.

## **Docker**

### **-volume\_driver <name>**

Nom du pilote utilisé lors de l'enregistrement du plug-in Docker. La valeur par défaut est `netapp` .

### **-driver\_port <port-number>**

Écoutez sur ce port plutôt que sur un socket de domaine UNIX.

### **-config <file>**

Obligatoire ; vous devez spécifier ce chemin vers un fichier de configuration back-end.

## **REPOS**

### **-address <ip-or-host>**

Spécifie l'adresse à laquelle le serveur REST de Trident doit écouter. Par défaut, `localhost`. Lorsque vous écoutez sur `localhost` et exécutez-les dans un pod Kubernetes, l'interface REST n'est pas directement accessible depuis l'extérieur du pod. `-address ""` Permet de rendre l'interface REST accessible à partir de l'adresse IP du pod.



Vous pouvez configurer l'interface REST de Trident pour écouter et utiliser l'interface `127.0.0.1` (pour IPv4) ou `[:1]` (pour IPv6) uniquement.

### **-port <port-number>**

Spécifie le port sur lequel le serveur REST de Trident doit écouter. La valeur par défaut est `8000`.

### **-rest**

Active l'interface REST. Valeur `true` par défaut.

## **Kubernetes et objets Trident**

Vous pouvez interagir avec Kubernetes et Trident à l'aide des API REST en lisant et en écrivant des objets de ressource. La relation entre Kubernetes et Trident, Trident et le stockage, ainsi que Kubernetes et le stockage est établie avec plusieurs objets de ressources. Certains de ces objets sont gérés par Kubernetes et d'autres sont gérés à l'aide de Trident.

### **Comment les objets interagissent-ils les uns avec les autres ?**

La manière la plus simple de comprendre les objets, leur rôle et leur interaction consiste à suivre une seule demande de stockage auprès d'un utilisateur Kubernetes :

1. Un utilisateur crée une `PersistentVolumeClaim` demande de nouvelle d' `PersistentVolume` une taille particulière à partir d'un Kubernetes `StorageClass` précédemment configuré par l'administrateur.
2. Kubernetes `StorageClass` identifie Trident comme provisionneur et inclut des paramètres qui indiquent à Trident comment provisionner un volume pour la classe demandée.
3. Trident se voit attribuer le `StorageClass` même nom qui identifie la correspondance `Backends` et `StoragePools` qu'il peut utiliser pour provisionner des volumes pour la classe.
4. Trident provisionne le stockage sur un back-end correspondant et crée deux objets : un `PersistentVolume` dans Kubernetes qui indique à Kubernetes comment rechercher, monter et traiter le volume, et un volume dans Trident qui conserve la relation entre le `PersistentVolume` et le stockage réel.
5. Kubernetes lie le `PersistentVolumeClaim` au nouveau `PersistentVolume`. Les pods incluant le `PersistentVolumeClaim` montent ce volume persistant sur tout hôte sur lequel il s'exécute.
6. Un utilisateur crée un `VolumeSnapshot` d'une demande de volume persistant existante, en utilisant un `VolumeSnapshotClass` qui pointe vers Trident.
7. Trident identifie le volume associé à la demande de volume persistant et crée un snapshot du volume sur son back-end. Elle crée également un `VolumeSnapshotContent` qui indique à Kubernetes comment identifier le Snapshot.
8. Un utilisateur peut créer un `PersistentVolumeClaim` utilisant `VolumeSnapshot` comme source.
9. Trident identifie le snapshot requis et exécute le même ensemble d'étapes que celles impliquées dans la création d'un `PersistentVolume` et d'un `Volume`.



Pour en savoir plus sur les objets Kubernetes, nous vous recommandons vivement de lire la "["Volumes persistants"](#)" section de la documentation Kubernetes.

## Objets Kubernetes `PersistentVolumeClaim`

Un objet Kubernetes `PersistentVolumeClaim` est une demande de stockage émise par un utilisateur de cluster Kubernetes.

Outre la spécification standard, Trident permet aux utilisateurs de spécifier les annotations spécifiques au volume suivantes s'ils veulent remplacer les valeurs par défaut que vous définissez dans la configuration back-end :

Annotation	Option de volume	Pilotes pris en charge
<code>trident.netapp.io/fileSystem</code>	Système de fichiers	ontap-san, solidfire-san, ontap-san-economy
<code>trident.netapp.io/cloneFromPVC</code>	Volume <code>cloneSourceVolume</code>	ontap-nas, ontap-san, solidfire-san, azure-netapp-files, gcp-cvs ontap-san-économie
<code>trident.netapp.io/splitOnClone</code>	<code>SplitOnClone</code>	ontap-nas, ontap-san
<code>trident.netapp.io/protocol</code>	protocole	toutes
<code>trident.netapp.io/exportPolicy</code>	<code>ExportPolicy</code>	ontap-nas, économie ontap-nas, ontap-nas-flexgroup

Annotation	Option de volume	Pilotes pris en charge
trident.netapp.io/snapshotPolicy	Politique de snapshots	ontap-nas, ontap-nas-économie, ontap-nas-flexgroup, ontap-san
trident.netapp.io/snapshotReserve	Réserve de snapshots	ontap-nas, ontap-nas-flexgroup, ontap-san, gcp-cvs
trident.netapp.io/snapshotDirectory	Répertoire de snapshots	ontap-nas, économie ontap-nas, ontap-nas-flexgroup
trident.netapp.io/unixPermissions	Autorisations unix	ontap-nas, économie ontap-nas, ontap-nas-flexgroup
trident.netapp.io/blockSize	Taille de bloc	solidfire-san

Si le volume persistant créé est associé à la Delete règle de récupération, Trident supprime le volume persistant et le volume de sauvegarde lorsque le volume persistant est libéré (c'est-à-dire lorsque l'utilisateur supprime la demande de volume persistant). En cas d'échec de l'action de suppression, Trident marque le volume persistant comme tel et tente régulièrement l'opération jusqu'à ce qu'il réussisse ou que le volume persistant soit supprimé manuellement. Si le volume persistant utilise Retain la règle, Trident l'ignore et suppose que l'administrateur le nettoie depuis Kubernetes et le back-end, ce qui permet de sauvegarder ou d'inspecter le volume avant sa suppression. Notez que la suppression du volume persistant n'entraîne pas la suppression du volume de sauvegarde par Trident. Vous devez le supprimer à l'aide de l'API REST (tridentctl).

Trident prend en charge la création de copies Snapshot de volumes à l'aide de la spécification CSI : vous pouvez créer un Snapshot de volume et l'utiliser comme source de données pour cloner des demandes de volume existantes. Ainsi, des copies instantanées de volumes persistants peuvent être exposées à Kubernetes sous forme de snapshots. Les snapshots peuvent ensuite être utilisés pour créer de nouveaux volumes persistants. Jetez un coup d'œil On-Demand Volume Snapshots à pour voir comment cela fonctionne.

Trident propose également les `cloneFromPVC` annotations et `splitOnClone` pour la création de clones. Vous pouvez utiliser ces annotations pour cloner une demande de volume persistant sans avoir à utiliser l'implémentation CSI.

Voici un exemple : si un utilisateur a déjà un PVC appelé `mysql`, l'utilisateur peut créer un nouveau PVC appelé à `mysqlclone` l'aide de l'annotation, telle que `trident.netapp.io/cloneFromPVC: mysql`. Avec ce jeu d'annotations, Trident clone le volume correspondant à la demande de volume `mysql` au lieu de provisionner un volume entièrement.

Prenez en compte les points suivants :

- Nous vous recommandons de cloner un volume inactif.
- Un volume persistant et son clone doivent se trouver dans le même namespace Kubernetes et avoir la même classe de stockage.
- Avec les `ontap-nas` pilotes et `ontap-san`, il peut être souhaitable de définir l'annotation PVC `trident.netapp.io/splitOnClone` en conjonction avec `trident.netapp.io/cloneFromPVC`. Avec la `trident.netapp.io/splitOnClone` valeur définie sur `true`, Trident divise le volume cloné du volume parent et, par conséquent, dissocie complètement le cycle de vie du volume cloné de son volume parent au détriment de la perte d'efficacité du stockage. L'impossibilité de `trident.netapp.io/splitOnClone` la configurer ou de la configurer sur `false` entraîne une réduction de la consommation d'espace sur le back-end, au détriment de la création de dépendances entre les volumes parent et clone, de sorte que le volume parent ne peut pas être supprimé, sauf si le clone est

supprimé en premier. Si le fractionnement du clone s'avère judicieux, il s'agit de cloner un volume de base de données vide où l'on peut attendre du volume et de son clone pour diverger considérablement, et ne bénéficier pas des fonctionnalités d'efficacité du stockage offertes par ONTAP.

Le sample-input répertoire contient des exemples de définitions de PVC à utiliser avec Trident. Reportez-vous à la pour une description complète des paramètres et des paramètres associés aux volumes Trident.

## Objets Kubernetes PersistentVolume

Un objet Kubernetes `PersistentVolume` représente un élément de stockage mis à disposition du cluster Kubernetes. Il dispose d'un cycle de vie indépendant du pod qui l'utilise.



Trident crée `PersistentVolume` des objets et les enregistre automatiquement dans le cluster Kubernetes en fonction des volumes qu'il provisionne. Vous n'êtes pas censé les gérer vous-même.

Lorsque vous créez une demande de volume virtuel qui fait référence à un volume basé sur Trident `StorageClass`, Trident provisionne un nouveau volume en utilisant la classe de stockage correspondante et enregistre un nouveau volume persistant pour ce volume. Lors de la configuration du volume provisionné et du volume persistant correspondant, Trident respecte les règles suivantes :

- Trident génère un nom de volume persistant pour Kubernetes et un nom interne utilisé pour le provisionnement du stockage. Dans les deux cas, il garantit que les noms sont uniques dans leur périmètre.
- La taille du volume correspond le plus possible à la taille demandée dans le PVC, bien qu'elle puisse être arrondie à la quantité la plus proche, selon la plate-forme.

## Objets Kubernetes StorageClass

Les objets Kubernetes `StorageClass` sont spécifiés par leur nom dans `PersistentVolumeClaims` pour provisionner le stockage avec un ensemble de propriétés. La classe de stockage elle-même identifie le mécanisme de provisionnement à utiliser et définit cet ensemble de propriétés, comme le mécanisme de provisionnement le comprend.

Il s'agit de l'un des deux objets de base qui doivent être créés et gérés par l'administrateur. L'autre est l'objet back-end Trident.

Voici à quoi ressemble un objet Kubernetes `StorageClass` utilisant Trident :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: <Name>
provisioner: csi.trident.netapp.io
mountOptions: <Mount Options>
parameters:
  <Trident Parameters>
allowVolumeExpansion: true
volumeBindingMode: Immediate
```

Ces paramètres sont spécifiques à Trident et indiquent à Trident comment provisionner des volumes pour la classe.

Les paramètres de classe de stockage sont les suivants :

Attribut	Type	Obligatoire	Description
attributs	chaîne map[string]	non	Voir la section attributs ci-dessous
StoragePools	Mapper[string]StringList	non	Mappage des noms backend avec les listes de pools de stockage dans
Des médutiques de stockage	Mapper[string]StringList	non	Mappage des noms backend avec les listes de pools de stockage dans
Exclus du stockagePools	Mapper[string]StringList	non	Mappage des noms backend avec les listes de pools de stockage dans

Les attributs de stockage et leurs valeurs possibles peuvent être classés en attributs de sélection des pools de stockage et en attributs Kubernetes.

### Attributs de sélection du pool de stockage

Ces paramètres déterminent quels pools de stockage gérés par Trident doivent être utilisés pour provisionner les volumes d'un type donné.

Attribut	Type	Valeurs	Offre	Demande	Pris en charge par
support <sup>1</sup>	chaîne	hdd, hybride, ssd	Le pool contient des supports de ce type ; hybride signifie les deux	Type de support spécifié	ontap-nas, ontap-nas-économie, ontap-nas-flexgroup, ontap-san, solidfire-san
Type de provisionnement	chaîne	fin, épais	Le pool prend en charge cette méthode de provisionnement	Méthode de provisionnement spécifiée	thick : tous les systèmes ONTAP ; thin : tous les systèmes ONTAP et solidfire-san

Attribut	Type	Valeurs	Offre	Demande	Pris en charge par
Type de dos	chaîne	ontap-nas, économie ontap-nas, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Le pool appartient à ce type de système back-end	Backend spécifié	Tous les conducteurs
snapshots	bool	vrai, faux	Le pool prend en charge les volumes dotés de snapshots	Volume sur lequel les snapshots sont activés	ontap-nas, ontap-san, solidfire-san, gcp-cvs
clones	bool	vrai, faux	Le pool prend en charge les volumes de clonage	Volume sur lequel les clones sont activés	ontap-nas, ontap-san, solidfire-san, gcp-cvs
le cryptage	bool	vrai, faux	Le pool prend en charge les volumes chiffrés	Volume avec chiffrement activé	ontap-nas, économie ontap-nas, ontap-nas-flexgroups, ontap-san
LES IOPS	int	entier positif	Le pool est en mesure de garantir l'IOPS dans cette plage	Volume garanti ces IOPS	solidfire-san

<sup>1</sup> : non pris en charge par les systèmes ONTAP Select

Dans la plupart des cas, les valeurs demandées influencent directement le provisionnement ; par exemple, la demande d'un provisionnement lourd entraîne un volume approvisionné. Un pool de stockage Element utilise ses IOPS minimales et maximales pour définir des valeurs de QoS plutôt que la valeur demandée. Dans ce cas, la valeur demandée est utilisée uniquement pour sélectionner le pool de stockage.

Idéalement, vous pouvez utiliser `attributes` seul pour modéliser les qualités du stockage dont vous avez besoin pour répondre aux besoins d'une classe particulière. Trident découvre et sélectionne automatiquement les pools de stockage correspondant à `all` du `attributes` que vous spécifiez.

Si vous ne parvenez pas à utiliser `attributes` pour sélectionner automatiquement les pools appropriés pour une classe, vous pouvez utiliser les `storagePools` paramètres et `additionalStoragePools` pour affiner davantage les pools ou même pour sélectionner un ensemble spécifique de pools.

Vous pouvez utiliser le `storagePools` paramètre pour restreindre davantage l'ensemble de pools correspondant à n'importe quel `attributes`. En d'autres termes, Trident utilise l'intersection des pools identifiés par les `attributes` paramètres et `storagePools` pour le provisionnement. Vous pouvez utiliser les paramètres seuls ou les deux ensemble.

Vous pouvez utiliser le `additionalStoragePools` paramètre pour étendre l'ensemble des pools utilisés par

Trident pour le provisionnement, quels que soient les pools sélectionnés par les attributes paramètres et storagePools.

Vous pouvez utiliser le excludeStoragePools paramètre pour filtrer l'ensemble de pools utilisés par Trident pour le provisionnement. L'utilisation de ce paramètre supprime tous les pools correspondant.

Dans les storagePools paramètres et additionalStoragePools , chaque entrée prend la forme <backend>:<storagePoolList>, où <storagePoolList> est une liste de pools de stockage séparés par des virgules pour le back-end spécifié. Par exemple, une valeur pour additionalStoragePools peut ressembler à ontapnas\_192.168.1.100:aggr1,aggr2;solidfire\_192.168.1.101:bronze. Ces listes acceptent les valeurs regex tant pour le back-end que pour les valeurs de liste. Vous pouvez utiliser tridentctl get backend pour obtenir la liste des systèmes back-end et leurs pools.

## Attributs Kubernetes

Ces attributs n'ont aucun impact sur la sélection des pools de stockage/systèmes back-end par Trident lors du provisionnement dynamique. En effet, ces attributs fournissent simplement les paramètres pris en charge par les volumes persistants de Kubernetes. Les nœuds worker sont responsables des opérations de création de système de fichiers et peuvent nécessiter des utilitaires de système de fichiers, tels que xfsprogs.

Attribut	Type	Valeurs	Description	Facteurs pertinents	Version Kubernetes
Fstype	chaîne	ext4, ext3, xfs	Type de système de fichiers pour les volumes en mode bloc	solidfire-san, ontap-nas, ontap-nas-économie, ontap-nas-flexgroup, ontap-san, ontap-san-économie	Tout
Volumeallowexpansion	booléen	vrai, faux	Activez ou désactivez la prise en charge pour augmenter la taille de la demande de volume persistant	ontap-nas, économie ontap-nas, ontap-nas-flexgroup, ontap-san, ontap-san-économie, solidfire-san, gcp-cvs, azure-netapp-files	1.11+
Volume Bindingmode	chaîne	Immédiat, WaitForFirstConsumer	Sélectionnez le moment où la liaison des volumes et le provisionnement dynamique se produisent	Tout	1.19 - 1.26

- Le `fsType` paramètre permet de contrôler le type de système de fichiers souhaité pour les LUN SAN. En outre, Kubernetes utilise également la présence de `fsType` dans une classe de stockage pour indiquer l'existence d'un système de fichiers. La propriété des volumes peut être contrôlée à l'aide du `fsGroup` contexte de sécurité d'un pod uniquement si `fsType` est défini. Reportez-vous "[Kubernetes : configurez un contexte de sécurité pour un pod ou un conteneur](#)" à la pour une vue d'ensemble sur la définition de la propriété du volume à l'aide du `fsGroup` contexte. Kubernetes appliquera la `fsGroup` valeur uniquement si :
  - `fsType` est défini dans la classe de stockage.
  - Le mode d'accès PVC est RWO.



Pour les pilotes de stockage NFS, un système de fichiers existe déjà dans le cadre de l'exportation NFS. Pour pouvoir utiliser `fsGroup` la classe de stockage, vous devez toujours spécifier une `fsType`. Vous pouvez la définir sur `nfs` ou toute valeur non nulle.

- Pour plus d'informations sur l'extension de volume, reportez-vous à la section "[Développement des volumes](#)".
- Le programme d'installation de Trident fournit plusieurs exemples de définitions de classe de stockage à utiliser avec Trident dans `sample-input/storage-class-*.yaml`. La suppression d'une classe de stockage Kubernetes entraîne également la suppression de la classe de stockage Trident correspondante.

## Objets Kubernetes `VolumeSnapshotClass`

Les objets Kubernetes `VolumeSnapshotClass` sont analogues à `StorageClasses`. Ils aident à définir plusieurs classes de stockage. Ils sont référencés par les snapshots de volume pour associer le snapshot à la classe d'instantanés requise. Chaque snapshot de volume est associé à une classe de snapshot de volume unique.

Un `VolumeSnapshotClass` doit être défini par un administrateur pour créer des instantanés. Une classe de snapshots de volume est créée avec la définition suivante :

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: csi-snapclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Le `driver` spécifie à Kubernetes que les demandes de snapshots de volumes de la `csi-snapclass` classe sont gérées par Trident. Le `deletionPolicy` spécifie l'action à effectuer lorsqu'un snapshot doit être supprimé. Lorsque `deletionPolicy` est défini sur `Delete`, les objets de snapshot du volume ainsi que le snapshot sous-jacent du cluster de stockage sont supprimés lors de la suppression d'un snapshot. Vous pouvez également la configurer sur `Retain` signifie que `VolumeSnapshotContent` et le snapshot physique sont conservés.

## Objets Kubernetes VolumeSnapshot

Un objet Kubernetes `VolumeSnapshot` est une demande de création d'une copie Snapshot d'un volume. Tout comme un volume persistant représente une demande de copie Snapshot d'un volume effectuée par un utilisateur, une copie Snapshot de volume est une demande de création d'un snapshot d'une demande de volume persistant existante.

Lorsqu'une demande de Snapshot de volume est émise, Trident gère automatiquement la création de la copie Snapshot du volume sur le back-end et expose la copie Snapshot en créant un objet unique `VolumeSnapshotContent`. Vous pouvez créer des instantanés à partir de ESV existantes et les utiliser comme source de données lors de la création de nouveaux ESV.

 Le cycle de vie d'un `VolumeSnapshot` est indépendant de la demande de volume persistant source : un snapshot persiste même après la suppression de la demande de volume persistant source.

Lors de la suppression d'un volume persistant qui possède des snapshots associés, Trident marque le volume de sauvegarde de ce volume persistant dans un état **Suppression**, mais ne le supprime pas complètement. Le volume est supprimé lorsque tous les snapshots associés sont supprimés.

## Objets Kubernetes VolumeSnapshotContent

Un objet Kubernetes `VolumeSnapshotContent` représente un snapshot d'un volume déjà provisionné. Elle est similaire à un `PersistentVolume` et signifie un snapshot provisionné sur le cluster de stockage. Comme `PersistentVolumeClaim` pour les objets et `PersistentVolume`, lors de la création d'un Snapshot, l'`'VolumeSnapshotContent'` objet conserve un mappage un-à-un sur l'`'VolumeSnapshot'` objet qui avait demandé la création du Snapshot.

L'`VolumeSnapshotContent` objet contient des détails qui identifient de manière unique le snapshot, tels que `'snapshotHandle'`. Il `snapshotHandle` s'agit d'une combinaison unique du nom du PV et du nom de l'`'VolumeSnapshotContent'` objet.

Lorsqu'une requête de snapshot est fournie, Trident crée le snapshot sur le back-end. Une fois le snapshot créé, Trident configure un `VolumeSnapshotContent` objet et expose ce dernier à l'API Kubernetes.

 En général, il n'est pas nécessaire de gérer `VolumeSnapshotContent` l'objet. Exception à cette règle : lorsque vous souhaitez "["Importer un instantané de volume"](#) créer des données en dehors d'Astra Trident.

## Objets Kubernetes CustomResourceDefinition

Les ressources personnalisées Kubernetes sont des terminaux de l'API Kubernetes définis par l'administrateur et utilisés pour regrouper des objets similaires. Kubernetes prend en charge la création de ressources personnalisées pour le stockage d'une collection d'objets. Vous pouvez obtenir ces définitions de ressources en exécutant `kubectl get crds`.

Les définitions de ressources personnalisées (CRD) et les métadonnées d'objet associées sont stockées sur le magasin de métadonnées Kubernetes. Ce qui évite d'avoir recours à un magasin séparé pour Trident.

ASTRA Trident utilise `CustomResourceDefinition` des objets pour préserver l'identité des objets Trident, tels que les systèmes back-end Trident, les classes de stockage Trident et les volumes Trident. Ces objets sont gérés par Trident. En outre, la structure d'instantané de volume CSI introduit quelques CRD nécessaires pour définir des instantanés de volume.

Les CRDS sont une construction Kubernetes. Les objets des ressources définies ci-dessus sont créés par Trident. Par exemple simple, lorsqu'un back-end est créé à l'aide de `tridentctl`, un objet CRD correspondant `tridentbackends` est créé pour être consommé par Kubernetes.

Voici quelques points à garder à l'esprit sur les CRD de Trident :

- Lorsque Trident est installé, un ensemble de CRD est créé et peut être utilisé comme tout autre type de ressource.
- Lors de la désinstallation de Trident à l'aide de la `tridentctl uninstall` commande, les modules Trident sont supprimés, mais les CRD créés ne sont pas nettoyés. Reportez-vous "["Désinstaller Trident"](#)" à la pour comprendre comment Trident peut être complètement supprimé et reconfiguré de zéro.

## Objets Astra Trident StorageClass

Trident crée des classes de stockage correspondantes pour les objets Kubernetes `StorageClass` qui spécifient `csi.trident.netapp.io` dans leur champ de provisionnement. Le nom de classe de stockage correspond à celui de l'objet Kubernetes `StorageClass` qu'il représente.



Avec Kubernetes, ces objets sont créés automatiquement lorsqu'un Kubernetes `StorageClass` qui utilise Trident en tant que provisionneur est enregistré.

Les classes de stockage comprennent un ensemble d'exigences pour les volumes. Trident mappe ces exigences avec les attributs présents dans chaque pool de stockage. S'ils correspondent, ce pool de stockage est une cible valide pour le provisionnement des volumes qui utilisent cette classe de stockage.

Vous pouvez créer des configurations de classes de stockage afin de définir directement des classes de stockage à l'aide de l'API REST. Toutefois, pour les déploiements Kubernetes, nous prévoyons qu'ils seront créés lors de l'enregistrement de nouveaux objets Kubernetes `StorageClass`.

## Objets back-end Astra Trident

Les systèmes back-end représentent les fournisseurs de stockage au-dessus desquels Trident provisionne des volumes. Une instance Trident unique peut gérer un nombre illimité de systèmes back-end.



Il s'agit de l'un des deux types d'objet que vous créez et gérez vous-même. L'autre est l'objet Kubernetes `StorageClass`.

Pour plus d'informations sur la construction de ces objets, reportez-vous à la section "["configuration des systèmes back-end"](#)".

## Objets Astra Trident StoragePool

Les pools de stockage représentent les emplacements distincts disponibles pour le provisionnement sur chaque système back-end. Pour ONTAP, ces derniers correspondent à des agrégats dans des SVM. Pour NetApp HCI/SolidFire, ils correspondent aux bandes QoS spécifiées par l'administrateur. Pour Cloud Volumes Service, ces régions correspondent à des régions du fournisseur cloud. Chaque pool de stockage dispose d'un ensemble d'attributs de stockage distincts, qui définissent ses caractéristiques de performances et ses caractéristiques de protection des données.

Contrairement aux autres objets ici, les candidats au pool de stockage sont toujours découverts et gérés automatiquement.

## Objets Astra Trident Volume

Les volumes sont l'unité de provisionnement de base, comprenant les terminaux back-end, tels que les partages NFS et les LUN iSCSI. Dans Kubernetes, ces valeurs correspondent directement à `PersistentVolumes`. Lorsque vous créez un volume, assurez-vous qu'il possède une classe de stockage, qui détermine l'emplacement de provisionnement de ce volume, ainsi que sa taille.

- Dans Kubernetes, ces objets sont gérés automatiquement. Vous pouvez les afficher pour voir le provisionnement Trident.
- Lors de la suppression d'un volume persistant avec des snapshots associés, le volume Trident correspondant est mis à jour avec un état **Suppression**. Pour que le volume Trident soit supprimé, vous devez supprimer les snapshots du volume.

Une configuration de volume définit les propriétés qu'un volume provisionné doit avoir.

Attribut	Type	Obligatoire	Description
version	chaîne	non	Version de l'API Trident (« 1 »)
nom	chaîne	oui	Nom du volume à créer
Classe de stockage	chaîne	oui	Classe de stockage à utiliser lors du provisionnement du volume
taille	chaîne	oui	Taille du volume à provisionner en octets
protocole	chaîne	non	Type de protocole à utiliser : « fichier » ou « bloc »
Nom interne	chaîne	non	Nom de l'objet sur le système de stockage, généré par Trident
Volume cloneSourceVolume	chaîne	non	ONTAP (nas, san) et SolidFire-* : nom du volume à cloner
SplitOnClone	chaîne	non	ONTAP (nas, san) : séparer le clone de son parent
Politique de snapshots	chaîne	non	ONTAP-* : stratégie d'instantané à utiliser
Réserve de snapshots	chaîne	non	ONTAP-* : pourcentage de volume réservé pour les snapshots
ExportPolicy	chaîne	non	ontap-nas* : export policy à utiliser

Attribut	Type	Obligatoire	Description
Répertoire de snapshots	bool	non	ontap-nas* : indique si le répertoire des snapshots est visible
Autorisations unix	chaîne	non	ontap-nas* : autorisations UNIX initiales
Taille de bloc	chaîne	non	SolidFire-*: Taille de bloc/secteur
Système de fichiers	chaîne	non	Type de système de fichiers

Trident génère `internalName` lors de la création du volume. Il s'agit de deux étapes. Tout d'abord, il ajoute le préfixe de stockage (le préfixe par défaut `trident` ou le préfixe dans la configuration back-end) au nom du volume, ce qui entraîne un nom de formulaire `<prefix>-<volume-name>`. Il procède ensuite à la désinfection du nom en remplaçant les caractères non autorisés dans le back-end. Pour les systèmes ONTAP back-end, il remplace les tirets par des traits de soulignement (le nom interne devient ainsi `<prefix>_<volume-name>`). Pour les systèmes back-end Element, il remplace les tirets de traits de soulignement.

Vous pouvez utiliser des configurations de volume pour provisionner directement des volumes à l'aide de l'API REST, mais dans les déploiements Kubernetes, la plupart des utilisateurs doivent utiliser la méthode Kubernetes standard `PersistentVolumeClaim`. Trident crée automatiquement cet objet volume dans le cadre du provisionnement.

## Objets Astra Trident Snapshot

Les snapshots sont une copie de volumes à un point dans le temps, qui peut être utilisée pour provisionner de nouveaux volumes ou restaurer l'état de ces volumes. Dans Kubernetes, ces données correspondent directement aux `VolumeSnapshotContent` objets. Chaque snapshot est associé à un volume, qui est la source des données du snapshot.

Chaque `Snapshot` objet comprend les propriétés répertoriées ci-dessous :

Attribut	Type	Obligatoire	Description
version	Chaîne	Oui	Version de l'API Trident (« 1 »)
nom	Chaîne	Oui	Nom de l'objet snapshot Trident
Nom interne	Chaîne	Oui	Nom de l'objet Snapshot Trident sur le système de stockage
Nom du volume	Chaîne	Oui	Nom du volume persistant pour lequel le snapshot est créé
Volume Nom interne	Chaîne	Oui	Nom de l'objet volume Trident associé sur le système de stockage



Dans Kubernetes, ces objets sont gérés automatiquement. Vous pouvez les afficher pour voir le provisionnement Trident.

Lors de la création d'une demande d'objet Kubernetes `VolumeSnapshot`, Trident crée un objet de snapshot sur le système de stockage qui soutient. Le `internalName` de cet objet de snapshot est généré en combinant le préfixe `snapshot-` et le `UID` de l'`VolumeSnapshot` objet (par exemple, `snapshot-e8d8a0ca-9826-11e9-9807-525400f3f660`). `volumeName` et `volumeInternalName` sont renseignés en obtenant les détails du volume de sauvegarde.

## Objet Astra Trident ResourceQuota

La déamonset Trident consomme une `system-node-critical` classe de priorité, la classe de priorité la plus élevée disponible dans Kubernetes, pour s'assurer qu'Astra Trident peut identifier et nettoyer les volumes lors de l'arrêt gracieux des nœuds et permettre aux pods de diabolodéfinis Trident d'anticiper les charges de travail avec une priorité inférieure dans les clusters où la pression des ressources est élevée.

Pour ce faire, Astra Trident utilise un `ResourceQuota` objet afin de s'assurer qu'une classe de priorité « système-nœud-critique » sur le démonset Trident est satisfaite. Avant le déploiement et la création d'un jeu de données, Astra Trident recherche `ResourceQuota` l'objet et, s'il n'est pas découvert, l'applique.

Si vous avez besoin de plus de contrôle sur le quota de ressources par défaut et la classe de priorité, vous pouvez générer un `custom.yaml` ou configurer l'`'ResourceQuota'` objet à l'aide du graphique Helm.

Voici un exemple de `'ResourceQuota'` objet hiérarchisant le demonset Trident.

```
apiVersion: <version>
kind: ResourceQuota
metadata:
  name: trident-csi
  labels:
    app: node.csi.trident.netapp.io
spec:
  scopeSelector:
    matchExpressions:
      - operator : In
        scopeName: PriorityClass
        values: ["system-node-critical"]
```

Pour plus d'informations sur les quotas de ressources, reportez-vous "[Kubernetes : quotas de ressources](#)" à la section .

## Nettoyez `ResourceQuota` si l'installation échoue

Dans les rares cas où l'installation échoue après la `ResourceQuota` création de l'objet, essayez d'abord, "[désinstallation](#)" puis réinstallez.

Si cela ne fonctionne pas, supprimez manuellement l'`'ResourceQuota'` objet.

## Déposer ResourceQuota

Si vous préférez contrôler votre propre allocation de ressources, vous pouvez supprimer l'objet Astra Trident ResourceQuota à l'aide de la commande :

```
kubectl delete quota trident-csi -n trident
```

## Normes de sécurité de pod (PSS) et contraintes de contexte de sécurité (SCC)

Les normes de sécurité de Kubernetes Pod (PSS) et les règles de sécurité de Pod (PSP) définissent des niveaux d'autorisation et limitent le comportement des pods. OpenShift Security Context Constraints (SCC) définit de façon similaire les restrictions de pod spécifiques à OpenShift Kubernetes Engine. Pour offrir cette personnalisation, Astra Trident autorise certaines autorisations lors de l'installation. Les sections suivantes décrivent en détail les autorisations définies par Astra Trident.



PSS remplace les politiques de sécurité Pod (PSP). La PSP est obsolète dans Kubernetes v1.21 et elle sera supprimée dans la version 1.25. Pour plus d'informations, reportez-vous ["Kubernetes : sécurité"](#) à .

## Contexte de sécurité Kubernetes requis et champs associés

Autorisations	Description
Privilégié	CSI nécessite que les points de montage soient bidirectionnels, ce qui signifie que le pod de nœud Trident doit exécuter un conteneur privilégié. Pour plus d'informations, reportez-vous <a href="#">"Kubernetes : propagation du montage"</a> à .
Mise en réseau d'hôtes	Requis pour le démon iSCSI. <code>iscsiadm</code> Gère les montages iSCSI et utilise la mise en réseau des hôtes pour communiquer avec le démon iSCSI.
IPC de l'hôte	Le NFS utilise la communication interprocess (IPC) pour communiquer avec le NFSD.
PID de l'hôte	Nécessaire pour démarrer <code>rpc-statd</code> pour NFS. ASTRA Trident interroge les processus hôtes pour déterminer si <code>rpc-statd</code> est exécuté avant le montage des volumes NFS.
Capacités	Cette <code>SYS_ADMIN</code> fonctionnalité est fournie dans le cadre des fonctionnalités par défaut pour les conteneurs privilégiés. Par exemple, Docker définit les fonctionnalités suivantes pour les conteneurs privilégiés : <code>CapPrm: 0000003ffffffffffff</code> <code>CapEff: 0000003ffffffffffff</code>

Autorisations	Description
Seccomp	Le profil Seccomp est toujours « confiné » dans des conteneurs privilégiés. Par conséquent, il ne peut pas être activé sur Astra Trident.
SELinux	Sur OpenShift, les conteneurs privilégiés sont exécutés dans <code>spc_t</code> le domaine (« conteneur super privilégié ») et les conteneurs non privilégiés dans le <code>container_t</code> domaine. Sur <code>containerd</code> , avec <code>container-selinux</code> installé, tous les conteneurs sont exécutés dans le <code>spc_t</code> domaine, ce qui désactive effectivement SELinux. Par conséquent, Astra Trident n'ajoute pas <code>seLinuxOptions</code> aux conteneurs.
DAC	Les conteneurs privilégiés doivent être exécutés en tant que root. Les conteneurs non privilégiés s'exécutent comme root pour accéder aux sockets unix requis par CSI.

## Normes de sécurité du pod (PSS)

Étiquette	Description	Valeur par défaut
pod-security.kubernetes.io/enforce pod-security.kubernetes.io/enforce-version	Permet au contrôleur et aux nœuds Trident d'être admis dans le namespace d'installation. Ne modifiez pas le libellé de l'espace de noms.	enforce: privileged enforce-version: <version of the current cluster or highest version of PSS tested.>



La modification des étiquettes de l'espace de noms peut entraîner l'absence de planification des modules, un "erreur de création: ..." ou un "avertissement: trident-csi-...". Dans ce cas, vérifiez si le libellé de l'espace de noms pour `privileged` a été modifié. Si c'est le cas, réinstallez Trident.

## Politiques de sécurité des pods (PSP)

Champ	Description	Valeur par défaut
allowPrivilegeEscalation	Les conteneurs privilégiés doivent autoriser l'escalade des priviléges.	true
allowedCSIDrivers	Trident n'utilise pas les volumes éphémères CSI en ligne.	Vide
allowedCapabilities	Les conteneurs Trident non privilégiés ne nécessitent pas de fonctionnalités supérieures à celles des ensembles par défaut et les conteneurs privilégiés se voient accorder toutes les capacités possibles.	Vide

Champ	Description	Valeur par défaut
allowedFlexVolumes	Trident n'utilise pas un "Pilote FlexVolume", donc ils ne sont pas inclus dans la liste des volumes autorisés.	Vide
allowedHostPaths	Le pod des nœuds Trident monte le système de fichiers racine du nœud, ce qui ne permet donc pas de définir cette liste.	Vide
allowedProcMountTypes	Trident n'utilise aucun ProcMountTypes.	Vide
allowedUnsafeSysctls	Trident n'exige pas de sécurité sysctls.	Vide
defaultAddCapabilities	Aucune fonctionnalité n'est requise pour être ajoutée aux conteneurs privilégiés.	Vide
defaultAllowPrivilegeEscalation	L'autorisation de réaffectation des priviléges est gérée dans chaque pod Trident.	false
forbiddenSysctls	Non sysctls sont autorisés.	Vide
fsGroup	Les conteneurs Trident s'exécutent en tant que root.	RunAsAny
hostIPC	Le montage des volumes NFS nécessite la communication de l'IPC hôte avec nfdsd	true
hostNetwork	Iscsiadm nécessite que le réseau hôte communique avec le démon iSCSI.	true
hostPID	Le PID de l'hôte est nécessaire pour vérifier si rpc-statd est exécuté sur le nœud.	true
hostPorts	Trident n'utilise aucun port hôte.	Vide
privileged	Les pods de nœuds Trident doivent exécuter un conteneur privilégié pour monter des volumes.	true
readOnlyRootFilesystem	Les pods de nœuds Trident doivent écrire dans le système de fichiers de nœuds.	false
requiredDropCapabilities	Les pods de nœuds Trident exécutent un conteneur privilégié et ne peuvent pas supprimer de fonctionnalités.	none
runAsGroup	Les conteneurs Trident s'exécutent en tant que root.	RunAsAny

Champ	Description	Valeur par défaut
runAsUser	Les conteneurs Trident s'exécutent en tant que root.	runAsAny
runtimeClass	Trident n'utilise pas RuntimeClasses .	Vide
seLinux	Trident ne définit pas seLinuxOptions, car il existe actuellement des différences dans la façon dont les temps d'exécution des conteneurs et les distributions Kubernetes gèrent SELinux.	Vide
supplementalGroups	Les conteneurs Trident s'exécutent en tant que root.	RunAsAny
volumes	Les pods Trident requièrent ces plug-ins de volume.	hostPath, projected, emptyDir

## Contraintes de contexte de sécurité (SCC)

Étiquettes	Description	Valeur par défaut
allowHostDirVolumePlugin	Les pods des nœuds Trident montent le système de fichiers racine du nœud.	true
allowHostIPC	Le montage des volumes NFS nécessite la communication de l'IPC hôte avec nfsd.	true
allowHostNetwork	Iscsiadm nécessite que le réseau hôte communique avec le démon iSCSI.	true
allowHostPID	Le PID de l'hôte est nécessaire pour vérifier si rpc-statd est exécuté sur le nœud.	true
allowHostPorts	Trident n'utilise aucun port hôte.	false
allowPrivilegeEscalation	Les conteneurs privilégiés doivent autoriser l'escalade des priviléges.	true
allowPrivilegedContainer	Les pods de nœuds Trident doivent exécuter un conteneur privilégié pour monter des volumes.	true
allowedUnsafeSysctls	Trident n'exige pas de sécurité sysctls.	none

Étiquettes	Description	Valeur par défaut
allowedCapabilities	Les conteneurs Trident non privilégiés ne nécessitent pas de fonctionnalités supérieures à celles des ensembles par défaut et les conteneurs privilégiés se voient accorder toutes les capacités possibles.	Vide
defaultAddCapabilities	Aucune fonctionnalité n'est requise pour être ajoutée aux conteneurs privilégiés.	Vide
fsGroup	Les conteneurs Trident s'exécutent en tant que root.	RunAsAny
groups	Ce SCC est spécifique à Trident et lié à son utilisateur.	Vide
readOnlyRootFilesystem	Les pods de nœuds Trident doivent écrire dans le système de fichiers de nœuds.	false
requiredDropCapabilities	Les pods de nœuds Trident exécutent un conteneur privilégié et ne peuvent pas supprimer de fonctionnalités.	none
runAsUser	Les conteneurs Trident s'exécutent en tant que root.	RunAsAny
seLinuxContext	Trident ne définit pas seLinuxOptions, car il existe actuellement des différences dans la façon dont les temps d'exécution des conteneurs et les distributions Kubernetes gèrent SELinux.	Vide
seccompProfiles	Les conteneurs privilégiés s'exécutent toujours « sans limite ».	Vide
supplementalGroups	Les conteneurs Trident s'exécutent en tant que root.	RunAsAny
users	Une entrée est fournie pour lier ce SCC à l'utilisateur Trident dans l'espace de noms Trident.	s/o
volumes	Les pods Trident requièrent ces plug-ins de volume.	hostPath, downwardAPI, projected, emptyDir

# Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

## Droits d'auteur

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Politique de confidentialité

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Source ouverte

Vous pouvez consulter les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp pour Astra Trident dans le fichier des avis pour chaque version à l'adresse <https://github.com/NetApp/trident/>.

## 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 JOUSSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

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

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

## Informations sur les marques commerciales

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