# Meilleures pratiques et recommandations

## Trident

NetApp
July 01, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/trident-2602/trident-reco/deploy-reco.html on July 01, 2026. Always check docs.netapp.com for the latest.

# Sommaire

# Meilleures pratiques et recommandations

## Déploiement

Utilisez les recommandations énumérées ici lors du déploiement de Trident.

### Déployer dans un espace de noms dédié

"Espaces de noms" assurent une séparation administrative entre différentes applications et constituent une barrière au partage des ressources. Par exemple, un PVC d'un espace de noms ne peut pas être consommé depuis un autre. Trident fournit des ressources PV à tous les espaces de noms du cluster Kubernetes et exploite ainsi un compte de service disposant de privilèges élevés.

De plus, l'accès au pod Trident pourrait 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 n'ont pas la possibilité d'accéder aux définitions d'objets Trident ou aux pods eux-mêmes.

### Utilisez des quotas et des limites de plage pour contrôler la consommation de stockage

Kubernetes possède deux fonctionnalités qui, combinées, offrent un mécanisme puissant pour limiter la consommation de ressources par les applications. Le "mécanisme de quota 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, sur une base par espace de noms. De plus, l'utilisation d'un "limite de portée" garantit que les requêtes PVC respectent à la fois une valeur minimale et maximale avant que la demande ne soit transmise au provisionneur.

Ces valeurs sont définies pour chaque espace de noms, ce qui signifie que chaque espace de noms doit avoir des valeurs définies qui correspondent à ses besoins en ressources. Voir ici pour des informations à propos de "comment tirer parti des quotas".

## Configuration du stockage

Chaque plateforme de stockage dans le portefeuille NetApp possède des capacités uniques qui bénéficient aux applications, conteneurisées ou non.

### Présentation de la plateforme

Trident fonctionne avec ONTAP et Element. Il n'existe pas de plateforme qui soit mieux adaptée à toutes les applications et à tous les scénarios qu'une autre ; cependant, les besoins de l'application et de l'équipe qui administre le dispositif doivent être pris en compte lors du choix d'une plateforme.

Il est recommandé de suivre les bonnes pratiques de base pour le système d'exploitation hôte avec le protocole que vous utilisez. Vous pouvez également envisager d'intégrer les bonnes pratiques applicatives, lorsqu'elles sont disponibles, avec le backend, la classe de stockage et les paramètres PVC afin d'optimiser le stockage pour des applications spécifiques.

# Meilleures pratiques ONTAP et Cloud Volumes ONTAP

Découvrez les meilleures pratiques pour configurer ONTAP et Cloud Volumes ONTAP pour Trident.

Les recommandations suivantes constituent des lignes directrices pour la configuration ONTAP pour les charges de travail conteneurisées, qui consomment des volumes provisionnés dynamiquement par Trident. Chacune d'elles doit être examinée et évaluée en fonction de sa pertinence pour votre environnement.

### Utilisez des SVM dédiés à Trident

Les machines virtuelles de stockage (SVM) assurent l'isolation et la séparation administrative entre les locataires sur un système ONTAP. L'attribution d'une SVM aux applications permet la délégation de privilèges et l'application des meilleures pratiques pour limiter la consommation de ressources.

Plusieurs options sont disponibles pour la gestion du SVM :

- Fournissez l'interface de gestion du cluster dans la configuration du backend, ainsi que les informations d'identification appropriées, et spécifiez le nom du SVM.
- Créez une interface de gestion dédiée pour la SVM en utilisant ONTAP System Manager ou la CLI.
- Partagez le rôle de gestion avec une interface de données NFS.

Dans chaque cas, l'interface doit être dans le DNS, et le nom DNS doit être utilisé lors de la configuration de Trident. Cela aide à faciliter certains scénarios de reprise après sinistre, par exemple, SVM-DR sans l'utilisation de la conservation de l'identité réseau.

Il n'y a pas de préférence entre une LIF de gestion dédiée ou partagée pour la SVM, toutefois, vous devez vous assurer que vos politiques de sécurité réseau sont compatibles avec l'approche que vous choisissez. Dans tous les cas, la LIF de gestion doit être accessible via DNS pour offrir une flexibilité maximale si "SVM-DR" est utilisée conjointement avec Trident.

### Limiter le nombre maximal de volumes

Les systèmes de stockage ONTAP ont un nombre maximal de volumes, qui varie selon la version du logiciel et la plateforme matérielle. Consultez "NetApp Hardware Universe" pour votre plateforme spécifique et votre version d'ONTAP afin de déterminer les limites exactes. Lorsque le nombre de volumes est épuisé, les opérations de provisionnement échouent non seulement pour Trident, mais pour toutes les demandes de stockage.

Les pilotes de Trident `ontap-nas` et `ontap-san` provisionnent un FlexVolume pour chaque volume persistant (PV) Kubernetes créé. Le pilote `ontap-nas-economy` crée environ un FlexVolume pour 200 PV (configurable entre 50 et 300). Le pilote `ontap-san-economy` crée environ un FlexVolume pour 100 PV (configurable entre 50 et 200). Pour éviter que Trident ne consomme tous les volumes disponibles sur le système de stockage, vous devez définir une limite sur le SVM. Vous pouvez le faire depuis la ligne de commandes :

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

La valeur pour `max-volumes` varie en fonction de 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
- Le nombre de volumes persistants attendus à être consommés par les applications Kubernetes

La `max-volumes` valeur correspond au total des volumes provisionnés sur l'ensemble des nœuds du cluster ONTAP, et non sur un nœud ONTAP individuel. Par conséquent, il se peut qu'un nœud de cluster ONTAP ait beaucoup plus ou beaucoup moins de volumes Trident provisionnés qu'un autre nœud.

Par exemple, un cluster ONTAP à deux nœuds peut héberger un maximum de 2 000 volumes FlexVol. Fixer le nombre maximal de volumes à 1 250 semble très raisonnable. Cependant, si seuls les "agrégats" volumes d'un nœud sont affectés à la SVM, ou si les agrégats affectés d'un nœud ne peuvent pas être provisionnés (par exemple, en raison de la capacité), alors l'autre nœud devient la cible de tous les volumes provisionnés par Trident. Cela signifie que la limite de volumes de ce nœud peut être atteinte avant que la valeur `max-volumes` ne soit atteinte, ce qui impacte à la fois Trident et les autres opérations de volumes utilisant ce nœud. **Vous pouvez éviter cette situation en vous assurant que les agrégats de chaque nœud du cluster sont affectés à la SVM utilisée par Trident en nombre égal.**

### Cloner un volume

NetApp Trident prend en charge le clonage de volumes lors de l'utilisation des `ontap-nas`, `ontap-san` et `solidfire-san` pilotes de stockage. Lors de l'utilisation des `ontap-nas-flexgroup` ou `ontap-nas-economy` pilotes, le clonage n'est pas pris en charge. La création d'un nouveau volume à partir d'un volume existant entraînera la création d'un nouvel instantané.

Évitez de cloner un PVC associé à un StorageClass différent. Effectuez les opérations de clonage au sein du même StorageClass pour garantir la compatibilité et éviter tout comportement inattendu.

### Limiter la taille maximale des volumes créés par Trident

Pour configurer la taille maximale des volumes pouvant être créés par Trident, utilisez le `limitVolumeSize` paramètre dans votre `backend.json` définition.

En plus de contrôler la taille du volume au niveau de la baie de stockage, vous devriez également tirer parti des capacités de Kubernetes.

### Limiter la taille maximale des FlexVols créés par Trident

Pour configurer la taille maximale pour les FlexVols utilisées 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 CHAP bidirectionnel

Vous pouvez spécifier les noms d'utilisateur et mots de passe de l'initiateur et de la cible CHAP dans la définition de votre backend et demander à Trident d'activer CHAP sur la SVM. En utilisant le paramètre `useCHAP` dans la configuration de votre backend, Trident authentifie les connexions iSCSI pour les backends ONTAP avec CHAP.

### Créer et utiliser une règle QoS SVM

L'utilisation d'une politique QoS ONTAP, appliquée à la SVM, limite le nombre d'IOPS consommables par les volumes provisionnés Trident. Cela permet d' "empêcher un tyran"éviter qu'un conteneur défaillant ou incontrôlé n'affecte les charges de travail en dehors de la SVM Trident.

Vous pouvez créer une politique QoS pour la SVM en quelques étapes. Consultez la documentation de votre version de ONTAP pour obtenir les informations les plus précises. L'exemple ci-dessous crée une politique 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>
```

De plus, si votre version d'ONTAP le permet, vous pouvez envisager d'utiliser un minimum de QoS pour garantir un certain débit aux charges de travail conteneurisées. La QoS adaptative n'est pas compatible avec une politique au niveau SVM.

Le nombre d'IOPS dédiés aux charges de travail conteneurisées dépend de nombreux aspects. Parmi ceux-ci, on trouve notamment :

- Autres charges de travail utilisant la baie de stockage. Si d'autres charges de travail, non liées au déploiement Kubernetes, utilisent les ressources de stockage, il convient de veiller à ce qu'elles ne soient pas accidentellement affectées négativement.
- Charges de travail prévues exécutées dans des conteneurs. Si des charges de travail ayant des exigences élevées en IOPS s'exécutent dans des conteneurs, une politique de QoS faible entraîne une mauvaise expérience.

Il est important de noter qu'une politique QoS définie au niveau de la SVM implique que tous les volumes provisionnés sur la SVM partagent le même pool d'IOPS. Si une application conteneurisée, ou un petit nombre d'applications conteneurisées, a des besoins élevés en IOPS, elle risque de pénaliser les autres charges de travail conteneurisées. Si tel est le cas, vous pouvez envisager d'utiliser une automatisation externe pour attribuer des politiques QoS par volume.

> Vous ne devez attribuer le groupe de stratégie QoS au SVM **que** si votre version d'ONTAP est antérieure à 9.8.

**Créer des groupes de règles QoS pour Trident**

La qualité de service (QoS) garantit que les performances des charges de travail critiques ne sont pas dégradées par des charges de travail concurrentes. Les groupes de règles QoS d'ONTAP offrent 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 la QoS, consultez "Garantir le débit avec QoS". Vous pouvez spécifier des groupes de règles QoS dans le backend ou dans un pool de stockage, et ils sont appliqués à chaque volume créé dans ce pool ou backend.

ONTAP propose deux types de groupes de stratégies QoS : traditionnels et adaptatifs. Les groupes de stratégies traditionnels offrent un débit maximal (ou minimal, dans les versions plus récentes) fixe en IOPS. La QoS adaptative ajuste automatiquement le débit à la taille de la charge de travail, en maintenant le ratio IOPS à To|Go à mesure que la taille de la charge de travail évolue. Cela représente un avantage considérable lorsque vous gérez des centaines ou des milliers de charges de travail dans un déploiement de grande envergure.

Tenez compte des points suivants lors de la création de groupes de règles QoS :

- Vous devez définir la `qosPolicy` clé dans le bloc `defaults` de la configuration du backend. Voir l'exemple de configuration du backend 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 groupes de stratégies par volume, afin que chaque volume bénéficie de l'ensemble du débit spécifié par le groupe de stratégies. Les groupes de stratégies partagés ne sont pas pris en charge.

Pour plus d'informations sur les groupes de politiques QoS, consultez "Référence des commandes ONTAP".

**Limiter l'accès aux ressources de stockage aux membres du cluster Kubernetes**

Limiter l'accès aux volumes NFS, aux LUN iSCSI et aux LUN FC créés par Trident est un élément essentiel de la posture de sécurité de votre déploiement Kubernetes. Cela empêche les hôtes qui ne font pas partie du cluster Kubernetes d'accéder aux volumes et de modifier potentiellement les données de manière inattendue.

Il est important de comprendre que les espaces de noms constituent la limite logique des ressources dans Kubernetes. On suppose que les ressources dans le même espace de noms peuvent être partagées, cependant, il est important de noter qu'il n'existe aucune capacité inter-espaces de noms. Cela signifie que même si les PV sont des objets globaux, lorsqu'ils sont liés à un PVC, ils ne sont accessibles que par les pods qui sont dans le même espace de noms. **Il est essentiel de veiller à utiliser les espaces de noms pour assurer la séparation lorsque cela est approprié.**

La principale préoccupation de la plupart des organisations concernant la sécurité des données dans un contexte Kubernetes est qu'un processus exécuté dans un conteneur puisse accéder à un stockage monté sur l'hôte, mais qui n'est pas destiné au conteneur. "Espaces de noms" sont conçus pour empêcher ce type de compromission. Il existe cependant une exception : les conteneurs privilégiés.

Un conteneur privilégié est un conteneur exécuté avec des permissions au niveau de l'hôte nettement supérieures à la normale. Celles-ci ne sont pas refusées par défaut, alors assurez-vous de désactiver la capacité en utilisant "politiques de sécurité des pods".

Pour les volumes nécessitant un accès depuis Kubernetes et des hôtes externes, le stockage doit être géré de manière traditionnelle, avec la création du PV par l'administrateur et non géré par Trident. Cela garantit que le

volume de stockage n'est détruit que lorsque Kubernetes et les hôtes externes sont déconnectés et n'utilisent plus le volume. De plus, une règle d'export peut être appliquée, ce qui permet l'accès depuis les nœuds du cluster Kubernetes et les serveurs cibles situés en dehors du cluster Kubernetes.

Pour les déploiements comportant des nœuds d'infrastructure dédiés (par exemple, OpenShift) ou d'autres nœuds incapables de planifier des applications utilisateur, des règles d'export distinctes doivent être utilisées afin de limiter davantage l'accès aux ressources de stockage. Cela inclut la création d'une règle d'export pour les services déployés sur ces nœuds d'infrastructure (par exemple, les services de métriques et de journalisation OpenShift), ainsi que pour les applications standard déployées sur des nœuds non dédiés à l'infrastructure.

#### Utilisez une règle d'export

Vous devez vous assurer qu'une règle d'export existe pour chaque backend, autorisant uniquement l'accès aux nœuds présents dans le cluster Kubernetes. Trident peut créer et gérer automatiquement des règles d'export. Ainsi, Trident limite l'accès aux volumes qu'il provisionne aux nœuds du cluster Kubernetes et simplifie l'ajout et la suppression de nœuds.

Vous pouvez également créer une règle d'export manuellement et la remplir avec une ou plusieurs règles d'export qui traitent chaque demande d'accès au nœud :

- Utilisez la `vserver export-policy create` commande ONTAP CLI pour créer la règle d'export.
- Ajoutez des règles à la règles d'export à l'aide de la commande CLI `vserver export-policy rule create` ONTAP.

L'exécution de ces commandes vous permet de restreindre quels nœuds Kubernetes ont accès aux données.

#### Désactiver `showmount` pour l'application SVM

La fonctionnalité `showmount` permet à un client NFS d'interroger le SVM pour obtenir une liste des exports NFS disponibles. Un pod déployé sur le cluster Kubernetes peut exécuter la commande `showmount -e` contre le SVM et recevoir une liste des montages disponibles, y compris ceux auxquels il n'a pas accès. Bien que cela, en soi, ne constitue pas une compromission de la sécurité, cela fournit des informations inutiles susceptibles d'aider un utilisateur non autorisé à se connecter à un export NFS.

Vous devez désactiver `showmount` en utilisant la commande ONTAP CLI au niveau SVM :

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```

## SolidFire meilleures pratiques

Découvrez les meilleures pratiques pour configurer le stockage SolidFire pour Trident.

#### Créer un compte SolidFire

Chaque compte SolidFire représente un propriétaire de volume unique et reçoit ses propres identifiants Challenge-Handshake Authentication Protocol (CHAP). Vous pouvez accéder aux volumes associés à un compte soit en utilisant le nom du compte et les identifiants CHAP correspondants, soit via un groupe d'accès aux volumes. Un compte peut avoir jusqu'à deux mille volumes qui lui sont attribués, mais un volume ne peut appartenir qu'à un seul compte.

### Créer une politique QoS

Utilisez les politiques de qualité de service (QoS) SolidFire si vous souhaitez créer et enregistrer un paramètre de qualité de service standardisé qui peut être appliqué à de nombreux volumes.

Vous pouvez configurer les paramètres QoS volume par volume. Les performances de chaque volume peuvent être garanties en définissant trois paramètres configurables qui définissent la QoS : Min IOPS, Max IOPS et Burst IOPS.

Voici les valeurs minimales, maximales et en rafale d'IOPS possibles pour la taille de bloc 4Kb.

| Paramètre IOPS | Définition | Valeur min. | valeur par défaut | Valeur maximale (4Kb) |
|---|---|---|---|---|
| IOPS minimales | Le niveau de performance garanti pour un volume. | 50 | 50 | 15000 |
| IOPS max | Les performances ne dépasseront pas cette limite. | 50 | 15000 | 200 000 |
| IOPS en rafale | Nombre maximal d'IOPS autorisés dans un scénario de rafale courte. | 50 | 15000 | 200 000 |

Bien que les valeurs Max IOPS et Burst IOPS puissent être fixées à 200 000, les performances maximales réelles d'un volume sont limitées par l'utilisation du cluster et les performances par nœud.

La taille des blocs et la bande passante influent directement sur le nombre d'IOPS. Lorsque la taille des blocs augmente, le système accroît la bande passante jusqu'au niveau nécessaire pour traiter les blocs plus volumineux. Lorsque la bande passante augmente, le nombre d'IOPS que le système peut atteindre diminue. Consultez "Qualité de service SolidFire" pour plus d'informations sur la QoS et les performances.

### Authentification SolidFire

Element prend en charge deux méthodes d'authentification : CHAP et les groupes d'accès aux volumes (VAG). CHAP utilise le protocole CHAP pour authentifier l'hôte auprès du backend. Les groupes d'accès aux volumes contrôlent l'accès aux volumes qu'ils provisionnent. NetApp recommande d'utiliser CHAP pour l'authentification, car c'est plus simple et il n'y a pas de limites de mise à l'échelle.

Trident avec le provisionneur CSI amélioré prend en charge l'authentification CHAP. Les VAG doivent être utilisés uniquement en mode de fonctionnement traditionnel non-CSI.

L'authentification CHAP (vérification que l'initiateur est bien l'utilisateur du volume) est prise en charge uniquement avec le contrôle d'accès basé sur les comptes. Si vous utilisez CHAP pour l'authentification, deux options sont disponibles : CHAP unidirectionnel et CHAP bidirectionnel. CHAP unidirectionnel authentifie l'accès au volume à l'aide du nom de compte SolidFire et du secret de l'initiateur. L'option CHAP bidirectionnel offre la méthode d'authentification la plus sécurisée, car le volume authentifie l'hôte via le nom de compte et le secret de l'initiateur, puis l'hôte authentifie le volume via le nom de compte et le secret de la cible.

Toutefois, si CHAP ne peut être activé et que des groupes d'accès aux volumes (VAG) 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, le contrôle d'accès basé sur le compte est utilisé. Si l'initiateur iSCSI n'est pas configuré pour utiliser l'authentification CHAP, alors le contrôle d'accès du Volume Access Group est utilisé.

### Où trouver plus d'informations ?

Certains documents de bonnes pratiques sont listés ci-dessous. Recherchez dans "Bibliothèque NetApp" les versions les plus récentes.

**ONTAP**

- "Guide des meilleures pratiques et de mise en œuvre NFS"
- "Administration SAN" (pour iSCSI)
- "Configuration iSCSI Express pour RHEL"

**Logiciel Element**

- "Configuration de SolidFire pour Linux"

**NetApp HCI**

- "NetApp HCI Prérequis de déploiement"
- "Accédez au NetApp Deployment Engine"

**Informations sur les meilleures pratiques d'application**

- "Meilleures pratiques pour MySQL sur ONTAP"
- "Meilleures pratiques pour MySQL sur SolidFire"
- "NetApp SolidFire et Cassandra"
- "Meilleures pratiques Oracle sur SolidFire"
- "Meilleures pratiques PostgreSQL sur SolidFire"

Toutes les applications ne disposent pas de directives spécifiques, il est important de travailler avec votre NetApp équipe et d'utiliser le "Bibliothèque NetApp" pour trouver la documentation la plus récente.

# Intégrer Trident

Pour intégrer Trident, les éléments de conception et d'architecture suivants doivent être intégrés : sélection et déploiement des pilotes, conception de la classe de stockage, conception du pool virtuel, impacts de la revendication de volume persistant (PVC) sur l'approvisionnement du stockage, opérations sur les volumes et déploiement des services OpenShift utilisant Trident.

### Sélection et déploiement du pilote

Sélectionnez et déployez un pilote backend pour votre système de stockage.

### Pilotes backend ONTAP

Les pilotes backend ONTAP se distinguent par le protocole utilisé et la manière dont les volumes sont provisionnés sur le système de stockage. Il convient donc d'examiner attentivement le pilote à déployer.

À un niveau supérieur, si votre application comporte des composants nécessitant un stockage partagé (plusieurs pods accédant au même PVC), les pilotes NAS seraient le choix par défaut, tandis que les pilotes iSCSI basés sur les blocs répondent aux besoins d'un stockage non partagé. Choisissez le protocole en fonction des exigences de l'application et du niveau de confort des équipes de stockage et d'infrastructure. De manière générale, il existe peu de différences entre eux pour la plupart des applications, donc la décision est souvent basée sur la nécessité ou non d'un stockage partagé (lorsque plus d'un pod aura besoin d'un accès simultané).

Les pilotes backend ONTAP disponibles sont :

- `ontap-nas` : Chaque PV provisionné est un ONTAP FlexVolume.
- `ontap-nas-economy`: Chaque PV provisionné est un qtree, avec un nombre configurable de qtrees par FlexVolume (la valeur par défaut est 200).
- `ontap-nas-flexgroup`: Chaque PV est provisionné en tant que ONTAP FlexGroup, et tous les agrégats affectés à une SVM sont utilisés.
- `ontap-san` : Chaque PV provisionné est un LUN au sein de son propre FlexVolume.
- `ontap-san-economy`: Chaque PV provisionné est un LUN, avec un nombre configurable de LUN par FlexVolume (100 par défaut).

Le choix entre les trois pilotes NAS a des répercussions sur les fonctionnalités qui sont mises à la disposition de l'application.

Notez que, dans les tableaux ci-dessous, toutes les fonctionnalités ne sont pas accessibles via Trident. Certaines doivent être appliquées par l'administrateur de stockage après le provisionnement si cette fonctionnalité est souhaitée. Les notes de bas de page en exposant distinguent la fonctionnalité par fonctionnalité et par pilote.

| Pilotes ONTAP NAS | Snapshots | Clones | Politiques d'exportation dynamiques | Multi-attach | QoS | Redimensionner | Réplication |
|---|---|---|---|---|---|---|---|
| `ontap-nas` | Oui | Oui | Oui | Oui | Oui | Oui | Oui |
| `ontap-nas-economy` | NO [3] | NO [3] | Oui | Oui | NO [3] | Oui | NO [3] |
| `ontap-nas-flexgroup` | Oui | NON | Oui | Oui | Oui | Oui | Oui |

Trident propose 2 pilotes SAN pour ONTAP, dont les capacités sont présentées ci-dessous.

| Pilotes ONTAP SAN | Snapshots | Clones | Multi-attach | CHAP bidirectionnel | QoS | Redimensionner | Réplication |
|---|---|---|---|---|---|---|---|
| `ontap-san` | Oui | Oui | Oui | Oui | Oui | Oui | Oui |

| Pilotes ONTAP SAN | Snapshots | Clones | Multi-attach | CHAP bidirectionnel | QoS | Redimensionner | Réplication |
|---|---|---|---|---|---|---|---|
| `ontap-san-economy` | Oui | Oui | Oui | Oui | NO [3] | Oui | NO [3] |

> Note de bas de page pour les tableaux ci-dessus : Yes [1] : Non géré par Trident Yes [2] : Géré par Trident, mais pas au niveau PV granulaire NO [3] : Non géré par Trident et pas au niveau PV granulaire Yes [4] : Pris en charge pour les volumes raw-block Yes [5] : Pris en charge par Trident

Les fonctionnalités qui ne sont pas granulaires au niveau du PV sont appliquées à l'ensemble du FlexVolume et tous les PV (c'est-à-dire les qtrees ou les LUNs dans des FlexVols partagés) partageront un calendrier commun.

Comme nous pouvons le voir dans les tableaux ci-dessus, une grande partie de la fonctionnalité entre le `ontap-nas` et le `ontap-nas-economy` est identique. Cependant, parce que le `ontap-nas-economy` pilote limite la capacité de contrôler la planification à la granularité par PV, cela peut affecter en particulier votre planification de reprise après sinistre et de sauvegarde. Pour les équipes de développement qui souhaitent exploiter la fonctionnalité de clonage de PVC sur le stockage ONTAP, cela n'est possible qu'en utilisant les `ontap-nas`, `ontap-san` ou `ontap-san-economy` pilotes.

Le `solidfire-san` driver est également capable de cloner des PVC.

#### Pilotes backend Cloud Volumes ONTAP

Cloud Volumes ONTAP offre le contrôle des données ainsi que des fonctionnalités de stockage de niveau entreprise pour divers cas d'utilisation, notamment le partage de fichiers et le stockage en mode bloc prenant en charge les protocoles NAS et SAN (NFS, SMB / CIFS et iSCSI). Les pilotes compatibles pour Cloud Volume ONTAP sont `ontap-nas`, `ontap-nas-economy`, `ontap-san` et `ontap-san-economy`. Ceux-ci sont applicables pour Cloud Volume ONTAP pour Azure, Cloud Volume ONTAP pour GCP.

#### Amazon FSx for ONTAP pilotes backend

Amazon FSx for NetApp ONTAP vous permet de tirer parti des fonctionnalités, des performances et des capacités d'administration NetApp que vous connaissez, tout en bénéficiant de la simplicité, de l'agilité, de la sécurité et de l'évolutivité du stockage des données sur AWS. FSx for ONTAP prend en charge de nombreuses fonctionnalités du système de fichiers ONTAP et des API d'administration. Les pilotes compatibles pour Cloud Volume ONTAP sont `ontap-nas`, `ontap-nas-economy`, `ontap-nas-flexgroup`, `ontap-san` et `ontap-san-economy`.

#### NetApp HCI/SolidFire pilotes backend

Le `solidfire-san` pilote utilisé avec les plateformes NetApp HCI/SolidFire aide l'administrateur à configurer un backend Element pour Trident sur la base des limites de QoS. Si vous souhaitez concevoir votre backend pour définir des limites de QoS spécifiques sur les volumes provisionnés par Trident, utilisez le paramètre `type` dans le fichier backend. L'administrateur peut également restreindre la taille du volume pouvant être créé sur le stockage à l'aide du paramètre `limitVolumeSize`. Actuellement, les fonctionnalités de stockage Element telles que le redimensionnement de volume et la réplication de volume ne sont pas prises en charge via le pilote `solidfire-san`. Ces opérations doivent être effectuées manuellement via l'interface web d'Element Software.

| Pilote SolidFire | Snapshots | Clones | Multi-attach | CHAP | QoS | Redimensionner | Réplication |
|---|---|---|---|---|---|---|---|
| `solidfire-san` | Oui | Oui | Oui | Oui | Oui | Oui | Oui |

> Note de bas de page : Oui [1] : Non géré par Trident Oui [2] : Pris en charge pour les volumes de blocs bruts

#### Pilotes backend Azure NetApp Files

Trident utilise le `azure-netapp-files` driver pour gérer le "Azure NetApp Files" service.

Vous trouverez plus d'informations sur ce pilote et sur la manière de le configurer dans "Configuration du backend Trident pour Azure NetApp Files".

| Pilote Azure NetApp Files | Snapshots | Clones | Multi-attach | QoS | Développer | Réplication |
|---|---|---|---|---|---|---|
| `azure-netapp-files` | Oui | Oui | Oui | Oui | Oui | Oui |

> Note de bas de page : Oui [1] : Non géré par Trident

## 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 explique comment concevoir une classe de stockage pour votre application.

#### Utilisation spécifique du backend

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. Trois ensembles de filtres peuvent être définis dans la classe de stockage : `storagePools`, `additionalStoragePools`, et/ou `excludeStoragePools`.

Le paramètre `storagePools` permet de restreindre le stockage à l'ensemble des pools correspondant à tout attribut spécifié. Le paramètre `additionalStoragePools` est utilisé pour étendre l'ensemble des pools que Trident utilise pour le provisionnement, ainsi que l'ensemble des pools sélectionnés par les attributs et les paramètres `storagePools`. Vous pouvez utiliser chaque 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 des pools listés qui correspondent aux attributs.

#### Émuler les politiques QoS

Si vous souhaitez concevoir des classes de stockage pour émuler des politiques de qualité de service, créez une classe de stockage avec l'attribut `media` comme `hdd` ou `ssd`. En fonction de l'attribut `media` mentionné dans la classe de stockage, Trident sélectionnera le backend approprié qui fournit des agrégats `hdd` ou `ssd` pour correspondre à l'attribut media, puis dirigera le provisionnement des volumes vers l'agrégat spécifique. Nous pouvons donc créer une classe de stockage PREMIUM avec l'attribut `media` défini comme `ssd`, ce qui pourrait être classé comme la politique QoS PREMIUM. Nous pouvons créer une autre classe de stockage STANDARD avec l'attribut media défini comme `hdd`, ce qui pourrait être classé comme la politique QoS

STANDARD. Nous pourrions également utiliser l'attribut ``IOPS'' dans la classe de stockage pour rediriger le provisionnement vers un appareil Element, qui peut être défini comme une politique QoS.

#### Utiliser le backend en fonction de fonctionnalités spécifiques

Les classes de stockage peuvent être conçues pour diriger l'allocation de volumes sur un backend spécifique où des fonctionnalités telles que l'allocation dynamique et statique, les snapshots, les clones et le chiffrement sont activés. Pour spécifier le stockage à utiliser, créez des classes de stockage qui spécifient le backend approprié avec la fonctionnalité requise activée.

#### Pools virtuels

Les pools virtuels sont disponibles pour tous les backends Trident. Vous pouvez définir des pools virtuels pour n'importe quel backend, en utilisant n'importe quel pilote que Trident fournit.

Les pools virtuels permettent à un administrateur de créer un niveau d'abstraction au-dessus des backends, référençables via les Storage Classes, pour une plus grande flexibilité et un placement efficace des volumes sur les backends. Différents backends peuvent être définis avec la même classe de service. De plus, plusieurs pools de stockage peuvent être créés sur un même backend mais avec des caractéristiques différentes. Lorsqu'une Storage Class est configurée avec un sélecteur comportant des étiquettes spécifiques, Trident choisit un backend correspondant à toutes les étiquettes du sélecteur pour y placer le volume. Si les étiquettes du sélecteur de la Storage Class correspondent à plusieurs pools de stockage, Trident en choisira un pour provisionner le volume.

## Conception de pool virtuel

Lors de la création d'un backend, il est généralement possible de spécifier un ensemble de paramètres. Il était impossible pour l'administrateur de créer un autre backend avec les mêmes informations d'identification de stockage et avec un ensemble de paramètres différent. Avec l'introduction des pools virtuels, ce problème a été atténué. Un pool virtuel est un niveau d'abstraction introduit entre le backend et la classe de stockage Kubernetes afin que l'administrateur puisse définir des paramètres ainsi que des étiquettes qui peuvent être référencées via les classes de stockage Kubernetes comme sélecteur, de manière indépendante du backend. Les pools virtuels peuvent être définis pour tous les backends NetApp pris en charge avec Trident. Cette liste inclut SolidFire/NetApp HCI, ONTAP, ainsi que 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 de backend. Il est également conseillé de ne pas 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. En utilisant l'implémentation de pool virtuel pour Cloud Volume Service for Azure NetApp Files, examinons comment nous pouvons configurer différentes classes de service. Configurez le backend Azure NetApp Files avec plusieurs étiquettes, représentant différents niveaux de performance. Définissez l'aspect `servicelevel` sur le niveau de performance approprié et ajoutez les autres aspects requis sous chaque étiquette. Créez maintenant différentes classes de stockage Kubernetes qui correspondront à différents pools virtuels. À l'aide du champ `parameters.selector`, chaque StorageClass 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 avec un ensemble spécifique d'aspects à partir d'un seul backend de stockage. Pour ce faire, configurez le backend avec plusieurs étiquettes et définissez les aspects

requis sous chaque étiquette. Créez ensuite différentes classes de stockage Kubernetes en utilisant le champ `parameters.selector` qui correspondrait à différents pools virtuels. Les volumes provisionnés sur le backend auront les aspects définis dans le pool virtuel choisi.

#### Caractéristiques du PVC qui affectent le provisionnement du stockage

Certains paramètres autres que la classe de stockage demandée peuvent affecter le processus de décision de provisionnement Trident lors de la création d'un PVC.

#### Mode d'accès

Lors d'une demande de stockage via un PVC, le mode d'accès est un champ obligatoire. Le mode souhaité peut affecter le backend sélectionné pour héberger la demande de stockage.

Trident tentera d'associer le protocole de stockage utilisé à la méthode d'accès spécifiée selon la matrice suivante. Ceci est indépendant de la plateforme de stockage sous-jacente.

| | ReadWriteOnce | ReadOnlyMany | ReadWriteMany |
|---|---|---|---|
| iSCSI | Oui | Oui | Oui (Raw block) |
| NFS | Oui | Oui | Oui |

Une demande de PVC ReadWriteMany soumise à un déploiement Trident sans backend NFS configuré n'entraînera pas la création de volume. Pour cette raison, le demandeur doit utiliser le mode d'accès approprié pour son application.

## Opérations de volume

#### Modifier les volumes persistants

Dans Kubernetes, les volumes persistants sont, à deux exceptions près, des objets immuables. Une fois créés, la politique de récupération et la taille peuvent être modifiées. Cependant, cela n'empêche pas que certains aspects du volume soient modifiés en dehors de Kubernetes. Cela peut être souhaitable afin de personnaliser le volume pour des applications spécifiques, de s'assurer que la capacité n'est pas accidentellement consommée, ou simplement de déplacer le volume vers un autre contrôleur de stockage pour n'importe quelle raison.

> Les provisionneurs intégrés de Kubernetes ne prennent pas en charge les opérations de redimensionnement de volumes pour les volumes persistants NFS, iSCSI ou FC pour le moment. Trident prend en charge l'extension des volumes NFS, iSCSI et FC.

Les détails de connexion du PV ne peuvent pas être modifiés après création.

#### Créer des instantanés de volume à la demande

Trident prend en charge la création à la demande d'instantanés de volumes et la création de PVC à partir d'instantanés grâce au framework CSI. Les instantanés constituent une méthode pratique pour conserver des copies des données à un instant précis et ont un cycle de vie indépendant du PV source dans Kubernetes. Ces instantanés peuvent être utilisés pour cloner des PVC.

#### Créer des volumes à partir d'instantanés

Trident prend également en charge la création de PersistentVolumes à partir d'instantanés de volume. Pour ce

faire, il suffit de créer un PersistentVolumeClaim et de mentionner l' `datasource`instantané requis à partir duquel le volume doit être créé. Trident gérera ce PVC en créant un volume avec les données présentes sur l'instantané. Grâce à cette fonctionnalité, il est possible de dupliquer des données entre régions, de créer des environnements de test, de remplacer intégralement un volume de production endommagé ou corrompu, ou de récupérer des fichiers et répertoires spécifiques et de les transférer vers un autre volume attaché.

**Déplacer les volumes dans le cluster**

Les administrateurs de stockage ont la possibilité de déplacer des volumes entre les agrégats et les contrôleurs dans le cluster ONTAP sans interruption pour le consommateur de stockage. Cette opération n'affecte pas Trident ni le cluster Kubernetes, tant que l'agrégat de destination est accessible par la SVM que Trident utilise. Il est important de noter que si l'agrégat a été nouvellement ajouté à la SVM, le backend devra être actualisé en le réajoutant à Trident. Cela déclenchera une réinvention de la SVM par Trident afin que le nouvel agrégat soit reconnu.

Cependant, le déplacement de volumes entre systèmes de stockage n'est pas pris en charge automatiquement par Trident. Cela inclut les SVM au sein d'un même cluster, entre clusters, ou vers une plateforme de stockage différente (même si ce système de stockage est connecté à Trident).

Si un volume est copié vers un autre emplacement, la fonctionnalité d'importation de volumes peut être utilisée pour importer les volumes actuels dans Trident.

**Étendre les volumes**

Trident prend en charge le redimensionnement des PV NFS, iSCSI et FC. Cela permet aux utilisateurs de redimensionner leurs volumes directement via la couche Kubernetes. L'expansion de volume est possible pour toutes les principales plateformes de stockage NetApp, y compris ONTAP, et les backends SolidFire/NetApp HCI. Pour permettre une expansion ultérieure, définissez `allowVolumeExpansion` sur `true` dans votre StorageClass associée au volume. Chaque fois que le volume persistant doit être redimensionné, modifiez l'annotation `spec.resources.requests.storage` dans la revendication de volume persistant à la taille de volume requise. Trident prendra automatiquement en charge le 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. Cette fonctionnalité est actuellement prise en charge par les `ontap-nas`, `ontap-nas-flexgroup`, `solidfire-san` et `azure-netapp-files` pilotes. Cette fonctionnalité est utile lors de la migration d'une application existante vers Kubernetes ou dans des scénarios de reprise après sinistre.

Lors de l'utilisation des pilotes ONTAP et `solidfire-san`, utilisez la commande `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` pour importer un volume existant dans Kubernetes afin qu'il soit géré par Trident. Le fichier PVC YAML ou JSON utilisé dans la commande d'importation de volume pointe vers une classe de stockage qui identifie Trident comme le provisionneur. Lorsque vous utilisez un backend NetApp HCI/SolidFire, assurez-vous que les noms de volumes sont uniques. Si les noms de volumes sont dupliqués, clonez le volume sous un nom unique afin que la fonctionnalité d'importation de volumes puisse les distinguer.

Si le `azure-netapp-files` driver est utilisé, utilisez la commande `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` pour importer le volume dans Kubernetes afin qu'il soit géré par Trident. Cela garantit une référence de volume unique.

Lorsque la commande ci-dessus est exécutée, Trident détecte le volume sur le backend et lit sa taille. Il ajoute automatiquement (et écrase si nécessaire) la taille du volume du PVC configuré. Trident crée ensuite le

nouveau PV et Kubernetes lie le PVC au PV.

Si un conteneur a été déployé de manière à nécessiter le PVC importé spécifique, il restera en attente jusqu'à ce que la paire PVC/PV soit liée via le processus d'importation de volume. Après la liaison de la paire PVC/PV, le conteneur devrait démarrer, à condition qu'il n'y ait pas d'autres problèmes.

### Service de registre

Le déploiement et la gestion du stockage pour le registre ont été documentés sur "netapp.io" dans le "blog".

### Service de journalisation

Comme les autres OpenShift services, le service de journalisation est déployé à l'aide d'Ansible avec des paramètres de configuration fournis par le fichier d'inventaire, également appelé hosts, fourni au playbook. Il existe deux méthodes d'installation qui seront abordées : le déploiement de la journalisation lors de l'installation initiale de OpenShift et le déploiement de la journalisation après que OpenShift a été installé.

À partir de la version 3.9 de Red Hat OpenShift, la documentation officielle déconseille l'utilisation de NFS pour le service de journalisation en raison de préoccupations concernant la corruption des données. Cette recommandation repose sur les tests effectués par Red Hat sur ses produits. Le serveur NFS ONTAP ne présente pas ces problèmes et peut facilement prendre en charge un déploiement de journalisation. En définitive, le choix du protocole pour le service de journalisation vous appartient, sachez simplement que les deux fonctionneront parfaitement avec les plateformes NetApp et qu'il n'y a aucune raison d'éviter NFS si c'est votre préférence.

Si vous choisissez d'utiliser NFS avec le service de journalisation, vous devrez définir la variable Ansible `openshift_enable_unsupported_configurations` sur `true` pour empêcher l'installateur d'échouer.

#### Commencer

Le service de journalisation peut, en option, être déployé à la fois pour les applications ainsi que pour les opérations principales du OpenShift cluster lui-même. 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 « ops », tandis que l'instance pour les applications ne les contient pas.

Il est important de configurer les variables Ansible en fonction de la méthode de déploiement afin de garantir que le stockage approprié est utilisé par les services sous-jacents. Examinons les options pour chacune des méthodes de déploiement.

Les tableaux ci-dessous ne contiennent que les variables pertinentes pour la configuration du stockage en lien avec le service de journalisation. Vous pouvez trouver d'autres options dans "Documentation de journalisation Red Hat OpenShift" qui doivent être examinées, configurées et utilisées en fonction de votre déploiement.

Les variables du tableau ci-dessous permettront au playbook Ansible de créer un PV et un PVC pour le service de journalisation en utilisant les informations fournies. Cette méthode est nettement moins flexible que l'utilisation du playbook d'installation du composant après l'installation de OpenShift, cependant, si vous disposez de volumes existants, c'est une option.

| Variable | Détails |
| --- | --- |
| `openshift_logging_storage_kind` | Définissez sur `nfs` pour que le programme d'installation crée un volume persistant NFS pour le service de journalisation. |
| `openshift_logging_storage_host` | Le nom d'hôte ou l'adresse IP de l'hôte NFS. Cela doit être défini sur la dataLIF de votre machine virtuelle. |
| `openshift_logging_storage_nfs_directory` | Chemin de montage pour l'export NFS. Par exemple, si le volume est monté comme `/openshift_logging`, vous utiliserez ce chemin pour cette variable. |
| `openshift_logging_storage_volume_name` | Le nom, par exemple `pv_ose_logs`, du PV à créer. |
| `openshift_logging_storage_volume_size` | La taille de l'export NFS, par exemple `100Gi`. |

Si votre OpenShift cluster est déjà en cours d'exécution, et que Trident est donc déployé et configuré, le programme d'installation peut utiliser le provisionnement dynamique pour créer les volumes. Les variables suivantes devront être configurées.

| Variable | Détails |
| --- | --- |
| `openshift_logging_es_pvc_dynamic` | Définissez sur true pour utiliser des volumes provisionnés dynamiquement. |
| `openshift_logging_es_pvc_storage_class_name` | Le nom de la classe de stockage qui sera utilisé dans le PVC. |
| `openshift_logging_es_pvc_size` | La taille du volume demandée dans le PVC. |
| `openshift_logging_es_pvc_prefix` | Un préfixe pour les PVC utilisés par le service de journalisation. |
| `openshift_logging_es_ops_pvc_dynamic` | Définissez sur `true` pour utiliser des volumes provisionnés dynamiquement pour l'instance de journalisation des opérations. |
| `openshift_logging_es_ops_pvc_storage_class_name` | Le nom de la classe de stockage pour l'instance de journalisation des opérations. |
| `openshift_logging_es_ops_pvc_size` | La taille de la requête de volume pour l'instance ops. |
| `openshift_logging_es_ops_pvc_prefix` | Un préfixe pour les PVC d'instance ops. |

#### Déployez la pile de journalisation

Si vous déployez la journalisation dans le cadre du processus d'installation initiale de OpenShift, il vous suffit de suivre la procédure de déploiement standard. Ansible configurera et déploiera les services et objets OpenShift nécessaires pour que le service soit disponible dès qu'Ansible a terminé.

Toutefois, si vous effectuez un déploiement après l'installation initiale, le playbook du composant devra être utilisé par Ansible. Ce processus peut légèrement varier selon les différentes versions de OpenShift, alors assurez-vous de lire et de suivre "Documentation de Red Hat OpenShift Container Platform 3.11" pour votre version.

## Service de métriques

Le service de métriques fournit à l'administrateur des informations précieuses concernant l'état, l'utilisation des ressources et la disponibilité du OpenShift cluster. Il est également nécessaire pour la fonctionnalité d'auto-scaling des pods et de nombreuses organisations utilisent les données du service de métriques pour leurs applications de refacturation et/ou de transparence des coûts.

Comme pour le service de journalisation, et OpenShift dans son ensemble, Ansible est utilisé pour déployer le service de métriques. De même que pour le service de journalisation, le service de métriques peut être déployé lors de la configuration initiale du cluster ou après sa mise en service en utilisant la méthode d'installation des composants. Les tableaux suivants contiennent les variables qui sont importantes lors de la configuration du stockage persistant pour le service de métriques.

Les tableaux ci-dessous ne contiennent que les variables pertinentes pour la configuration du stockage en lien avec le service de métriques. De nombreuses autres options sont décrites dans la documentation, qui doivent être examinées, configurées et utilisées selon votre déploiement.

| Variable | Détails |
|---|---|
| `openshift_metrics_storage_kind` | Définissez sur `nfs` pour que le programme d'installation crée un volume persistant NFS pour le service de journalisation. |
| `openshift_metrics_storage_host` | Le nom d'hôte ou l'adresse IP de l'hôte NFS. Cela doit être défini sur la dataLIF de votre SVM. |
| `openshift_metrics_storage_nfs_directory` | Chemin de montage pour l'export NFS. Par exemple, si le volume est monté comme `/openshift_metrics`, vous utiliserez ce chemin pour cette variable. |
| `openshift_metrics_storage_volume_name` | Le nom, par exemple `pv_ose_metrics`, du PV à créer. |
| `openshift_metrics_storage_volume_size` | La taille de l'export NFS, par exemple `100Gi`. |

Si votre OpenShift cluster est déjà en cours d'exécution, et que Trident est donc déployé et configuré, le programme d'installation peut utiliser le provisionnement dynamique pour créer les volumes. Les variables suivantes devront être configurées.

| Variable | Détails |
|---|---|
| `openshift_metrics_cassandra_pvc_prefix` | Un préfixe à utiliser pour les PVC de métriques. |
| `openshift_metrics_cassandra_pvc_size` | La taille des volumes à demander. |
| `openshift_metrics_cassandra_storage_type` | Le type de stockage à utiliser pour les métriques, cela doit être défini sur dynamique pour qu'Ansible puisse créer des PVC avec la classe de stockage appropriée. |
| `openshift_metrics_cassanda_pvc_storage_class_name` | Le nom de la classe de stockage à utiliser. |

#### Déployez le service de métriques

Une fois les variables Ansible appropriées définies dans votre fichier hosts/inventory, déployez le service à l'aide d'Ansible. Si vous effectuez le déploiement au moment de l'installation de OpenShift, alors le PV sera créé et utilisé automatiquement. Si vous déployez à l'aide des playbooks de composants, après l'installation de OpenShift, alors Ansible crée les PVC nécessaires et, après que Trident a provisionné le stockage pour eux, déploie le service.

Les variables ci-dessus, ainsi que le processus de déploiement, peuvent changer avec chaque version de OpenShift. Assurez-vous de consulter et de suivre "Guide de déploiement OpenShift de Red Hat" pour votre version afin qu'elle soit configurée pour votre environnement.

# Protection des données et reprise après sinistre

Découvrez les options de protection et de récupération pour Trident et les volumes créés avec Trident. Vous devez disposer d'une stratégie de protection des données et de récupération pour chaque application nécessitant une persistance.

## Réplication et récupération de Trident

Vous pouvez créer une sauvegarde pour restaurer Trident en cas de sinistre.

#### Réplication Trident

Trident utilise les 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 en utilisant "Kubernetes : sauvegarde d'un cluster etcd".
2. Placez les fichiers de sauvegarde sur un volume FlexVol

> NetApp recommande de protéger la SVM où le volume FlexVol réside avec une relation SnapMirror vers une autre SVM.

#### Récupération de Trident

En utilisant les CRD Kubernetes et l'instantané etcd du cluster Kubernetes, vous pouvez récupérer Trident.

#### Étapes

1. Depuis la SVM de destination, montez le volume qui contient les fichiers de données etcd de Kubernetes et les certificats sur l'hôte qui sera configuré comme nœud maître.
2. Copiez tous les certificats requis relatifs au 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 en utilisant "Kubernetes : restauration d'un cluster etcd".
4. Exécutez `kubectl get crd` pour vérifier que toutes les ressources personnalisées Trident sont opérationnelles et récupérez les objets Trident pour vérifier que toutes les données sont disponibles.

## Réplication et récupération de SVM

Trident ne peut pas configurer les relations de réplication, cependant, l'administrateur de stockage peut utiliser "ONTAP SnapMirror" pour répliquer une SVM.

En cas de sinistre, vous pouvez activer le SVM de destination SnapMirror pour commencer à servir les données. Vous pouvez revenir au SVM principal une fois les systèmes rétablis.

### À propos de cette tâche

Tenez compte des points suivants lors de l'utilisation de la fonctionnalité de réplication SVM SnapMirror :

- Vous devez créer un backend distinct pour chaque SVM avec SVM-DR activé.
- Configurez les classes de stockage pour sélectionner les backends répliqués uniquement lorsque cela est nécessaire afin d'éviter que des volumes qui n'ont pas besoin de réplication soient provisionnés sur les backends qui prennent en charge SVM-DR.
- Les administrateurs d'applications doivent comprendre les coûts et la complexité supplémentaires associés à la réplication et examiner attentivement leur plan de reprise avant de commencer ce processus.

### Réplication SVM

Vous pouvez utiliser "ONTAP : SnapMirror réplication SVM" pour créer la relation de réplication SVM.

SnapMirror vous permet de définir des options pour contrôler ce qui doit être répliqué. Vous devrez connaître les options que vous avez sélectionnées lors de l'exécution Récupération SVM à l'aide de Trident.

- "-identity-preserve true"réplique l'intégralité de la configuration SVM.
- "-discard-configs réseau" exclut les LIF et les paramètres réseau associés.
- "-identity-preserve false" Réplique uniquement les volumes et la configuration de sécurité.

### Récupération SVM à l'aide de Trident

Trident ne détecte pas automatiquement les pannes de SVM. En cas de sinistre, l'administrateur peut déclencher manuellement le basculement de Trident vers le nouveau SVM.

### Étapes

1. Annulez les transferts SnapMirror planifiés et en cours, interrompez la relation de réplication, arrêtez la SVM source puis activez la SVM de destination SnapMirror.
2. Si vous avez spécifié `-identity-preserve false` ou `-discard-config network` lors de la configuration de votre réplication SVM, mettez à jour `managementLIF` et `dataLIF` dans le fichier de définition du backend Trident.
3. Confirmer `storagePrefix` est présent dans le fichier de définition du backend Trident. Ce paramètre ne peut pas être modifié. Omettre `storagePrefix` entraînera l'échec de la mise à jour du backend.
4. Mettez à jour tous les backends requis pour refléter le nouveau nom de la SVM de destination en utilisant :

```
./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 redémarrer tous les pods d'application.

Si vous avez spécifié `-identity-preserve true`, tous les volumes provisionnés par Trident commencent à servir des données lorsque le SVM de destination est activé.

### Réplication et récupération de volume

Trident ne peut pas configurer les relations de réplication SnapMirror, cependant, l'administrateur de stockage peut utiliser "Réplication et récupération ONTAP SnapMirror" pour répliquer les volumes créés par Trident.

Vous pouvez ensuite importer les volumes récupérés dans Trident en utilisant "tridentctl volume import".

L'importation n'est pas prise en charge sur `ontap-nas-economy`, `ontap-san-economy`, ou `ontap-flexgroup-economy` pilotes.

### protection des données Snapshot

Vous pouvez protéger et restaurer des données à l'aide de :

- Un contrôleur de snapshots externe et des CRD pour créer des snapshots de volumes persistants (PVs) Kubernetes.

  "Instantanés de volume"

- Utilisez les snapshots ONTAP pour restaurer l'intégralité du contenu d'un volume ou pour récupérer des fichiers ou des LUN individuels.

  "Instantanés ONTAP"

# Automatisation du basculement des applications avec état avec Trident

La fonctionnalité de détachement forcé de Trident permet de détacher automatiquement les volumes des nœuds défaillants d'un cluster Kubernetes, évitant ainsi la corruption des données et garantissant la disponibilité des applications. Cette fonctionnalité est particulièrement utile dans les scénarios où des nœuds deviennent indisponibles ou sont mis hors ligne pour maintenance.

### Détails concernant le détachement forcé

Le détachement forcé est disponible pour `ontap-san`, `ontap-san-economy`, `ontap-nas` et `ontap-nas-economy` uniquement. Avant d'activer le détachement forcé, l'arrêt brutal des nœuds (NGNS) doit être activé sur le cluster Kubernetes. NGNS est activé par défaut pour Kubernetes 1.28 et versions ultérieures. Pour plus d'informations, consultez "Kubernetes : arrêt non gracieux d'un nœud".

Lorsque vous utilisez le `ontap-nas` ou `ontap-nas-economy` pilote, vous devez définir le paramètre `autoExportPolicy` dans la configuration du backend sur `true` afin que Trident puisse restreindre l'accès depuis le nœud Kubernetes avec la contamination appliquée à l'aide de politiques d'exportation gérées.

Étant donné que Trident repose sur Kubernetes NGNS, ne supprimez pas `out-of-service` les taints d'un nœud défaillant tant que toutes les charges de travail non tolérables n'ont pas été reprogrammées. Appliquer ou supprimer le taint sans précaution peut compromettre la protection des données du backend.

Lorsque l'administrateur du cluster Kubernetes a appliqué la `node.kubernetes.io/out-of-service=nodeshutdown:NoExecute`taint au nœud et `enableForceDetach`est définie sur `true`, Trident déterminera l'état du nœud et :

1. Arrêtez l'accès E/S du backend pour les volumes montés sur ce nœud.
2. Marquez l'objet nœud Trident comme `dirty` (non sûr pour les nouvelles publications).

Le contrôleur Trident refusera les nouvelles demandes de publication de volumes tant que le nœud n'aura pas été requalifié (après avoir été marqué comme `dirty`) par le pod Trident du nœud. Les charges de travail planifiées avec un PVC monté (même après que le nœud de cluster soit opérationnel et prêt) ne seront pas acceptées tant que Trident ne peut pas vérifier le nœud `clean` (sécurisé pour de nouvelles publications).

Lorsque l'intégrité du nœud est rétablie et que la contamination est supprimée, Trident :

1. Identifiez et nettoyez les chemins publiés obsolètes sur le nœud.
2. Si le nœud est dans un `cleanable` état (la contamination hors service a été supprimée et le nœud est dans un `Ready` état) et que tous les chemins publiés obsolètes sont propres, Trident réadmettra le nœud en `clean` et autorisera de nouveaux volumes publiés sur le nœud.

## Détails sur le basculement automatique

Vous pouvez automatiser le processus de déconnexion forcée grâce à l'intégration avec "opérateur de vérification de l'état des nœuds (NHC)". Lorsqu'une défaillance de nœud se produit, NHC déclenche la remédiation du nœud Trident (TNR) et la déconnexion forcée automatiquement en créant un CR TridentNodeRemediation dans l'espace de noms de Trident, définissant le nœud défaillant. La TNR est créée uniquement lors d'une défaillance de nœud et supprimée par NHC une fois que le nœud est remis en ligne ou supprimé.

### Échec du processus de suppression du pod du nœud

Le basculement automatique sélectionne les charges de travail à retirer du nœud défaillant. Lorsqu'un TNR est créé, le contrôleur TNR marque le nœud comme sale, empêchant toute nouvelle publication de volume et commence à supprimer les pods compatibles avec le détachement forcé ainsi que leurs attachements de volumes.

Tous les volumes/PVC pris en charge par force-detach sont pris en charge par automated-failover :

- Volumes NAS et NAS-economy utilisant des politiques d'auto-exportation (SMB n'est pas encore pris en charge).
- Volumes SAN et SAN-economy.

Consultez Détails concernant le détachement forcé.

**Comportement par défaut**:

- Les pods utilisant des volumes compatibles avec le détachement forcé sont supprimés du nœud défaillant. Kubernetes les reprogrammera sur un nœud sain.
- Les pods utilisant un volume non pris en charge par le force-detach, y compris les volumes non-Trident, ne sont pas supprimés du nœud défaillant.
- Les pods sans état (et non les PVC) ne sont pas supprimés du nœud défaillant, sauf si l'annotation du pod `trident.netapp.io/podRemediationPolicy: delete` est définie.

**Remplacement du comportement de suppression des pods** :

Le comportement de suppression des pods peut être personnalisé à l'aide d'une annotation : `trident.netapp.io/podRemediationPolicy[retain, delete]`. Ces annotations sont examinées et utilisées lors d'un basculement. Appliquez des annotations à la spécification du pod du déploiement/replicaset Kubernetes pour éviter que l'annotation ne disparaisse après un basculement :

- `retain` - Le pod ne sera PAS supprimé du nœud défaillant lors d'un basculement automatique.
- `delete` - Le pod sera supprimé du nœud défaillant lors d'un basculement automatique.

Ces annotations peuvent être appliquées à n'importe quel pod.

- Les opérations d'E/S seront bloquées uniquement sur les nœuds défaillants pour les volumes prenant en charge force-detach.
- Pour les volumes qui ne prennent pas en charge le détachement forcé, il existe un risque de corruption des données et de problèmes de multi-connexion.

**CR TridentNodeRemediation**

Le TridentNodeRemediation (TNR) CR définit un nœud défaillant. Le nom du TNR est le nom du nœud défaillant.

**Exemple de TNR**:

```
apiVersion: trident.netapp.io/v1
kind: TridentNodeRemediation
metadata:
  name: <K8s-node-name>
spec: {}
```

**États TNR** : Utilisez les commandes suivantes pour afficher l'état des TNR :
`kubectl get tnr <name> -n <trident-namespace>`

Les TNR peuvent se trouver dans l'un des états suivants :

- *Remédiation* :
  - Cessez l'accès aux E/S du backend pour les volumes pris en charge par force-detach montés sur ce nœud.
  - L'objet nœud Trident est marqué comme sale (non sûr pour les nouvelles publications).
  - Supprimez les pods et les attachements de volumes du nœud

- *Récupération du nœud en attente*:
  - Le contrôleur attend que le nœud soit de nouveau en ligne.
  - Une fois le nœud en ligne, publish-enforcement garantira que le nœud est propre et prêt pour de nouvelles publications de volumes.
- Si le nœud est supprimé de K8s, le contrôleur TNR supprimera le TNR et cessera la réconciliation.
- *Réussi*:
  - Toutes les étapes de correction et de récupération du nœud ont été réalisées avec succès. Le nœud est propre et prêt pour la publication de nouveaux volumes.
- *Échec* :
  - Erreur irrécupérable. Les raisons de l'erreur sont indiquées dans le champ status.message de la CR.

**Activation du basculement automatique**

**Prérequis** :

- Assurez-vous que le détachement forcé est activé avant d'activer le basculement automatique. Pour plus d'informations, consultez Détails concernant le détachement forcé.
- Installez la vérification de l'état (NHC) dans le cluster Kubernetes.
  - "Installer operator-sdk".
  - Installez Operator Lifecycle Manager (OLM) dans le cluster s'il n'est pas déjà installé : `operator-sdk olm install`.
  - Installer l'opérateur de vérification de l'état du nœud `kubectl create -f https://operatorhub.io/install/node-healthcheck-operator.yaml`.

> Vous pouvez également utiliser d'autres méthodes pour détecter les défaillances de nœud, comme spécifié dans la section [Integrating Custom Node Health Check Solutions] ci-dessous.

Voir "Opérateur de vérification de l'état des nœuds" pour plus d'informations.

**Étapes**

1. Créez une ressource personnalisée NodeHealthCheck (NHC) dans l'espace de noms Trident pour surveiller les nœuds de travail du cluster. Exemple :

```
apiVersion: remediation.medik8s.io/v1alpha1
kind: NodeHealthCheck
metadata:
  name: <CR name>
spec:
  selector:
    matchExpressions:
      - key: node-role.kubernetes.io/control-plane
        operator: DoesNotExist
      - key: node-role.kubernetes.io/master
        operator: DoesNotExist
  remediationTemplate:
    apiVersion: trident.netapp.io/v1
    kind: TridentNodeRemediationTemplate
    namespace: <Trident installation namespace>
    name: trident-node-remediation-template
  minHealthy: 0 # Trigger force-detach upon one or more node failures
  unhealthyConditions:
    - type: Ready
      status: "False"
      duration: 0s
    - type: Ready
      status: Unknown
      duration: 0s
```

2. Appliquez le CR de vérification de l'état du nœud dans l'espace de noms `trident`.

```
kubectl apply -f <nhc-cr-file>.yaml -n <trident-namespace>
```

La ressource personnalisée (CR) ci-dessus est configurée pour surveiller les nœuds de travail K8s et détecter les états Ready: false et Unknown. Automated-Failover sera déclenché lorsqu'un nœud passe à l'état Ready: false ou Ready: Unknown.

Le `unhealthyConditions` dans le CR utilise un délai de grâce de 0 seconde. Cela provoque un basculement automatique immédiat dès que K8s définit la condition Ready : false, ce qui se produit après que K8s a perdu le signal de présence d'un nœud. K8s attend par défaut 40 secondes après le dernier signal de présence avant de définir Ready : false. Ce délai de grâce peut être personnalisé dans les options de déploiement de K8s.

Pour plus d'options de configuration, veuillez vous référer à "Documentation de l'opérateur Node-Healthcheck-Operator".

**Informations de configuration supplémentaires**

Lorsque Trident est installé avec le détachement forcé activé, deux ressources supplémentaires sont automatiquement créées dans l'espace de noms Trident pour faciliter l'intégration avec NHC : TridentNodeRemediationTemplate (TNRT) et ClusterRole.

**TridentNodeRemediationTemplate (TNRT)** :

Le TNRT sert de modèle au contrôleur NHC, qui utilise TNRT pour générer des ressources TNR selon les besoins.

```
apiVersion: trident.netapp.io/v1
kind: TridentNodeRemediationTemplate
metadata:
  name: trident-node-remediation-template
  namespace: trident
spec:
  template:
    spec: {}
```

**ClusterRole** :

Un rôle de cluster est également ajouté lors de l'installation lorsque le détachement forcé est activé. Cela donne à NHC les autorisations pour les TNR dans l'espace de noms Trident.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  labels:
    rbac.ext-remediation/aggregate-to-ext-remediation: "true"
  name: tridentnoderemediation-access
rules:
- apiGroups:
  - trident.netapp.io
  resources:
  - tridentnoderemediationtemplates
  - tridentnoderemediations
  verbs:
  - get
  - list
  - watch
  - create
  - update
  - patch
  - delete
```

**Mises à niveau et maintenance des clusters K8s**

Pour éviter tout basculement, suspendez le basculement automatique pendant la maintenance ou la mise à niveau de K8s, lorsque les nœuds doivent être arrêtés ou redémarrés. Vous pouvez suspendre le CR NHC (décrit ci-dessus) en modifiant son CR :

```
kubectl patch NodeHealthCheck <cr-name> --patch
'{"spec":{"pauseRequests":["<description-for-reason-of-pause>"]}}' --type=merge
```

Cela suspend le basculement automatique. Pour réactiver le basculement automatique, supprimez le pauseRequests de la spécification après la fin de la maintenance.

#### Limitations

- Les opérations d'E/S sont bloquées uniquement sur les nœuds défaillants pour les volumes pris en charge par force-detach. Seuls les pods utilisant des volumes/PVCs pris en charge par force-detach sont automatiquement supprimés.
- Le basculement automatique et le détachement forcé s'exécutent au sein du pod trident-controller. Si le nœud hébergeant trident-controller tombe en panne, le basculement automatique sera différé jusqu'à ce que K8s déplace le pod vers un nœud sain.

#### Intégration de solutions personnalisées de vérification de l'état des nœuds

Vous pouvez remplacer Node Healthcheck Operator par d'autres outils de détection des pannes de nœuds pour déclencher un basculement automatique. Pour garantir la compatibilité avec le mécanisme de basculement automatique, votre solution personnalisée doit :

- Créez un TNR lorsqu'une défaillance de nœud est détectée, en utilisant le nom du nœud défaillant comme nom du CR TNR.
- Supprimez le TNR lorsque le nœud a récupéré et que le TNR est à l'état Succeeded.

# Sécurité

## Sécurité

Utilisez les recommandations listées ici pour garantir que votre installation Trident est sécurisée.

#### Exécutez 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 Trident ou aux pods afin de garantir un stockage fiable et de bloquer toute activité malveillante potentielle.

Pour séparer les autres applications et utilisateurs de Trident, installez toujours Trident dans son propre espace de noms Kubernetes (`trident`). Mettre Trident dans son propre espace de noms garantit que seul le personnel administratif de Kubernetes a accès au pod Trident et aux artefacts (tels que les secrets backend et CHAP, le cas échéant) stockés dans les objets CRD de l'espace de noms. Vous devez vous assurer que seuls les administrateurs ont accès à l'espace de noms Trident et donc à l'application `tridentctl`.

#### Utilisez l'authentification CHAP avec les backends SAN ONTAP

Trident prend en charge l'authentification CHAP pour les charges de travail ONTAP SAN (à l'aide des pilotes `ontap-san` et `ontap-san-economy`). NetApp recommande d'utiliser l'authentification CHAP bidirectionnelle avec Trident pour l'authentification entre un hôte et le système de stockage.

Pour les backends ONTAP qui utilisent les pilotes de stockage SAN, Trident peut configurer le CHAP bidirectionnel et gérer les noms d'utilisateur et les secrets CHAP via `tridentctl`. Reportez-vous à

"Préparez-vous à configurer le backend avec les pilotes SAN ONTAP" pour comprendre comment Trident configure CHAP sur les backends ONTAP.

#### Utilisez l'authentification CHAP avec NetApp HCI et SolidFire backends

NetApp recommande de déployer CHAP bidirectionnel pour garantir l'authentification entre un hôte et les backends NetApp HCI et SolidFire. Trident utilise un objet secret qui inclut deux mots de passe CHAP par locataire. Lorsque Trident est installé, il gère les secrets CHAP et les stocke dans un objet CR `tridentvolume` pour le PV respectif. Lorsque vous créez un PV, Trident utilise les secrets CHAP pour initier une session iSCSI et communiquer avec le système NetApp HCI et SolidFire via CHAP.

Les volumes créés par Trident ne sont associés à aucun Volume Access Group.

#### Utilisez Trident avec NVE et NAE

NetApp ONTAP assure le chiffrement des données au repos afin de protéger les données sensibles en cas de vol, de retour ou de réutilisation d'un disque. Pour plus de détails, consultez "Configurer l'aperçu du chiffrement des volumes NetApp".

- Si NAE est activé sur le backend, tout volume provisionné dans Trident sera activé NAE.
  - Vous pouvez définir le indicateur de chiffrement NVE sur `""` pour créer des volumes compatibles NAE.
- Si NAE n'est pas activé sur le backend, tout volume provisionné dans Trident sera activé NVE à moins que l'indicateur de chiffrement NVE ne soit défini sur `false` (la valeur par défaut) dans la configuration du backend.

Les volumes créés dans Trident sur un backend activé NAE doivent être chiffrés NVE ou NAE.

- Vous pouvez définir le indicateur de chiffrement NVE sur `true` dans la configuration du backend Trident pour remplacer le chiffrement NAE et utiliser une clé de chiffrement spécifique pour chaque volume.
- Définir le drapeau de chiffrement NVE sur `false` sur un backend activé NAE crée un volume activé NAE. Vous ne pouvez pas désactiver le chiffrement NAE en définissant le drapeau de chiffrement NVE sur `false`.

- Vous pouvez créer manuellement un volume NVE dans Trident en définissant explicitement le indicateur de chiffrement NVE sur `true`.

Pour plus d'informations sur les options de configuration du backend, consultez :

- "Options de configuration SAN ONTAP"
- "Options de configuration NAS ONTAP"

## Linux Unified Key Setup (LUKS)

Vous pouvez activer Linux Unified Key Setup (LUKS) pour chiffrer les volumes ONTAP SAN et ONTAP SAN ECONOMY sur Trident. Trident prend en charge la rotation des phrases de passe et l'extension de volume pour les volumes chiffrés avec LUKS.

Dans Trident, les volumes chiffrés LUKS utilisent le cypher et le mode aes-xts-plain64, comme recommandé par "NIST".

Le chiffrement LUKS n'est pas pris en charge pour les systèmes ASA r2. Pour des informations sur les systèmes ASA r2, voir "En savoir plus sur les systèmes de stockage ASA r2".

**Avant de commencer**

- Les nœuds de travail doivent avoir cryptsetup 2.1 ou une version supérieure (mais inférieure à 3.0) installée. Pour plus d'informations, consultez "Gitlab : cryptsetup".
- Pour des raisons de performance, NetApp recommande que les nœuds de travail prennent en charge Advanced Encryption Standard New Instructions (AES-NI). Pour vérifier la prise en charge d'AES-NI, exécutez la commande suivante :

```
grep "aes" /proc/cpuinfo
```

Si aucune réponse n'est renvoyée, votre processeur ne prend pas en charge AES-NI. Pour plus d'informations sur AES-NI, visitez : "Intel: Instructions Advanced Encryption Standard (AES-NI)".

### Activer le chiffrement LUKS

Vous pouvez activer le chiffrement par volume, côté hôte, à l'aide de Linux Unified Key Setup (LUKS) pour les volumes ONTAP SAN et ONTAP SAN ECONOMY.

**Étapes**

1. Définissez les attributs de chiffrement LUKS dans la configuration du backend. Pour plus d'informations sur les options de configuration du backend pour ONTAP SAN, consultez "Options de configuration SAN ONTAP".

```
{
  "storage": [
    {
      "labels": {
        "luks": "true"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "true"
      }
    },
    {
      "labels": {
        "luks": "false"
      },
      "zone": "us_east_1a",
      "defaults": {
        "luksEncryption": "false"
      }
    }
  ]
}
```

2. Utilisez `parameters.selector` pour définir les pools de stockage utilisant le chiffrement 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
```

#### Limitations

Les volumes chiffrés LUKS ne peuvent pas bénéficier de la déduplication et de la compression ONTAP.

### Configuration du backend pour l'importation des volumes LUKS

Pour importer un volume LUKS, vous devez définir `luksEncryption` sur (`true` dans le backend. L' `luksEncryption`option indique à Trident si le volume est conforme LUKS (`true`) ou non conforme LUKS (`false`), comme illustré 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 dynamiquement des volumes LUKS, définissez l'annotation `trident.netapp.io/luksEncryption` sur `true` et incluez une classe de stockage compatible LUKS dans le PVC 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
```

### Faire pivoter une phrase de passe LUKS

Vous pouvez faire pivoter la phrase de passe LUKS et confirmer la rotation.

> N'oubliez pas votre phrase de passe tant que vous n'avez pas vérifié qu'elle n'est plus utilisée par aucun volume, instantané ou secret. Si une phrase de passe référencée est perdue, vous pourriez être dans l'incapacité de monter le volume et les données resteront chiffrées et inaccessibles.

#### À propos de cette tâche

La rotation de la phrase de passe LUKS a lieu lorsqu'un pod qui monte le volume est créé après la spécification d'une nouvelle phrase de passe LUKS. Lorsqu'un nouveau pod est créé, Trident compare la phrase de passe LUKS du volume à la phrase de passe active dans le secret.

- Si la phrase de passe sur le volume ne correspond pas à la phrase de passe active dans le secret, une rotation a lieu.
- 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` et `node-publish-secret-namespace` paramètres 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. Identifiez les phrases de passe existantes sur le volume ou le snapshot.

**Volume**

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["A"]
```

**Instantané**

```
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 du volume en spécifiant la nouvelle et l'ancienne phrase de passe. Assurez-vous que `previous-luke-passphrase-name` et `previous-luks-passphrase` correspondent à la phrase de passe précédente.

```
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 en montant le volume. Ceci est nécessaire pour initier la rotation.
5. Vérifiez que la phrase de passe a été modifiée.

**Volume**

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["B"]
```

**Instantané**

```
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 renouvelée lorsque seule la nouvelle phrase de passe est renvoyée sur le volume et l'instantané.

> 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'expansion du volume

Vous pouvez activer l'extension de volume sur un volume chiffré LUKS.

### Étapes

1. Activez la `CSINodeExpandSecret` feature gate (bêta 1.25+). Consultez "Kubernetes 1.25 : Utilisez des secrets pour l'extension des volumes CSI pilotée par les nœuds" pour plus de détails.
2. Ajoutez les `node-expand-secret-name` et `node-expand-secret-namespace` paramètres 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 lancez une extension de stockage en ligne, le kubelet transmet les informations d'identification appropriées au driver.

## Chiffrement Kerberos en vol

En utilisant le chiffrement Kerberos in-flight, vous pouvez améliorer la sécurité d'accès aux données en activant le chiffrement pour le trafic entre votre cluster géré et le stockage backend.

Trident prend en charge le chiffrement Kerberos pour ONTAP en tant que backend de stockage :

- **On-premise ONTAP** - Trident prend en charge le chiffrement Kerberos sur les connexions NFSv3 et NFSv4 depuis Red Hat OpenShift et les clusters Kubernetes en amont vers les volumes ONTAP sur site.

Vous pouvez créer, supprimer, redimensionner, prendre un instantané, cloner, cloner en lecture seule et importer des volumes qui utilisent le chiffrement NFS.

### Configurer le chiffrement Kerberos en transit avec les volumes ONTAP sur site

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un système de stockage ONTAP sur site.

> Le chiffrement Kerberos pour le trafic NFS avec des backends de stockage ONTAP sur site n'est pris en charge qu'à l'aide du `ontap-nas` storage driver.

**Avant de commencer**

- Assurez-vous d'avoir accès à l' `tridentctl`utilitaire.
- Assurez-vous de disposer d'un accès administrateur au système de stockage ONTAP.
- Assurez-vous de connaître le nom du ou des volumes que vous partagerez depuis le stockage backend ONTAP.
- Assurez-vous d'avoir préparé la machine virtuelle de stockage ONTAP pour prendre en charge le chiffrement Kerberos pour les volumes NFS. Consultez "Activer Kerberos sur une dataLIF" pour obtenir des instructions.
- Assurez-vous que tous les volumes NFSv4 que vous utilisez avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section « Configuration du domaine NFSv4 » (page 13) de NetApp "NetApp NFSv4 : améliorations et guide des bonnes pratiques".

#### Ajouter ou modifier les règles d'export ONTAP

Vous devez ajouter des règles aux règles d'export ONTAP existantes ou créer de nouvelles règles d'export prenant en charge le chiffrement Kerberos pour le volume racine de la machine virtuelle de stockage ONTAP, ainsi que pour tous les volumes ONTAP partagés avec le cluster Kubernetes en amont. Les règles d'export que vous ajoutez, ou les nouvelles règles d'export que vous créez, doivent prendre en charge les protocoles d'accès et les autorisations d'accès suivants :

**Protocoles d'accès**

Configurez la règle d'export avec les protocoles d'accès NFS, NFSv3 et NFSv4.

**Détails d'accès**

Vous pouvez configurer l'une des trois versions différentes du chiffrement Kerberos, en fonction de vos

besoins pour le volume :

- **Kerberos 5** - (authentification et chiffrement)
- **Kerberos 5i** - (authentification et chiffrement avec protection de l'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 doivent monter les volumes NFS avec un mélange de chiffrement 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 |

Consultez la documentation suivante pour savoir comment créer des règles d'export ONTAP et des règles de règles d'export :

- "Créer une règles d'export"
- "Ajouter une règle à une règle d'export"

#### Créer un backend de stockage

Vous pouvez créer une configuration de stockage Trident qui inclut la capacité de chiffrement Kerberos.

**À propos de cette tâche**

Lorsque vous créez un fichier de configuration du 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 vie privée)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de chiffrement Kerberos dans la liste des paramètres, seule la première option est utilisée.

**Étapes**

1. Sur le cluster géré, créez un fichier de configuration du backend de stockage en utilisant l'exemple suivant. Remplacez les valeurs entre crochets <> avec 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 backend échoue, cela signifie qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour en 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 à nouveau la commande create.

#### Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec chiffrement Kerberos.

**À propos de cette tâche**

Lorsque vous créez un objet de 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 vie privée)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de chiffrement 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 backend de stockage est différent de celui que vous spécifiez dans l'objet de classe de stockage, l'objet de classe de stockage prévaut.

**Étapes**

1. Créez un objet Kubernetes StorageClass en utilisant 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 devriez voir une sortie similaire à la suivante :

```
NAME          PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

#### Approvisionner des volumes

Après avoir créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour obtenir des instructions, consultez "Provisionner un volume".

### Configurer le chiffrement Kerberos en transit avec les volumes Azure NetApp Files

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un seul backend de stockage Azure NetApp Files ou un pool virtuel de backends de stockage Azure NetApp Files.

#### Avant de commencer

- Assurez-vous d'avoir activé Trident sur le cluster Red Hat OpenShift géré.
- Assurez-vous d'avoir accès à l' `tridentctl`utilitaire.
- Assurez-vous d'avoir préparé le stockage Azure NetApp Files pour le chiffrement Kerberos en prenant note des exigences et en suivant les instructions dans "Documentation Azure NetApp Files".
- Assurez-vous que tous les volumes NFSv4 que vous utilisez avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section « Configuration du domaine NFSv4 » (page 13) de NetApp "NetApp NFSv4 : améliorations et guide des bonnes pratiques".

#### Créer un backend de stockage

Vous pouvez créer une configuration de stockage backend Azure NetApp Files qui inclut la capacité de chiffrement Kerberos.

#### À propos de cette tâche

Lorsque vous créez un fichier de configuration de stockage qui configure le chiffrement Kerberos, vous pouvez le définir de sorte qu'il soit appliqué à l'un des deux niveaux possibles :

- Le **niveau du backend de stockage** utilisant le `spec.kerberos` champ
- Le **niveau de pool virtuel** utilisant le champ `spec.storage.kerberos`

Lorsque vous définissez la configuration au niveau du pool virtuel, le pool est sélectionné à l'aide de l'étiquette dans la classe de stockage.

À chaque niveau, vous pouvez spécifier l'une des trois versions différentes du chiffrement 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 vie privée)

#### Étapes

1. Sur le cluster géré, créez un fichier de configuration du backend de stockage en utilisant l'un des exemples suivants, selon l'endroit où vous devez définir le backend de stockage (au niveau du backend de stockage ou au niveau du pool virtuel). Remplacez les valeurs entre crochets <> avec les informations de votre environnement :

**Exemple de niveau de backend 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 niveau 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 backend échoue, cela signifie qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour en 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 à nouveau la commande create.

#### Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec chiffrement Kerberos.

**Étapes**

1. Créez un objet Kubernetes StorageClass en utilisant 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 devriez voir une sortie similaire à la suivante :

```
NAME          PROVISIONER             AGE
sc-nfs        csi.trident.netapp.io   15h
```

#### Approvisionner des volumes

Après avoir créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour obtenir des instructions, consultez "Provisionner un volume".

## Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU 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.