Meilleures pratiques et recommandations

Trident

NetApp
January 15, 2026

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"Elles assurent une séparation administrative entre les différentes applications et constituent un obstacle 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 par conséquent un compte de service disposant de privilèges élevés.

De plus, l'accès au module Trident pourrait permettre à un utilisateur d'accéder aux identifiants du système de stockage et à d'autres informations sensibles. Il est important de veiller à ce que les utilisateurs de l'application et les applications de gestion n'aient pas la possibilité d'accéder aux définitions d'objets Trident ni aux pods eux-mêmes.

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

Kubernetes possède deux fonctionnalités qui, combinées, constituent un mécanisme puissant pour limiter la consommation de ressources par les applications. Le "mécanisme de quotas de stockage" permet à l'administrateur de mettre en œuvre des limites de consommation de capacité et de nombre d'objets globales et spécifiques à la classe de stockage, sur une base d'espace de noms. De plus, en utilisant un "limite de portée" garantit que les demandes de PVC respectent une valeur minimale et maximale avant d'être transmises au fournisseur.

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. Consultez cette page pour obtenir des informations sur "comment tirer parti des quotas" .

Configuration de stockage

Chaque plateforme de stockage du portefeuille NetApp possède des capacités uniques qui profitent aux applications, conteneurisées ou non.

Présentation de la plateforme

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

Vous devez suivre les bonnes pratiques de base pour le système d'exploitation hôte avec le protocole que vous utilisez. Vous pouvez également envisager d'intégrer, le cas échéant, les meilleures pratiques d'application aux paramètres backend, de classe de stockage et de PVC afin d'optimiser le stockage pour des applications spécifiques.

ONTAP et Cloud Volumes ONTAP

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

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

Utilisez des SVM dédiés à Trident

Les machines virtuelles de stockage (SVM) fournissent une isolation et une séparation administrative entre les locataires sur un système ONTAP . L'affectation 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 l'interface de ligne de commande (CLI).
- Partagez le rôle de gestion avec une interface de données NFS.

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

Il n'y a pas de préférence entre une LIF de gestion dédiée ou partagée pour la SVM ; cependant, vous devez vous assurer que vos politiques de sécurité réseau sont alignées sur l'approche que vous choisissez. Quoi qu'il en soit, l'interface LIF de gestion doit être accessible via DNS afin de faciliter une flexibilité maximale. "SVM-DR" être utilisé en conjonction avec Trident.

Limiter le nombre de volumes maximum

Les systèmes de stockage ONTAP ont un nombre maximal de volumes, qui varie en fonction de la version du logiciel et de la plateforme matérielle. Se référer à "Hardware Universe NetApp" pour votre plateforme et votre version ONTAP spécifiques 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.

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

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

La valeur de `max-volumes` varie en fonction de plusieurs critères propres 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 qui devraient être consommés par les applications Kubernetes

Le `max-volumes` La valeur correspond au volume total provisionné sur l'ensemble des nœuds du cluster ONTAP , et non sur un nœud ONTAP individuel. Par conséquent, vous pouvez rencontrer certaines conditions dans lesquelles un nœud de cluster ONTAP peut avoir beaucoup plus ou moins de volumes provisionnés Trident qu'un autre nœud.

Par exemple, un cluster ONTAP à deux nœuds peut héberger un maximum de 2000 volumes FlexVol . Fixer le nombre maximal de volumes à 1250 semble tout à fait raisonnable. Cependant, si seulement "agrégats" Si les agrégats d'un nœud sont affectés à la SVM ou ne peuvent pas être provisionnés (par exemple, en raison de la capacité), alors l'autre nœud devient la cible pour tous les volumes provisionnés Trident . Cela signifie que la limite de volume pourrait être atteinte pour ce nœud avant le `max-volumes` La valeur est atteinte, ce qui a un impact sur Trident et sur les autres opérations de volume utilisant ce nœud. **Vous pouvez éviter cette situation en veillant à ce que les agrégats de chaque nœud du cluster soient affectés en nombre égal au SVM utilisé par Trident .**

Cloner un volume

NetApp Trident prend en charge le clonage de volumes lors de l'utilisation de `ontap-nas` , `ontap-san` , `solidfire-san` , et `gcp-cvs` pilotes de stockage. Lors de l'utilisation du `ontap-nas-flexgroup` ou `ontap-nas-economy` Le clonage des pilotes 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 une StorageClass différente. Effectuez les opérations de clonage au sein de la même StorageClass afin de garantir la compatibilité et d'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 devez également exploiter les fonctionnalités de Kubernetes.

Limiter la taille maximale des FlexVols créés par Trident

Pour configurer la taille maximale des FlexVols utilisés comme pools pour les pilotes ontap-san-economy et ontap-nas-economy, utilisez le `limitVolumePoolSize` paramètre dans votre `backend.json` définition.

Configurez Trident pour utiliser CHAP bidirectionnel

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

Créer et utiliser une politique QoS SVM

L'utilisation d'une politique QoS ONTAP , appliquée au SVM, limite le nombre d'IOPS consommables par les volumes provisionnés Trident . Cela contribue à "prévenir l'intimidation" ou un conteneur incontrôlé susceptible d'affecter les charges de travail en dehors du SVM Trident .

Vous pouvez créer une politique QoS pour la SVM en quelques étapes. Pour obtenir les informations les plus précises, veuillez consulter la documentation correspondant à votre version d' ONTAP . 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 prend en charge, 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 facteurs. Cela comprend 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 que ces charges de travail ne soient pas accidentellement affectées négativement.
- Charges de travail attendues exécutées dans des conteneurs. Si des charges de travail ayant des exigences élevées en matière d'IOPS s'exécutent dans des conteneurs, une politique de QoS faible se traduira par une mauvaise expérience.

Il est important de rappeler qu'une politique QoS attribuée au niveau de la SVM a pour conséquence que tous les volumes provisionnés sur la SVM partagent le même pool d'IOPS. Si une ou quelques applications conteneurisées ont des exigences élevées en matière d'IOPS, elles pourraient devenir un frein pour les autres charges de travail conteneurisées. Dans ce cas, vous pourriez 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 ONTAP est antérieure à 9.8.

Créer des groupes de stratégies 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 politiques QoS ONTAP offrent des options 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 grâce à la QoS" . Vous pouvez spécifier des groupes de stratégies QoS dans le système dorsal ou dans un pool de stockage, et ils sont appliqués à chaque volume créé dans ce pool ou ce système dorsal.

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

Tenez compte des éléments suivants lors de la création de groupes de stratégies QoS :

- Vous devriez paramétrer le `qosPolicy` clé dans le `defaults` bloc de la configuration du backend. Voir l'exemple de configuration 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 du débit total spécifié par le groupe de stratégies. Les groupes de politiques partagées 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 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 part du principe que les ressources appartenant au même espace de noms peuvent être partagées ; cependant, et c'est important, 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 se trouvent dans le même espace de noms. **Il est essentiel de veiller à ce que les espaces de noms soient utilisés pour assurer la séparation lorsque cela est approprié.**

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

Un conteneur privilégié est un conteneur exécuté avec des autorisations au niveau de l'hôte nettement supérieures à la normale. Ces options ne sont pas désactivées par défaut ; assurez-vous donc de désactiver

cette fonctionnalité en utilisant "politiques de sécurité des pods" .

Pour les volumes pour lesquels l'accès est souhaité à la fois depuis Kubernetes et des hôtes externes, le stockage doit être géré de manière traditionnelle, avec le PV introduit par l'administrateur et non géré par Trident. Cela garantit que le volume de stockage n'est détruit que lorsque les hôtes Kubernetes et externes se sont déconnectés et n'utilisent plus le volume. De plus, une politique d'exportation personnalisée peut être appliquée, permettant 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 politiques d'exportation distinctes doivent être utilisées pour limiter davantage l'accès aux ressources de stockage. Cela inclut la création d'une politique d'exportation pour les services déployés sur ces nœuds d'infrastructure (par exemple, les services de métriques et de journalisation OpenShift) et les applications standard déployées sur des nœuds non infrastructurels.

Utilisez une politique d'exportation dédiée

Vous devez vous assurer qu'une politique d'exportation existe pour chaque backend, n'autorisant l'accès qu'aux nœuds présents dans le cluster Kubernetes. Trident peut créer et gérer automatiquement des politiques d'exportation. De cette façon, Trident limite l'accès aux volumes qu'il provisionne aux nœuds du cluster Kubernetes et simplifie l'ajout/la suppression de nœuds.

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

- Utilisez le `vserver export-policy create` Commande CLI ONTAP pour créer la politique d'exportation.
- Ajoutez des règles à la politique d'exportation en utilisant `vserver export-policy rule create` Commande CLI ONTAP .

L'exécution de ces commandes vous permet de restreindre l'accès aux données aux nœuds Kubernetes qui les utilisent.

Désactiver `showmount` pour l'application SVM

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

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

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

Bonnes pratiques SolidFire

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 son propre ensemble d'identifiants CHAP (Challenge-Handshake Authentication Protocol). Vous pouvez accéder aux volumes attribués à un compte soit en utilisant le nom du compte et les informations d'identification CHAP correspondantes, soit via un groupe d'accès aux volumes. Un compte peut se voir attribuer jusqu'à deux mille volumes, 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 définir les paramètres QoS volume par volume. Les performances de chaque volume peuvent être assurées en définissant trois paramètres configurables qui définissent la QoS : IOPS min, IOPS max et IOPS en rafale.

Voici les valeurs IOPS minimales, maximales et en rafale possibles pour une taille de bloc de 4 Ko.

Paramètre IOPS	Définition	Valeur minimale	Valeur par défaut	Valeur maximale (4 Ko)
IOPS minimales	Le niveau de performance garanti pour un volume donné.	50	50	15000
IOPS max	Les performances ne dépasseront pas cette limite.	50	15000	200 000
IOPS en rafale	Nombre maximal d'IOPS autorisé 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 de chaque nœud.

La taille des blocs et la bande passante ont une influence directe sur le nombre d'IOPS. À mesure que la taille des blocs augmente, le système accroît sa bande passante au niveau nécessaire pour traiter ces blocs plus volumineux. À mesure que la bande passante augmente, le nombre d'IOPS que le système est capable d'atteindre diminue. Se référer à "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 serveur. Les groupes d'accès aux volumes contrôlent l'accès aux volumes qu'ils provisionnent. NetApp recommande l'utilisation de CHAP pour l'authentification car il est plus simple et ne présente aucune limite d'évolutivité.

Trident, avec son provisionneur CSI amélioré, prend en charge l'utilisation de l'authentification CHAP. Les VAG ne doivent être utilisés qu'en mode de fonctionnement traditionnel, hors CSI.

L'authentification CHAP (vérification que l'initiateur est l'utilisateur du volume prévu) n'est prise en charge qu'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. Le protocole CHAP unidirectionnel authentifie l'accès au volume en utilisant le nom de compte SolidFire et le secret de l'initiateur. L'option CHAP bidirectionnelle offre la méthode d'authentification du volume la plus sûre, 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 cible.

Toutefois, si CHAP ne peut pas être activé et que des VAG sont nécessaires, créez le groupe d'accès et ajoutez les initiateurs hôtes et les volumes au groupe d'accès. Chaque IQN que vous ajoutez à un groupe d'accès peut accéder à chaque volume du groupe avec ou sans authentification CHAP. Si l'initiateur iSCSI est configuré pour utiliser l'authentification CHAP, un contrôle d'accès basé sur les comptes est utilisé. Si l'initiateur iSCSI n'est pas configuré pour utiliser l'authentification CHAP, alors le contrôle d'accès du groupe d'accès aux volumes est utilisé.

Où trouver plus d'informations ?

Vous trouverez ci-dessous une liste de quelques documents présentant les meilleures pratiques. Rechercher le "Bibliothèque NetApp" pour les versions les plus récentes.

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

Logiciel Element

- "Configuration de SolidFire pour Linux"
- NetApp HCI*
- "Prérequis pour le déploiement de NetApp HCI"
- "Accédez au moteur de déploiement NetApp"

Informations sur les meilleures pratiques d'application

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

Toutes les applications ne disposent pas de directives spécifiques ; il est important de collaborer avec votre équipe NetApp et d'utiliser les "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 à l'aide de Trident.

Sélection et déploiement des conducteurs

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

Pilotes backend ONTAP

Les pilotes backend ONTAP se différencient par le protocole utilisé et par la manière dont les volumes sont provisionnés sur le système de stockage. Par conséquent, réfléchissez bien avant de choisir 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 basés sur NAS seraient le choix par défaut, tandis que les pilotes iSCSI basés sur des blocs répondraient 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. D'une manière générale, il y a peu de différence entre eux pour la plupart des applications, la décision repose donc souvent sur la nécessité ou non d'un stockage partagé (où plusieurs pods auront besoin d'un accès simultané).

Les pilotes backend ONTAP disponibles sont :

- `ontap-nas`Chaque PV provisionné est un FlexVolume ONTAP complet.
- `ontap-nas-economy`Chaque PV provisionné est un qtree, avec un nombre configurable de qtrees par FlexVolume (la valeur par défaut est de 200).
- `ontap-nas-flexgroup`Chaque PV est provisionné en tant que FlexGroup ONTAP complet, 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 mises à la disposition de l'application.

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

Pilotes ONTAP NAS	Snapshots	Clones	Politiques d'exportation dynamiques	Multi-attache	Qualité de service	Redimensionner	Réplication
`ontap-nas`	Oui	Oui	Oui, note de bas de page : 5[]	Oui	Oui, note de bas de page : 1[]	Oui	Oui, note de bas de page : 1[]
`ontap-nas-economy`	NO [3]	NO [3]	Oui, note de bas de page : 5[]	Oui	NO [3]	Oui	NO [3]
`ontap-nas-flexgroup`	Oui, note de bas de page : 1[]	NON	Oui, note de bas de page : 5[]	Oui	Oui, note de bas de page : 1[]	Oui	Oui, note de bas de page : 1[]

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

Pilotes SAN ONTAP	Snapshots	Clones	Multi-attache	CHAP bidirectionnel	Qualité de service	Redimensionner	Réplication
`ontap-san`	Oui	Oui	Oui, note de bas de page : 4[]	Oui	Oui, note de bas de page : 1[]	Oui	Oui, note de bas de page : 1[]
`ontap-san-economy`	Oui	Oui	Oui, note de bas de page : 4[]	Oui	NO [3]	Oui	NO [3]

> Notes de bas de page pour les tableaux ci-dessus : Oui¹ : Non géré par Trident ; Oui² : Géré par Trident, mais pas au niveau des volumes persistants ; Non³ : Non géré par Trident et pas au niveau des volumes persistants ; Oui⁴ : Pris en charge pour les volumes à blocs bruts ; Oui⁵ : 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 LUN dans les FlexVols partagés) partageront un calendrier commun.

Comme on peut le constater dans les tableaux ci-dessus, une grande partie des fonctionnalités entre les `ontap-nas` et `ontap-nas-economy` c'est la même chose. Cependant, parce que le `ontap-nas-economy` Le pilote limite la capacité de contrôler la planification au niveau de chaque PV, ce qui 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 PVC sur le stockage ONTAP , cela n'est possible qu'en utilisant le `ontap-nas` , `ontap-san` ou `ontap-san-economy` conducteurs.

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

Pilotes backend Cloud Volumes ONTAP

Cloud Volumes ONTAP offre un contrôle des données ainsi que des fonctionnalités de stockage de classe entreprise pour divers cas d'utilisation, notamment les partages de fichiers et le stockage au niveau 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` . Ces instructions s'appliquent à Cloud Volume ONTAP pour Azure et à Cloud Volume ONTAP pour GCP.

Pilotes backend Amazon FSx pour ONTAP

Amazon FSx for NetApp ONTAP vous permet de tirer parti des fonctionnalités, des performances et des capacités d'administration de 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 pour 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` .

Pilotes de backend NetApp HCI/ SolidFire

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

Pilote SolidFire	Snapshots	Clones	Multi-attache	TYPE	Qualité de service	Redimensionner	Réplication
`solidfire-san`	Oui	Oui	Oui, note de bas de page : 2[]	Oui	Oui	Oui	Oui, note de bas de page : 1[]

> Note de bas de page : Oui¹ : Non géré par Trident ² : Pris en charge pour les volumes de blocs bruts

Pilotes de backend Azure NetApp Files

Trident utilise le `azure-netapp-files` le conducteur doit gérer le"Azure NetApp Files" service.

Vous trouverez plus d'informations sur ce pilote et sa configuration dans"Configuration du backend Trident pour Azure NetApp Files" .

Pilote de Azure NetApp Files	Snapshots	Clones	Multi-attache	Qualité de service	Développer	Réplication
`azure-netapp-files`	Oui	Oui	Oui	Oui	Oui	Oui, note de bas de page : 1[]

> Note de bas de page : Oui, note de bas de page 1 : Non géré par Trident

Cloud Volumes Service sur le pilote backend Google Cloud

Trident utilise le `gcp-cvs` Pilote permettant de se connecter au Cloud Volumes Service sur Google Cloud.

Le `gcp-cvs` Le pilote utilise des pools virtuels pour abstraire le backend et permettre à Trident de déterminer l'emplacement des volumes. L'administrateur définit les pools virtuels dans le `backend.json` fichiers. Les classes de stockage utilisent des sélecteurs pour identifier les pools virtuels par étiquette.

- Si des pools virtuels sont définis dans le backend, Trident tentera de créer un volume dans les pools de stockage Google Cloud auquel ces pools virtuels seront limités.
- Si les pools virtuels ne sont pas définis dans le backend, Trident sélectionnera un pool de stockage Google Cloud parmi les pools de stockage disponibles dans la région.

Pour configurer le backend Google Cloud sur Trident, vous devez spécifier `projectNumber` , `apiRegion` , et `apiKey` dans le fichier backend. Vous trouverez le numéro de projet dans la console Google Cloud. La clé API est extraite du fichier de clé privée du compte de service que vous avez créé lors de la configuration de l'accès API pour Cloud Volumes Service sur Google Cloud.

Pour plus d'informations sur les types de services et les niveaux de service de Cloud Volumes Service sur Google Cloud, veuillez consulter la documentation."Découvrez la prise en charge de CVS pour GCP par Trident" .

Pilote Cloud Volumes Service pour Google Cloud	Snapshots	Clones	Multi-attache	Qualité de service	Développer	Réplication
`gcp-cvs`	Oui	Oui	Oui	Oui	Oui	Disponible uniquement sur le type de service CVS-Performance.

Notes de réplication

- La réplication n'est pas gérée par Trident.
- Le clone sera créé dans le même pool de stockage que le volume source.

Conception de classe de stockage

Il est nécessaire de configurer et d'appliquer individuellement les classes de stockage 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 quel pool de stockage ou ensemble de pools doit être utilisé avec cette classe de stockage spécifique. Trois ensembles de filtres peuvent être définis dans la classe de stockage : `storagePools` , `additionalStoragePools` et/ou `excludeStoragePools` .

Le `storagePools` Ce paramètre permet de limiter le stockage à l'ensemble des pools correspondant aux

attributs spécifiés. Le `additionalStoragePools` Ce paramètre permet d'étendre l'ensemble des pools que Trident utilise pour le provisionnement, en plus de l'ensemble des pools sélectionnés par les attributs et `storagePools` paramètres. Vous pouvez utiliser l'un ou l'autre paramètre seul ou les deux ensemble pour vous assurer que l'ensemble approprié de pools de stockage est sélectionné.

Le `excludeStoragePools` Ce paramètre permet d'exclure spécifiquement l'ensemble de 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 le `media` attribut comme `hdd` ou `ssd` . Basé sur le `media` L'attribut mentionné dans la classe de stockage permettra à Trident de sélectionner le backend approprié qui sert `hdd` ou `ssd` regroupe les données pour correspondre à l'attribut média, puis dirige la mise à disposition des volumes vers l'agrégat spécifique. Nous pouvons donc créer une classe de stockage PREMIUM qui aurait `media` attribut défini comme `ssd` qui pourrait être classée comme la politique QoS PREMIUM. Nous pouvons créer une autre classe de stockage STANDARD dont l'attribut média serait défini sur `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 dispositif 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 le provisionnement des volumes sur un backend spécifique où des fonctionnalités telles que le provisionnement fin et épais, les instantanés, les clones et le chiffrement sont activées. Pour spécifier le stockage à utiliser, créez des classes de stockage qui définissent le système de stockage approprié avec la fonctionnalité requise activée.

Piscines virtuelles

Des pools virtuelles sont disponibles pour tous les backends Trident . Vous pouvez définir des pools virtuels pour n'importe quel backend, en utilisant n'importe quel pilote fourni par Trident .

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

Conception de piscine virtuelle

Lors de la création d'un backend, vous pouvez généralement spécifier un ensemble de paramètres. Il était impossible pour l'administrateur de créer un autre backend avec les mêmes identifiants de stockage et un ensemble de paramètres différent. L'introduction des pools virtuels a résolu ce problème. Un pool virtuel est une abstraction de niveau introduite entre le backend et la classe de stockage Kubernetes. L'administrateur peut ainsi définir des paramètres ainsi que des étiquettes référencées via les classes de stockage Kubernetes comme sélecteur, indépendamment du backend. Les pools virtuels peuvent être définis pour tous les backends NetApp pris en charge par Trident. Cela inclut SolidFire/ NetApp HCI, ONTAP, Cloud Volumes Service sur GCP, ainsi qu'Azure 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 plutôt un nouveau pool virtuel.

Émulation de différents niveaux de service/QoS

Il est possible de concevoir des pools virtuels pour émuler des classes de services. En utilisant l'implémentation de pool virtuel pour Cloud Volume Service pour Azure NetApp Files, examinons comment configurer différentes classes de service. Configurez le backend Azure NetApp Files avec plusieurs étiquettes, représentant différents niveaux de performance. Ensemble `servicelevel` ajouter les aspects au niveau de performance approprié et ajouter les autres aspects requis sous chaque étiquette. Créez maintenant différentes classes de stockage Kubernetes qui correspondront à différents pools virtuels. En utilisant le `parameters.selector` Dans ce champ, chaque StorageClass indique quels pools virtuels peuvent être utilisés pour héberger un volume.

Attribuer un ensemble spécifique d'aspects

Il est possible de concevoir plusieurs pools virtuelles présentant des caractéristiques spécifiques à partir d'un seul système de stockage dorsal. Pour ce faire, configurez le backend avec plusieurs étiquettes et définissez les aspects requis sous chaque étiquette. Créez maintenant différentes classes de stockage Kubernetes en utilisant `parameters.selector` champ qui correspondrait à différents pools virtuels. Les volumes provisionnés sur le système dorsal auront les caractéristiques définies dans le pool virtuel choisi.

Caractéristiques du PVC qui affectent la capacité de 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 une PVC, l'un des champs obligatoires est le mode d'accès. Le mode souhaité peut affecter le serveur dorsal sélectionné pour héberger la requête de stockage.

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

	Lire/Écrire une seule fois	Lecture seule de plusieurs	Lire/Écrire/Nombreux
iSCSI	Oui	Oui	Oui (bloc cru)
NFS	Oui	Oui	Oui

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

Opérations de volume

Modifier les volumes persistants

Les volumes persistants sont, à deux exceptions près, des objets immuables dans Kubernetes. Une fois créée, la politique de récupération et la taille peuvent être modifiées. Cependant, cela n'empêche pas certains aspects du volume d'être modifiés en dehors de Kubernetes. Cela peut s'avérer utile pour personnaliser le volume en fonction d'applications spécifiques, pour éviter toute consommation accidentelle de capacité, ou

simplement pour déplacer le volume vers un autre contrôleur de stockage pour quelque raison que ce soit.

> Les provisionneurs intégrés à Kubernetes ne prennent pas en charge les opérations de redimensionnement de volume pour les PV 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 sa création.

Créer des instantanés de volume à la demande

Trident prend en charge la création d'instantanés de volumes à la demande et la création de PVC à partir d'instantanés à l'aide du framework CSI. Les snapshots offrent une méthode pratique pour conserver des copies ponctuelles des données 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 volumes. Pour ce faire, il suffit de créer un PersistentVolumeClaim et de mentionner le `datasource` comme instantané requis à partir duquel le volume doit être créé. Trident gérera ce PVC en créant un volume contenant 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 connecté.

Déplacer les volumes dans le cluster

Les administrateurs de stockage ont la possibilité de déplacer des volumes entre les agrégats et les contrôleurs du cluster ONTAP sans perturber le consommateur de stockage. Cette opération n'affecte ni Trident ni le cluster Kubernetes, tant que l'agrégat de destination est un agrégat auquel le SVM utilisé par Trident a accès. Il est important de noter que si l'agrégat a été récemment ajouté au SVM, le backend devra être actualisé en le réajoutant à Trident. Cela déclenchera une nouvelle inventaire du SVM par Trident afin que le nouvel agrégat soit reconnu.

Cependant, le déplacement de volumes entre les systèmes backend n'est pas pris en charge automatiquement par Trident. Cela inclut entre les SVM du même cluster, entre les clusters ou sur 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 fonction d'importation de volumes peut être utilisée pour importer les volumes actuels dans Trident.

Augmenter les volumes

Trident prend en charge le redimensionnement des volumes persistants NFS, iSCSI et FC. Cela permet aux utilisateurs de redimensionner leurs volumes directement via la couche Kubernetes. L'extension de volume est possible pour toutes les principales plateformes de stockage NetApp , y compris ONTAP, SolidFire/ NetApp HCI et les backends Cloud Volumes Service . Pour permettre une éventuelle extension ultérieure, définissez `allowVolumeExpansion` à `true` dans votre StorageClass associée au volume. Lorsque le volume persistant doit être redimensionné, modifiez le `spec.resources.requests.storage` annotation dans la revendication de volume persistant à la taille de volume requise. Trident se chargera automatiquement du redimensionnement du volume sur le cluster de stockage.

Importer un volume existant dans Kubernetes

L'importation de volumes permet d'importer un volume de stockage existant dans un environnement Kubernetes. Ceci est actuellement pris en charge par le `ontap-nas` , `ontap-nas-flexgroup` , `solidfire-san` , `azure-netapp-files` , et `gcp-cvs` conducteurs. Cette fonctionnalité est utile lors du portage d'une application existante vers Kubernetes ou lors de scénarios de reprise après sinistre.

Lors de l'utilisation d' ONTAP et `solidfire-san` conducteurs, utilisez la commande `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` importer un volume existant dans Kubernetes pour qu'il soit géré par Trident. Le fichier YAML ou JSON du PVC utilisé dans la commande d'importation de volume pointe vers une classe de stockage qui identifie Trident comme le provisionneur. Lors de l'utilisation d'un système dorsal 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 fonction d'importation de volumes puisse les distinguer.

Si le `azure-netapp-files` ou `gcp-cvs` Le pilote 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 trouvera le volume sur le serveur et lira sa taille. Il ajoutera automatiquement (et écrasera si nécessaire) la taille du volume configurée du PVC. Trident crée ensuite le nouveau PV et Kubernetes lie le PVC au PV.

Si un conteneur était déployé de manière à nécessiter le PVC importé spécifique, il resterait en attente jusqu'à ce que la paire PVC/PV soit liée via le processus d'importation de volume. Une fois la paire PVC/PV assemblée, le conteneur devrait remonter, à condition qu'il n'y ait pas d'autres problèmes.

Service d'enregistrement

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 services OpenShift, 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. Deux méthodes d'installation seront abordées : le déploiement de la journalisation lors de l'installation initiale d'OpenShift et le déploiement de la journalisation après l'installation d'OpenShift.

> 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 problèmes de corruption de données. Cela 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 fonctionnent 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` à `true` pour éviter que l'installation ne tombe en panne.

Commencer

Le service de journalisation peut, en option, être déployé à la fois pour les applications et pour les opérations de base du cluster OpenShift 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 pour les opérations contiennent le terme « ops », contrairement à l'instance pour les applications.

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

> Les tableaux ci-dessous contiennent uniquement les variables pertinentes pour la configuration du stockage en ce qui concerne le service de journalisation. Vous pouvez trouver d'autres options dans"Documentation de journalisation de Red Hat OpenShift" qui doivent être examinés, configurés et utilisés 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 des composants après l'installation d'OpenShift ; cependant, si vous disposez de volumes existants, elle reste une option.

Variable	Détails
`openshift_logging_storage_kind`	Réglé 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. Cette valeur doit être définie sur le dataLIF de votre machine virtuelle.
`openshift_logging_storage_nfs_directory`	Le chemin de montage pour l'exportation NFS. Par exemple, si le volume est joint comme `/openshift_logging` Vous utiliseriez 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'exportation NFS, par exemple `100Gi` .

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

Variable	Détails
`openshift_logging_es_pvc_dynamic`	Définissez cette option sur « true » pour utiliser des volumes provisionnés dynamiquement.
`openshift_logging_es_pvc_storage_class_name`	Le nom de la classe de stockage qui sera utilisée dans le PVC.
`openshift_logging_es_pvc_size`	Le volume demandé dans le PVC.
`openshift_logging_es_pvc_prefix`	Un préfixe pour les PVC utilisés par le service d'exploitation forestière.
`openshift_logging_es_ops_pvc_dynamic`	Réglé sur `true` utiliser des volumes provisionnés dynamiquement pour l'instance de journalisation des opérations.

Variable	Détails
`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 d'opérations.
`openshift_logging_es_ops_pvc_prefix`	Un préfixe pour les PVC d'instance d'opérations.

Déployez la pile de journalisation

Si vous déployez la journalisation dans le cadre du processus d'installation initial d'OpenShift, il vous suffit de suivre la procédure de déploiement standard. Ansible configurera et déploiera les services et objets OpenShift nécessaires afin que le service soit disponible dès que l'exécution d'Ansible sera terminée.

Toutefois, si vous effectuez un déploiement après l'installation initiale, Ansible devra utiliser le playbook du composant. Ce processus peut légèrement varier selon les versions d'OpenShift ; assurez-vous donc de lire et de suivre les instructions."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 cluster OpenShift. Elle est également nécessaire pour la fonctionnalité de mise à l'échelle automatique des pods, et de nombreuses organisations utilisent les données du service de métriques pour leurs applications de refacturation et/ou de présentation.

Comme pour le service de journalisation et pour OpenShift dans son ensemble, Ansible est utilisé pour déployer le service de métriques. De même que 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 de composants. Les tableaux suivants contiennent les variables 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 ce qui concerne le service de métriques. De nombreuses autres options sont décrites dans la documentation et doivent être examinées, configurées et utilisées en fonction de votre déploiement.

Variable	Détails
`openshift_metrics_storage_kind`	Réglé 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. Cette valeur doit être définie sur dataLIF pour votre SVM.
`openshift_metrics_storage_nfs_directory`	Le chemin de montage pour l'exportation NFS. Par exemple, si le volume est joint comme `/openshift_metrics` Vous utiliseriez 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'exportation NFS, par exemple `100Gi` .

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

Variable	Détails
`openshift_metrics_cassandra_pvc_prefix`	Un préfixe à utiliser pour les PVC 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 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.

Déployer 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 lors de l'installation d'OpenShift, le PV sera créé et utilisé automatiquement. Si vous déployez à l'aide des playbooks de composants, après l'installation d'OpenShift, Ansible crée les PVC nécessaires et, une fois que Trident a provisionné le stockage pour ceux-ci, déploie le service.

Les variables ci-dessus, ainsi que le processus de déploiement, peuvent changer avec chaque version d'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 et de récupération des données pour chaque application ayant une exigence de persistance.

Réplication et récupération du Trident

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

Réplication du 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 à l'aide de"Kubernetes : Sauvegarde d'un cluster etcd" .
2. Placez les artefacts de sauvegarde sur un FlexVol volume

> NetApp recommande de protéger le SVM sur lequel réside le FlexVol par une relation SnapMirror avec un 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 contenant les fichiers de données et les certificats etcd de Kubernetes 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. Courir `kubectl get crd` vérifier que toutes les ressources personnalisées Trident sont opérationnelles et récupérer les objets Trident pour vérifier que toutes les données sont disponibles.

Réplication et récupération SVM

Trident ne permet pas de configurer les relations de réplication ; toutefois, 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 diffuser des données. Vous pourrez revenir au système principal une fois les systèmes restaurés.

À propos de cette tâche

Tenez compte des points suivants lors de l'utilisation de la fonctionnalité de réplication SVM de 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 d'être répliqués soient provisionnés sur les backends qui prennent en charge SVM-DR.
- Les administrateurs d'applications doivent prendre en compte les coûts et la complexité supplémentaires liés à la réplication et examiner attentivement leur plan de reprise d'activité avant d'entamer ce processus.

Réplication SVM

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

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

- "-identité-préserver vrai"réplique l'intégralité de la configuration SVM.
- "-discard-configs réseau"Exclut les LIF et les paramètres réseau associés.
- "-identité-préserver faux"Réplique uniquement les volumes et la configuration de sécurité.

Récupération SVM à l'aide de Trident

Trident ne détecte pas automatiquement les défaillances des SVM. En cas de sinistre, l'administrateur peut lancer manuellement le basculement Trident vers la nouvelle SVM.

Étapes

1. Annulez les transferts SnapMirror planifiés et en cours, interrompez la relation de réplication, arrêtez le SVM source puis activez le 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 le `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. Omission `storagePrefix` provoquera l'échec de la mise à jour du serveur.
4. Mettez à jour tous les serveurs d'arrière-plan 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 de l'application.

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

Réplication et récupération de volume

Trident ne peut pas configurer les relations de réplication SnapMirror ; toutefois, 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"importation de volume tridentctl" .

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

Protection des données instantanées

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

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

  "Instantanés de volume"

- Les snapshots ONTAP permettent de restaurer l'intégralité du contenu d'un volume ou de récupérer des fichiers ou des LUN individuels.

  "Instantanés ONTAP"

Sécurité

Sécurité

Suivez les recommandations ci-dessous pour garantir la sécurité de votre installation

Trident .

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`). Placer 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'accès à `tridentctl` application.

Utilisez l'authentification CHAP avec les backends SAN ONTAP.

Trident prend en charge l'authentification basée sur CHAP pour les charges de travail ONTAP SAN (en utilisant le `ontap-san` et `ontap-san-economy` conducteurs). NetApp recommande l'utilisation du protocole CHAP bidirectionnel avec Trident pour l'authentification entre un hôte et le système de stockage dorsal.

Pour les backends ONTAP utilisant les pilotes de stockage SAN, Trident peut configurer un protocole CHAP bidirectionnel et gérer les noms d'utilisateur et les secrets CHAP via `tridentctl` . Se référer 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 les backends NetApp HCI et SolidFire.

NetApp recommande le déploiement du protocole CHAP bidirectionnel pour garantir l'authentification entre un hôte et les serveurs dorsaux NetApp HCI et SolidFire . Trident utilise un objet secret qui inclut deux mots de passe CHAP par locataire. Lors de son installation, Trident gère les secrets CHAP et les stocke dans un `tridentvolume` Objet CR 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 groupe d'accès aux volumes.

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, reportez-vous à"Présentation de la configuration du chiffrement de volume NetApp" .

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

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

- Vous pouvez définir l'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 l'indicateur de chiffrement NVE sur `false` sur un backend compatible NAE crée un volume compatible NAE. Vous ne pouvez pas désactiver le chiffrement NAE en définissant l'indicateur de chiffrement NVE sur `false` .

- Vous pouvez créer manuellement un volume NVE dans Trident en définissant explicitement l'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 ONTAP NAS"

Configuration unifiée des clés Linux (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 LUKS.

Dans Trident, les volumes chiffrés LUKS utilisent le chiffrement 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 plus d'informations sur les systèmes ASA r2, consultez"En savoir plus sur les systèmes de stockage ASA r2" .

Avant de commencer

- Les nœuds de travail doivent avoir cryptsetup 2.1 ou supérieur (mais inférieur à 3.0) installé. Pour plus d'informations, consultez"Gitlab : cryptsetup" .
- Pour des raisons de performance, NetApp recommande que les nœuds de travail prennent en charge les nouvelles instructions de la norme de chiffrement avancé (AES-NI). Pour vérifier la prise en charge d'AES-NI, exécutez la commande suivante :

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

Si aucune réponse n'est reçue, votre processeur ne prend pas en charge AES-NI. Pour plus d'informations sur AES-NI, consultez :"Intel : Instructions de la norme de chiffrement avancée (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, veuillez consulter la documentation."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. Utiliser `parameters.selector` définir les pools de stockage à l'aide du 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 contenant la phrase de passe LUKS. Par exemple:

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

Limites

Les volumes 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 configurer `luksEncryption` à(`true` en arrière-plan. Le `luksEncryption` Cette option indique à Trident si le volume est conforme à la norme LUKS.(`true`) ou non conforme à LUKS(`false`) comme le montre 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` à `true` et inclure 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
```

Rotation d'une phrase de passe LUKS

Vous pouvez modifier la phrase de passe LUKS et confirmer la modification.

> N'oubliez pas une phrase de passe tant que vous n'avez pas vérifié qu'elle n'est plus référencée par aucun volume, instantané ou secret. Si la phrase de passe de référence est perdue, vous risquez de ne pas pouvoir monter le volume et les données resteront chiffrées et inaccessibles.

À propos de cette tâche

La rotation de la phrase de passe LUKS se produit lorsqu'un pod qui monte le volume est créé après la spécification d'une nouvelle phrase de passe LUKS. Lors de la création d'un nouveau pod, Trident compare la phrase de passe LUKS du volume à la phrase de passe active du secret.

- Si la phrase de passe figurant sur le volume ne correspond pas à la phrase de passe active dans le secret, une rotation a lieu.
- Si la phrase de passe figurant sur le volume correspond à la phrase de passe active dans le secret, le `previous-luks-passphrase` Ce paramètre est ignoré.

Étapes

1. Ajoutez le `node-publish-secret-name` et `node-publish-secret-namespace` Paramètres de StorageClass. Par exemple:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identifier les phrases de passe existantes sur le volume ou l'instantané.

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 pour spécifier les nouvelles et anciennes phrases de passe. Assurer `previous-luke-passphrase-name` et `previous-luks-passphrase` correspondre 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 lancer 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 a été 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 une nouvelle capsule 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. Activer `CSINodeExpandSecret` fonctionnalité gate (bêta 1.25+). Se référer à "Kubernetes 1.25 : Utilisation des secrets pour l'extension des volumes CSI pilotée par les nœuds" pour plus de détails.
2. Ajoutez le `node-expand-secret-name` et `node-expand-secret-namespace` Paramètres de 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 l'extension du stockage en ligne, le kubelet transmet les informations d'identification appropriées au pilote.

Chiffrement Kerberos en transit

En utilisant le chiffrement Kerberos en transit, vous pouvez améliorer la sécurité d'accès aux données en activant le chiffrement du trafic entre votre cluster géré et le système de stockage dorsal.

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

- * ONTAP sur site* - 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 utilisant 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 systèmes de stockage ONTAP sur site n'est pris en charge qu'avec l'interface suivante : `ontap-nas` pilote de stockage.

Avant de commencer

- Assurez-vous d'avoir accès à `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 système de stockage ONTAP .
- Assurez-vous d'avoir préparé la machine virtuelle de stockage ONTAP pour prendre en charge le chiffrement Kerberos pour les volumes NFS. Se référer à "Activer Kerberos sur une LIF de données" pour les 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 NetApp NFSv4 (page 13) du manuel. "Guide des améliorations et des bonnes pratiques NetApp NFSv4" .

Ajouter ou modifier les politiques d'exportation ONTAP

Vous devez ajouter des règles aux politiques d'exportation ONTAP existantes ou créer de nouvelles politiques d'exportation 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 de politique d'exportation que vous ajoutez, ou les nouvelles politiques d'exportation que vous créez, doivent prendre en charge les protocoles d'accès et les autorisations d'accès suivants :

Protocoles d'accès

Configurez la politique d'exportation 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 des besoins de votre 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 de stratégie d'exportation 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 politiques d'exportation ONTAP et des règles de politique d'exportation :

- "Créer une politique d'exportation"
- "Ajouter une règle à une politique d'exportation"

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 de stockage dorsal qui configure le chiffrement Kerberos, vous pouvez spécifier l'une des trois versions différentes de chiffrement Kerberos à l'aide de `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 sera utilisée.

Étapes

1. Sur le cluster géré, créez un fichier de configuration de stockage en utilisant l'exemple suivant. Remplacez les valeurs entre crochets <> par les informations provenant 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, c'est qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

Une fois le problème du fichier de configuration identifié et corrigé, vous pouvez exécuter à nouveau la commande de création.

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 de `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 sera utilisée. Si le niveau de chiffrement que vous avez spécifié dans la configuration du backend de stockage est différent de celui que vous avez spécifié dans l'objet de classe de stockage, c'est l'objet de classe de stockage qui prévaut.

Étapes

1. Créez un objet StorageClass Kubernetes 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 obtenir un résultat similaire à celui-ci :

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

Volumes de provision

Une fois que vous avez créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour les instructions, reportez-vous à "Provisionnez 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 `tridentctl` utilitaire.
- Assurez-vous d'avoir préparé le système de stockage Azure NetApp Files pour le chiffrement Kerberos en prenant en compte les exigences et en suivant les instructions. "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 NetApp NFSv4 (page 13) du manuel. "Guide des améliorations et des bonnes pratiques NetApp NFSv4" .

Créer un backend de stockage

Vous pouvez créer une configuration de stockage backend Azure NetApp Files incluant la fonctionnalité 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 suivants :

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

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 de backend de stockage en utilisant l'un des exemples suivants, selon l'endroit où vous devez définir le backend de stockage (niveau du backend de stockage ou niveau du pool virtuel). Remplacez les valeurs entre crochets <> par les informations provenant de votre environnement :

Exemple de niveau 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 piscine virtuelle

```
---
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, c'est qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

Une fois le problème du fichier de configuration identifié et corrigé, vous pouvez exécuter à nouveau la commande de création.

Créer une classe de stockage

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

Étapes

1. Créez un objet StorageClass Kubernetes 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 obtenir un résultat similaire à celui-ci :

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

Volumes de provision

Une fois que vous avez créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour les instructions, reportez-vous à "Provisionnez un volume" .