Meilleures pratiques et recommandations

Trident

NetApp
January 14, 2026

Sommaire

Meilleures pratiques et recommandations

Déploiement

Suivez les recommandations répertoriées ici lors du déploiement de Trident.

Déploiement dans un namespace dédié

"Espaces de noms" séparation administrative entre les différentes applications et obstacle au partage des ressources. Par exemple, un volume persistant ne peut pas être consommé depuis un autre espace de noms. Trident fournit des ressources PV à tous les namespaces du cluster Kubernetes et utilise donc un compte de service qui a un Privileges élevé.

L'accès au pod Trident peut également permettre à un utilisateur d'accéder aux identifiants du système de stockage et à d'autres informations sensibles. Il est important de s'assurer que les utilisateurs d'applications et les applications de gestion ne peuvent pas accéder aux définitions d'objets Trident ou aux pods eux-mêmes.

Utilisez les quotas et les limites des plages pour contrôler la consommation du stockage

Kubernetes dispose de deux fonctionnalités qui, lorsqu'elles sont combinées, fournissent un mécanisme puissant pour limiter la consommation des ressources par les applications. "mécanisme de quotas de stockage"Permet à l'administrateur de mettre en œuvre des limites de consommation de capacité et de nombre d'objets globales et spécifiques à chaque classe de stockage, par espace de noms. En outre, l'utilisation d'un "limite de plage" garantit que les demandes de volume persistant sont à la fois dans les limites minimum et maximum avant que la demande ne soit transmise au provisionneur.

Ces valeurs sont définies par espace de noms, ce qui signifie que chaque espace de noms doit avoir des valeurs définies qui correspondent à leurs besoins en ressources. Voir ici pour plus d'informations sur "comment exploiter les quotas".

Configuration de stockage sous-jacente

Chaque plateforme de stockage du portefeuille NetApp dispose de fonctionnalités uniques qui bénéficient aux applications, conteneurisées ou non.

Présentation de la plateforme

Trident fonctionne avec ONTAP et Element. Il n'existe pas de plate-forme mieux adaptée à toutes les applications et tous les scénarios qu'une autre. Cependant, les besoins de l'application et l'équipe chargée de l'administration du périphérique doivent être pris en compte lors du choix d'une plate-forme.

Vous devez suivre les meilleures pratiques de base du système d'exploitation hôte avec le protocole utilisé. Vous pouvez éventuellement envisager d'intégrer les meilleures pratiques des applications, le cas échéant, avec des paramètres de back-end, de classe de stockage et de volume persistant afin d'optimiser le stockage pour certaines applications.

Meilleures pratiques pour ONTAP et Cloud Volumes ONTAP

Découvrez les bonnes pratiques pour la configuration d'ONTAP et de Cloud Volumes ONTAP pour Trident.

Les recommandations suivantes sont des instructions de configuration de ONTAP pour les workloads conteneurisés, qui consomment des volumes provisionnés dynamiquement par Trident. Chaque élément doit être pris en compte et évalué en fonction de la pertinence dans votre environnement.

Utilisation de SVM(s) dédié(s) à Trident

Les machines virtuelles de stockage (SVM) assurent l'isolation et la séparation administrative entre les locataires sur un système ONTAP. La dédier un SVM aux applications permet de déléguer des privilèges et d'appliquer les meilleures pratiques en matière de limitation de la consommation des ressources.

Plusieurs options sont disponibles pour la gestion de la SVM :

- Fournir l'interface de gestion du cluster en configuration back-end avec les identifiants appropriés et spécifier le nom du SVM
- Créer une interface de gestion dédiée pour le SVM via ONTAP System Manager ou l'interface de ligne de commande.
- Partage du rôle de gestion avec une interface de données NFS

Dans chaque cas, l'interface doit être dans DNS et le nom DNS doit être utilisé lors de la configuration de Trident. Ainsi, certaines scénarios de reprise après incident, par exemple SVM-DR, sans conservation des identités de réseau.

Il n'existe aucune préférence entre une LIF de gestion dédiée ou partagée pour le SVM, cependant, vous devez vous assurer que vos stratégies de sécurité réseau sont en adéquation avec l'approche de votre choix. Quoi qu'il en soit, la LIF de gestion doit être accessible via DNS afin de faciliter une flexibilité maximale doit "SVM-DR" être utilisée conjointement avec Trident.

Limitez le nombre maximal de volumes

Les systèmes de stockage ONTAP disposent d'un nombre maximal de volumes, qui varie selon la version logicielle et la plateforme matérielle. Reportez-vous "NetApp Hardware Universe" à la pour connaître votre plate-forme spécifique et la version de ONTAP pour déterminer les limites exactes. Lorsque le nombre de volumes est épuisé, les opérations de provisionnement échouent non seulement pour Trident, mais pour l'ensemble des requêtes de stockage.

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

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

La valeur de varie en fonction de `max-volumes` plusieurs critères spécifiques à votre environnement :

- Le nombre de volumes existants dans le cluster ONTAP
- Le nombre de volumes que vous prévoyez de provisionner en dehors de Trident pour d'autres applications
- Nombre de volumes persistants que les applications Kubernetes devraient consommer

`max-volumes`La valeur correspond au total des volumes provisionnés sur tous les nœuds du cluster ONTAP et non sur un nœud ONTAP individuel. Par conséquent, vous pouvez rencontrer des situations où un nœud de cluster ONTAP peut avoir plus ou moins de volumes provisionnés Trident qu'un autre nœud.

Par exemple, un cluster ONTAP à deux nœuds peut héberger un maximum de 2000 volumes flexibles. Avoir le volume maximum réglé sur 1250 semble très raisonnable. Toutefois, si seul un nœud est attribué au SVM ou si "64 bits" les agrégats attribués à partir d'un nœud ne peuvent pas être provisionnés sur (par exemple, en raison de la capacité), l'autre nœud devient la cible de tous les volumes provisionnés Trident. Cela signifie que la limite de volume peut être atteinte pour ce nœud avant que la valeur ne `max-volumes` soit atteinte, ce qui a un impact sur les opérations de volume Trident et autres qui utilisent ce nœud. **Vous pouvez éviter cette situation en vous assurant que les agrégats de chaque nœud du cluster sont attribués à la SVM utilisée par Trident en chiffres égaux.**

Limitez la taille maximale des volumes créés par Trident

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

Vous devez aussi exploiter les fonctionnalités Kubernetes pour contrôler la taille du volume au niveau de la baie de stockage.

Limitez la taille maximale des volumes FlexVol créés par Trident

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

Configurez Trident pour utiliser le protocole CHAP bidirectionnel

Vous pouvez spécifier l'initiateur CHAP et les noms d'utilisateur et mots de passe cibles dans votre définition du système back-end et activer Trident sur la SVM. En utilisant `useCHAP` le paramètre de votre configuration back-end, Trident authentifie les connexions iSCSI pour les systèmes back-end ONTAP avec le protocole CHAP.

Création et utilisation d'une politique de QoS de SVM

L'utilisation d'une politique de QoS de ONTAP appliquée au SVM limite le nombre de consommables d'IOPS par les volumes provisionnés par Trident. Cela permet à "évitez un tyran" ou à un conteneur hors contrôle d'affecter les charges de travail en dehors de la SVM Trident.

Vous pouvez créer une politique de QoS pour la SVM en quelques étapes. Consultez la documentation de votre version de ONTAP pour obtenir des informations précises. L'exemple ci-dessous crée une politique de QoS qui limite le nombre total d'IOPS disponibles pour la SVM à 5000.

```
# create the policy group for the SVM
qos policy-group create -policy-group <policy_name> -vserver <svm_name>
-max-throughput 5000iops

# assign the policy group to the SVM, note this will not work
# if volumes or files in the SVM have existing QoS policies
vserver modify -vserver <svm_name> -qos-policy-group <policy_name>
```

Si votre version d'ONTAP la prend en charge, il est également possible d'utiliser un minimum de QoS pour garantir un débit minimum pour les workloads conteneurisés. La QoS adaptative n'est pas compatible avec une règle de niveau SVM.

Le nombre d'IOPS dédiées aux workloads conteneurisés dépend de plusieurs aspects. Entre autres choses :

- Autres charges de travail qui utilisent la baie de stockage. Si certaines charges de travail, autres que celles liées au déploiement Kubernetes avec les ressources de stockage, veillez à ne pas affecter accidentellement ces charges de travail.
- Workloads attendus s'exécutant dans des conteneurs. Si des charges de travail qui exigent des IOPS élevées s'exécutent dans des conteneurs, une faible politique de QoS entraîne une mauvaise expérience.

Il est important de rappeler qu'une politique de QoS attribuée au niveau du SVM entraîne tous les volumes provisionnés sur la SVM et partageant le même pool d'IOPS. Si l'une des applications conteneurisées a une exigence d'IOPS élevées, elle pourrait devenir une force dominante pour les autres workloads conteneurisés. Dans ce cas, vous pourriez envisager d'utiliser l'automatisation externe pour attribuer des règles de QoS par volume.

Vous devez affecter la « policy group » QoS à la SVM **Only** si la version de votre ONTAP est antérieure à 9.8.

Création de groupes de règles de QoS pour Trident

La qualité de service (QoS) garantit que les performances des workloads stratégiques ne sont pas dégradées par des charges de travail concurrentes. Les groupes de règles de QoS de ONTAP proposent des options de QoS pour les volumes et permettent aux utilisateurs de définir le plafond de débit pour une ou plusieurs charges de travail. Pour plus d'informations sur QoS, reportez-vous à "Débit garanti avec la QoS". Vous pouvez spécifier des groupes de règles de QoS dans le back-end ou dans un pool de stockage, et ils sont appliqués à chaque volume créé dans ce pool ou back-end.

ONTAP propose deux types de groupes de règles de QoS : classiques et évolutifs. Les groupes de règles classiques fournissent un débit minimal (ou minimal, dans les versions ultérieures) plat en IOPS. La QoS adaptative ajuste automatiquement le débit en fonction de la taille du workload. Elle maintient le rapport entre les IOPS et les To|Go en fonction de l'évolution de la taille du workload. Vous pouvez ainsi gérer des centaines, voire des milliers de charges de travail dans le cadre d'un déploiement à grande échelle.

Avant de créer des groupes de règles de QoS, tenez compte des points suivants :

- Vous devez définir la `qosPolicy` clé dans le `defaults` bloc de la configuration back-end. Voir l'exemple de configuration back-end suivant :

```
  ---
version: 1
storageDriverName: ontap-nas
managementLIF: 0.0.0.0
dataLIF: 0.0.0.0
svm: svm0
username: user
password: pass
defaults:
  qosPolicy: standard-pg
storage:
- labels:
    performance: extreme
  defaults:
    adaptiveQosPolicy: extremely-adaptive-pg
- labels:
    performance: premium
  defaults:
    qosPolicy: premium-pg
```

- Vous devez appliquer les « policy groups » par volume pour que chaque volume bénéficie de l'intégralité du débit spécifié par le « policy group ». Les groupes de stratégies partagés ne sont pas pris en charge.

Pour plus d'informations sur les groupes de règles QoS, reportez-vous "Commandes QoS de ONTAP 9.8" à la section .

Limitez l'accès aux ressources de stockage aux membres du cluster Kubernetes

La limitation de l'accès aux volumes NFS et aux LUN iSCSI créés par Trident est un composant stratégique du niveau de sécurité pour votre déploiement Kubernetes. En effet, les hôtes qui ne font pas partie du cluster Kubernetes n'accèdent pas aux volumes et peuvent modifier les données de façon inattendue.

Il est important de comprendre que les espaces de noms sont la limite logique des ressources dans Kubernetes. L'hypothèse est que les ressources dans un même espace de noms peuvent être partagées, mais, surtout, il n'existe aucune fonctionnalité de multi-espace de noms. Même si les volumes persistants sont des objets globaux, lorsqu'ils sont liés à une demande de volume persistant, ils ne sont accessibles que par des pods qui se trouvent dans le même espace de noms. **Il est essentiel de s'assurer que les espaces de noms sont utilisés pour fournir la séparation, le cas échéant.**

La préoccupation principale de la plupart des entreprises en ce qui concerne la sécurité des données dans un contexte Kubernetes est qu'un processus dans un conteneur peut accéder au stockage monté sur l'hôte, mais qui n'est pas destiné au conteneur. "Espaces de noms" sont conçus pour empêcher ce type de compromis. Toutefois, il y a une exception : les conteneurs privilégiés.

Un conteneur privilégié est un conteneur exécuté avec beaucoup plus d'autorisations au niveau de l'hôte que la normale. Ils ne sont pas refusés par défaut. Assurez-vous donc de désactiver cette fonctionnalité à l'aide de "stratégies de sécurité des pods".

Pour les volumes pour lesquels l'accès est demandé depuis Kubernetes et des hôtes externes, le stockage doit être géré de manière classique, avec le volume persistant introduit par l'administrateur et non géré par

Trident. Cela garantit que le volume de stockage est détruit uniquement lorsque les hôtes Kubernetes et externes sont déconnectés et qu'ils n'utilisent plus le volume. En outre, il est possible d'appliquer une export policy personnalisée qui permet l'accès depuis les nœuds de cluster Kubernetes et les serveurs ciblés à l'extérieur du cluster Kubernetes.

Pour les déploiements avec des nœuds d'infrastructure dédiés (par exemple OpenShift) ou d'autres nœuds ne pouvant pas planifier les applications utilisateur, des règles d'exportation distinctes doivent être utilisées pour limiter davantage l'accès aux ressources de stockage. Cela inclut la création d'une export policy pour les services qui sont déployés sur ces nœuds d'infrastructure (par exemple les services OpenShift Metrics et Logging Services), ainsi que pour les applications standard déployées sur des nœuds non liés à l'infrastructure.

Utiliser une export policy dédiée

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

Vous pouvez également créer une export policy manuellement et la remplir à l'aide d'une ou plusieurs règles d'exportation qui traitent chaque demande d'accès de nœud :

- Utiliser `vserver export-policy create` la commande de l'interface de ligne de commandes ONTAP pour créer les export policy.
- Ajoutez des règles à la export policy à l'aide de la `vserver export-policy rule create` commande de l'interface de ligne de commandes ONTAP.

L'exécution de ces commandes vous permet de limiter l'accès aux données aux nœuds Kubernetes.

Désactivez `showmount` pour le SVM d'application

La `showmount` fonctionnalité permet à un client NFS d'interroger le SVM sur la liste des exports NFS disponibles. Un pod déployé dans le cluster Kubernetes peut émettre la `showmount -e` commande contre la LIF de données et recevoir une liste des montages disponibles, y compris ceux auxquels il n'a pas accès. Bien qu'il ne s'agisse pas d'un compromis sur la sécurité, cette solution fournit des informations inutiles susceptibles d'aider un utilisateur non autorisé à se connecter à une exportation NFS.

Pour la désactiver `showmount`, utiliser la commande CLI ONTAP au niveau du SVM :

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

Les meilleures pratiques pour SolidFire

Découvrez les bonnes pratiques pour la configuration du stockage SolidFire pour Trident.

Créer un compte SolidFire

Chaque compte SolidFire représente un propriétaire de volume unique et reçoit ses propres informations d'identification CHAP (Challenge-Handshake Authentication Protocol). Vous pouvez accéder aux volumes affectés à un compte en utilisant le nom du compte et les informations d'identification CHAP relatives ou par le biais d'un groupe d'accès de volume. Un compte peut comporter jusqu'à deux milliers de volumes qui lui sont attribués, mais un volume ne peut appartenir qu'à un seul compte.

Création d'une règle de QoS

Utilisez les règles de QoS SolidFire pour créer et enregistrer des paramètres de qualité de service standardisés qui peuvent être appliqués à de nombreux volumes.

Vous pouvez définir des paramètres de QoS par volume. Les performances de chaque volume peuvent être garanties en définissant trois paramètres configurables pour définir les QoS : IOPS min, IOPS max et IOPS en rafale.

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

Paramètre IOPS	Définition	Valeur min	Valeur par défaut	Valeur max. (4 Ko)
IOPS min	Niveau de performance garanti pour un volume.	50	50	15000
IOPS max	La performance ne dépassera pas cette limite.	50	15000	200 000
IOPS en rafale	IOPS maximales autorisées en rafale,	50	15000	200 000

Même si les IOPS maximales et en rafale peuvent être définies jusqu'à 200,000, les performances maximales réelles d'un volume sont limitées par l'utilisation du cluster et les performances par nœud.

La taille et la bande passante des blocs influencent directement le nombre d'opérations d'entrée/sortie par seconde. Lorsque la taille de bloc augmente, le système augmente la bande passante jusqu'au niveau nécessaire pour traiter les tailles de bloc de taille supérieure. Lorsque la bande passante augmente, le nombre d'IOPS augmente, le système peut atteindre une baisse. Pour plus d'informations sur la qualité de service et les performances, reportez-vous à la section "Qualité de service SolidFire".

Authentification SolidFire

Element prend en charge deux méthodes d'authentification : CHAP et VAG (Volume Access Groups). CHAP utilise le protocole CHAP pour authentifier l'hôte au back-end. Les groupes d'accès de volume contrôlent l'accès aux volumes qu'ils provisionne. NetApp recommande d'utiliser le protocole CHAP pour l'authentification, car il est plus simple et ne comporte pas de limites d'évolutivité.

Trident avec le mécanisme de provisionnement CSI amélioré prend en charge l'authentification CHAP. Les VAGs ne doivent être utilisés que dans le mode de fonctionnement traditionnel non CSI.

L'authentification CHAP (vérification que l'initiateur est l'utilisateur de volume prévu) n'est prise en charge qu'avec un contrôle d'accès basé sur le compte. Si vous utilisez CHAP pour l'authentification, deux options sont disponibles : CHAP unidirectionnel et CHAP bidirectionnel. L'authentification CHAP unidirectionnelle authentifie l'accès au volume à l'aide du nom du compte SolidFire et du secret de l'initiateur. L'option CHAP bidirectionnelle fournit le moyen le plus sûr d'authentifier le volume car le volume authentifie l'hôte via le nom du compte et le secret de l'initiateur, puis l'hôte authentifie le volume via le nom du compte et le secret cible.

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

Où trouver plus d'informations ?

Une partie de la documentation sur les meilleures pratiques est présentée ci-dessous. Recherchez les versions les plus récentes dans le "Bibliothèque NetApp".

ONTAP

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

Logiciel Element

- "Configuration de SolidFire pour Linux"

NetApp HCI

- "Conditions préalables au déploiement de NetApp HCI"
- "Accès au moteur de déploiement NetApp"

Information sur les pratiques exemplaires des applications

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

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

Intégrez Trident

Pour intégrer Trident, les éléments de conception et d'architecture suivants nécessitent une intégration : sélection et déploiement des pilotes, conception des classes de stockage, conception des pools virtuels, impact de la demande de volume persistant sur le provisionnement du stockage, les opérations des volumes et le déploiement des services OpenShift à l'aide de Trident.

Choix et déploiement du conducteur

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

Pilotes ONTAP backend

Les pilotes back-end ONTAP sont différenciés par le protocole utilisé et le mode de provisionnement des volumes sur le système de stockage. Par conséquent, réfléchissez bien au choix du conducteur à déployer.

À un niveau plus élevé, si votre application dispose de composants qui nécessitent un stockage partagé (plusieurs modules accédant au même volume de demande de volume persistant), les pilotes NAS seraient la solution par défaut, tandis que les pilotes iSCSI basés sur les blocs répondent aux besoins d'un stockage non partagé. Choisir le protocole en fonction des besoins de l'application et du niveau de confort des équipes chargées du stockage et de l'infrastructure. En règle générale, ces différences sont peu nombreuses pour la plupart des applications. La décision dépend donc souvent de la nécessité d'un stockage partagé (dans lequel plusieurs pods auront besoin d'un accès simultané).

Les pilotes ONTAP backend disponibles sont les suivants :

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

Le choix entre les trois pilotes NAS a des ramifications sur les fonctionnalités mises à disposition de l'application.

Notez que dans les tableaux ci-dessous, toutes les fonctionnalités ne sont pas exposées via Trident. L'administrateur du stockage doit appliquer une partie après le provisionnement si cette fonctionnalité est souhaitée. Les notes de bas de page en exposant distinguent les fonctionnalités par fonction et pilote.

Pilotes NAS de ONTAP	Snapshots	Clones	Règles d'exportation dynamiques	Multi-attacher	La QoS	Redimensionner	La réplication
`ontap-nas`	Oui	Oui	Note de bas de page : 5[]	Oui	Note de bas de page : 1[]	Oui	Note de bas de page : 1[]
`ontap-nas-economy`	Note de bas de page : 3[]	Note de bas de page : 3[]	Note de bas de page : 5[]	Oui	Note de bas de page : 3[]	Oui	Note de bas de page : 3[]
`ontap-nas-flexgroup`	Note de bas de page : 1[]	NON	Note de bas de page : 5[]	Oui	Note de bas de page : 1[]	Oui	Note de bas de page : 1[]

Trident propose 2 pilotes SAN pour ONTAP, dont les fonctionnalités sont indiquées ci-dessous.

Pilotes SAN de ONTAP	Snapshots	Clones	Multi-attacher	Chap bi-directionnel	La QoS	Redimensionner	La réplication
`ontap-san`	Oui	Oui	Note de bas de page : 4[]	Oui	Note de bas de page : 1[]	Oui	Note de bas de page : 1[]
`ontap-san-economy`	Oui	Oui	Note de bas de page : 4[]	Oui	Note de bas de page : 3[]	Oui	Note de bas de page : 3[]

> Note de bas de page pour les tableaux ci-dessus: Yes [1]: Non géré par Trident Yes [2]: Géré par Trident, mais non par PV granulaire Yes [3]: Non géré par Trident et non par PV granulaire Yes [4]: Supporté pour les volumes de bloc brut Yes [5]: Supporté par Trident

Les fonctionnalités qui ne sont pas granulaires volume persistant sont appliquées à l'ensemble du volume flexible et tous les volumes persistants (qtrees ou LUN inclus dans les volumes FlexVol partagés) partageront une planification commune.

Comme nous le voyons dans les tableaux ci-dessus, la plupart des fonctionnalités entre `ontap-nas` et `ontap-nas-economy` sont identiques. Toutefois, comme `ontap-nas-economy` le pilote limite la capacité à contrôler la planification au niveau de la granularité par volume persistant, cela peut avoir un impact particulier sur la planification de la reprise d'activité et de la sauvegarde. Pour les équipes de développement qui souhaitent exploiter la fonctionnalité de clonage PVC sur le stockage ONTAP, cette fonctionnalité n'est possible que lorsque des pilotes , `ontap-san` ou `ontap-san-economy` sont utilisés `ontap-nas`.

Le `solidfire-san` pilote peut également cloner des ESV.

Pilotes Cloud Volumes ONTAP backend

Cloud Volumes ONTAP assure le contrôle des données et des fonctionnalités de stockage haute performance dans divers cas d'utilisation, notamment pour les partages de fichiers et le stockage de niveau bloc qui servent les protocoles NAS et SAN (NFS, SMB/CIFS et iSCSI). Les pilotes compatibles avec Cloud Volume ONTAP sont `ontap-nas`, `ontap-nas-economy` `ontap-san` et `ontap-san-economy`. Applicable à Cloud Volume ONTAP pour Azure, Cloud Volume ONTAP pour GCP.

Pilotes backend Amazon FSX pour ONTAP

Avec Amazon FSX pour NetApp ONTAP, vous exploitez les fonctionnalités, les performances et les capacités d'administration d'NetApp que vous connaissez déjà, tout en profitant de la simplicité, de l'agilité, de la sécurité et de l'évolutivité du stockage des données sur AWS. FSX pour ONTAP prend en charge de nombreuses fonctionnalités de système de fichiers ONTAP et API d'administration. Les pilotes compatibles avec Cloud Volume ONTAP sont `ontap-nas`, , `ontap-nas-economy` `ontap-nas-flexgroup` `ontap-san` et `ontap-san-economy`.

Pilotes back-end NetApp HCI/SolidFire

Le `solidfire-san` pilote utilisé avec les plateformes NetApp HCI/SolidFire permet à l'administrateur de configurer un back-end Element pour Trident en fonction des limites de QoS. Si vous souhaitez concevoir votre back-end de façon à définir les limites de QoS spécifiques sur les volumes provisionnés par Trident, utilisez le

`type` paramètre dans le fichier back-end. L'administrateur peut également limiter la taille du volume qui pourrait être créé sur le stockage à l'aide du `limitVolumeSize` paramètre. Actuellement, les fonctionnalités de stockage Element comme le redimensionnement de volume et la réplication de volume ne sont pas prises en charge par le `solidfire-san` pilote. Ces opérations doivent être effectuées manuellement via l'interface utilisateur Web du logiciel Element.

Pilote SolidFire	Snapshots	Clones	Multi-attacher	CHAP	La QoS	Redimensionner	La réplication
`solidfire-san`	Oui	Oui	Note de bas de page : 2[]	Oui	Oui	Oui	Note de bas de page : 1[]

> Note de bas de page : Yes [1] : non géré par Trident Yes [2] : pris en charge pour les volumes de bloc brut

Pilotes Azure NetApp Files backend

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

Pour plus d'informations sur ce pilote et sur sa configuration"Configuration Trident back-end pour Azure NetApp Files", reportez-vous à la section .

Pilote Azure NetApp Files	Snapshots	Clones	Multi-attacher	La QoS	Développement	La réplication
`azure-netapp-files`	Oui	Oui	Oui	Oui	Oui	Note de bas de page : 1[]

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

Cloud Volumes Service sur le pilote back-end Google Cloud

Trident utilise le `gcp-cvs` pilote pour établir un lien avec Cloud Volumes Service sur Google Cloud.

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

- Si des pools virtuels sont définis en back-end, Trident essaie de créer un volume dans les pools de stockage Google Cloud auxquels ces pools virtuels sont limités.
- Si les pools virtuels ne sont pas définis dans le back-end, Trident sélectionne un pool de stockage Google Cloud dans les pools de stockage disponibles de la région.

Pour configurer le back-end Google Cloud sur Trident, vous devez spécifier `projectNumber`, `apiRegion` et `apiKey` dans le fichier back-end. Le numéro de projet est indiqué dans la console Google Cloud. La clé API est utilisée depuis le fichier de clé privée du compte de service que vous avez créé lors de la configuration de l'accès API pour Cloud Volumes Service sur Google Cloud.

Pour plus d'informations sur Cloud Volumes Service sur les types de services et les niveaux de service Google Cloud, reportez-vous à "En savoir plus sur la prise en charge de Trident pour CVS pour GCP"la section .

Pilote Cloud Volumes Service pour Google Cloud	Snapshots	Clones	Multi-attacher	La QoS	Développement	La réplication
`gcp-cvs`	Oui	Oui	Oui	Oui	Oui	Disponible uniquement sur le type de service CVS-Performance.

Notes de réplication

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

Conception de classe de stockage

Chaque classe de stockage doit être configurée et appliquée pour créer un objet de classe de stockage Kubernetes. Cette section décrit comment concevoir un système de stockage pour votre application.

Utilisation du système back-end spécifique

Le filtrage peut être utilisé au sein d'un objet de classe de stockage spécifique pour déterminer le pool de stockage ou l'ensemble de pools à utiliser avec cette classe de stockage spécifique. Trois jeux de filtres peuvent être définis dans la classe de stockage : `storagePools`, `additionalStoragePools` et/ou `excludeStoragePools`.

Le `storagePools` paramètre permet de limiter le stockage à l'ensemble de pools correspondant à n'importe quel attribut spécifié. Le `additionalStoragePools` paramètre permet d'étendre l'ensemble des pools utilisés par Trident pour le provisionnement, ainsi que l'ensemble des pools sélectionnés par les attributs et les `storagePools` paramètres. Vous pouvez utiliser l'un ou l'autre paramètre seul ou les deux ensemble pour vous assurer que l'ensemble approprié de pools de stockage est sélectionné.

Le `excludeStoragePools` paramètre est utilisé pour exclure spécifiquement l'ensemble de pools répertoriés qui correspondent aux attributs.

Émuler les règles de QoS

Si vous souhaitez concevoir des classes de stockage pour émuler des stratégies de qualité de service, créez une classe de stockage avec `media` l'attribut comme `hdd` ou `ssd`. En fonction de l' `media`attribut mentionné dans la classe de stockage, Trident sélectionne le back-end approprié qui sert `hdd` ou `ssd` regroupe les agrégats pour correspondre à l'attribut de support, puis dirige le provisionnement des volumes vers l'agrégat spécifique. Nous pouvons donc créer une PRIME DE classe de stockage dont l'attribut aurait `media` été défini et `ssd` qui pourrait être classé comme la politique de QoS PREMIUM. Nous pouvons créer une autre NORME de classe de stockage dont l'attribut de support est défini comme `hdd', qui pourrait être classé comme règle de QoS STANDARD. Nous pourrions également utiliser l'attribut « IOPS » de la classe de stockage pour rediriger le provisionnement vers une appliance Element qui peut être définie comme une règle de QoS.

Utilisation du système back-end en fonction de fonctionnalités spécifiques

Les classes de stockage peuvent être conçues pour diriger le provisionnement des volumes sur un système back-end spécifique, où des fonctionnalités telles que le provisionnement fin et lourd, les copies Snapshot, les clones et le chiffrement sont activées. Pour spécifier le stockage à utiliser, créez des classes de stockage qui spécifient le back-end approprié avec la fonction requise activée.

Pools virtuels

Des pools virtuels sont disponibles pour tous les systèmes Trident back-end. Vous pouvez définir des pools virtuels pour n'importe quel système back-end, à l'aide de n'importe quel pilote fourni par Trident.

Les pools virtuels permettent à un administrateur de créer un niveau d'abstraction sur les systèmes back-end, qui peut être référencé via des classes de stockage, pour une plus grande flexibilité et un placement efficace des volumes dans les systèmes back-end. Différents systèmes back-end peuvent être définis avec la même classe de service. En outre, il est possible de créer plusieurs pools de stockage sur le même back-end, mais avec des caractéristiques différentes. Lorsqu'une classe de stockage est configurée avec un sélecteur portant les étiquettes spécifiques, Trident choisit un back-end qui correspond 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 choisit l'un d'eux pour provisionner le volume.

Conception de pool virtuel

Lors de la création d'un backend, vous pouvez généralement spécifier un ensemble de paramètres. Il était impossible pour l'administrateur de créer un autre système back-end avec les mêmes identifiants de stockage et avec un ensemble de paramètres différent. Grâce à l'introduction de pools virtuels, ce problème a été résolu. Les pools virtuels sont une abstraction de niveau introduite entre le back-end et la classe de stockage Kubernetes. L'administrateur peut ainsi définir des paramètres et des étiquettes que l'on peut référencer via les classes de stockage Kubernetes comme un sélecteur, de façon indépendante du back-end. Des pools virtuels peuvent être définis pour tous les systèmes NetApp back-end pris en charge avec Trident. Il s'agit notamment des systèmes SolidFire/NetApp HCI, ONTAP, Cloud Volumes Service sur GCP et Azure NetApp Files.

> Lors de la définition de pools virtuels, il est recommandé de ne pas tenter de réorganiser l'ordre des pools virtuels existants dans une définition backend. Il est également conseillé de ne pas modifier/modifier les attributs d'un pool virtuel existant et de définir un nouveau pool virtuel à la place.

Émulation de différents niveaux de service/QoS

Il est possible de concevoir des pools virtuels pour émuler des classes de service. Grâce à l'implémentation du pool virtuel pour Cloud volumes Service pour Azure NetApp Files, examinons comment nous pouvons configurer différentes classes de service. Configurer le back-end Azure NetApp Files avec plusieurs étiquettes représentant différents niveaux de performances. Définissez `servicelevel` l'aspect sur le niveau de performance approprié et ajoutez d'autres aspects requis sous chaque étiquette. Créez désormais différentes classes de stockage Kubernetes qui seraient mappées sur différents pools virtuels. En utilisant ce `parameters.selector` champ, chaque classe de stockage indique quels pools virtuels peuvent être utilisés pour héberger un volume.

Attribution d'un ensemble spécifique d'aspects

Il est possible de concevoir plusieurs pools virtuels, dont les aspects sont spécifiques, à partir d'un système back-end unique. Pour ce faire, configurez le back-end avec plusieurs étiquettes et définissez les aspects requis sous chaque étiquette. Créez maintenant différentes classes de stockage Kubernetes à l'aide du `parameters.selector` champ qui serait mappé sur différents pools virtuels. Les volumes provisionnés sur

le back-end possèdent les aspects définis dans le pool virtuel choisi.

Caractéristiques des PVC qui affectent le provisionnement du stockage

Certains paramètres au-delà de la classe de stockage requise peuvent affecter le processus de décision de provisionnement Trident lors de la création d'une demande de volume persistant.

Mode d'accès

Lors de la demande de stockage via un PVC, l'un des champs obligatoires est le mode d'accès. Le mode désiré peut affecter le back-end sélectionné pour héberger la demande de stockage.

Trident tente de faire correspondre le protocole de stockage utilisé avec la méthode d'accès spécifiée selon la matrice suivante. Cette technologie est indépendante de la plateforme de stockage sous-jacente.

	ReadWriteOnce	ReadOnlyMany	ReadWriteMany
ISCSI	Oui	Oui	Oui (bloc brut)
NFS	Oui	Oui	Oui

Toute demande de volume persistant ReadWriteMany soumise à un déploiement Trident sans système back-end NFS configuré entraînera le provisionnement d'un volume. Pour cette raison, le demandeur doit utiliser le mode d'accès qui convient à son application.

Opérations de volume

Modifier les volumes persistants

Les volumes persistants sont, à deux exceptions près, des objets immuables dans Kubernetes. Une fois créée, la règle de récupération et la taille peuvent être modifiées. Toutefois, certains aspects du volume ne peuvent pas être modifiés en dehors de Kubernetes. Vous pouvez ainsi personnaliser le volume pour des applications spécifiques, en veillant à ce que la capacité ne soit pas accidentellement consommée ou tout simplement pour déplacer le volume vers un autre contrôleur de stockage pour n'importe quelle raison.

> Les actuellement sur provisionnement des arborescences Kubernetes ne prennent pas en charge les opérations de redimensionnement des volumes pour les volumes NFS ou iSCSI PVS. Trident prend en charge l'extension des volumes NFS et iSCSI.

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

Création de copies Snapshot de volume à la demande

Trident prend en charge la création de copies Snapshot de volume à la demande et la création d'ESV à partir de copies Snapshot à l'aide du framework CSI. Les snapshots constituent une méthode pratique de conservation des copies ponctuelles des données et ont un cycle de vie indépendant du volume persistant source dans Kubernetes. Ces snapshots peuvent être utilisés pour cloner des demandes de volume persistant.

Créer des volumes à partir de copies Snapshot

Trident prend également en charge la création de volumes Persistentvolumes à partir de snapshots de volumes. Pour ce faire, il suffit de créer une demande de volume persistant et de mentionner l' `datasource` comme instantané requis à partir duquel le volume doit être créé. Trident traitera cette demande de volume persistant en créant un volume avec les données présentes sur le snapshot. Grâce à cette fonctionnalité, il est

possible de dupliquer des données entre régions, de créer des environnements de test, de remplacer un volume de production endommagé ou corrompu dans son intégralité, ou de récupérer des fichiers et des répertoires spécifiques et de les transférer vers un autre volume attaché.

Déplacement des volumes dans le cluster

Les administrateurs du stockage peuvent déplacer des volumes entre les agrégats et les contrôleurs du cluster ONTAP sans interruption pour l'utilisateur du stockage. Cette opération n'affecte ni Trident ni le cluster Kubernetes, tant que l'agrégat de destination est un auquel le SVM utilisé par Trident peut accéder. Important : si l'agrégat vient d'être ajouté au SVM, le back-end devra être actualisé en l'ajoutant à Trident. Cela déclenchera Trident à réinventorier le SVM afin que le nouvel agrégat soit reconnu.

Cependant, la migration de volumes entre systèmes back-end n'est pas prise 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 fonctionnalité d'importation de volume peut être utilisée pour importer les volumes actuels dans Trident.

Développement des volumes

Trident prend en charge le redimensionnement des volumes persistants NFS et iSCSI. Les utilisateurs peuvent ainsi redimensionner leurs volumes directement via la couche Kubernetes. L'extension de volume est possible pour toutes les principales plateformes de stockage NetApp, y compris ONTAP, SolidFire/NetApp HCI et les systèmes back-end Cloud Volumes Service. Pour autoriser une éventuelle extension ultérieurement, définissez `allowVolumeExpansion` sur `true` dans votre classe de stockage associée au volume. Lorsque le volume persistant doit être redimensionné, modifiez l' `spec.resources.requests.storage`annotation de la demande de volume persistant en fonction de la taille de volume requise. Trident s'occupe automatiquement du redimensionnement du volume sur le cluster de stockage.

Importer un volume existant dans Kubernetes

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

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

Si le `azure-netapp-files` pilote ou `gcp-cvs` est utilisé, utilisez la commande `tridentctl import volume <backend-name> <volume path> -f /path/pvc.yaml` pour importer le volume dans Kubernetes et le gérer par Trident. Cela garantit une référence de volume unique.

Lors de l'exécution de la commande ci-dessus, Trident trouve le volume sur le back-end et lit sa taille. Il ajoute automatiquement (et écrase si nécessaire) la taille du volume de la demande de volume configurée. Trident crée ensuite le nouveau volume persistant et Kubernetes lie la demande de volume persistant.

Lorsqu'un conteneur a été déployé de façon à ce qu'il ait besoin de la demande de volume persistant importée spécifique, il resterait dans un état en attente jusqu'à ce que la paire PVC/PV soit liée via le processus

d'importation de volume. Une fois la paire PVC/PV liée, le conteneur doit s'installer, à condition qu'il n'y ait pas d'autres problèmes.

Le déploiement des services OpenShift

Les services de cluster à valeur ajoutée OpenShift offrent des fonctionnalités importantes aux administrateurs de clusters et aux applications hébergées. Le stockage utilisé par ces services peut être provisionné à l'aide des ressources locales. Toutefois, la capacité, la performance, la récupération et la durabilité du service sont souvent limitées. En tirant parti d'une baie de stockage d'entreprise pour fournir la capacité nécessaire à ces services, nous pouvons obtenir un service considérablement amélioré. Cependant, comme pour toutes les applications, OpenShift et les administrateurs de stockage doivent travailler en étroite collaboration afin de déterminer les options les plus adaptées à chacun d'entre eux. La documentation Red Hat doit être largement exploitée pour déterminer les exigences et s'assurer que les besoins en matière de dimensionnement et de performances sont satisfaits.

Service de registre

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

Service de journalisation

Comme les autres services OpenShift, le service de journalisation est déployé à l'aide d'Ansible avec les paramètres de configuration fournis par le fichier d'inventaire, également appelé hôtes, fourni avec le PlayBook. Deux méthodes d'installation sont proposées : le déploiement de la journalisation lors de l'installation initiale d'OpenShift et le déploiement de la journalisation une fois OpenShift installé.

> À partir de la version 3.9 de Red Hat OpenShift, la documentation officielle recommande à NFS d'utiliser le service de journalisation en raison de problèmes de corruption des données. Ceci est basé sur les tests Red Hat de leurs produits. Le serveur NFS ONTAP ne présente pas ces problèmes et peut facilement soutenir un déploiement de journalisation. En fin de compte, le choix du protocole pour le service de journalisation constitue un bon choix. Il suffit de savoir que les deux fonctionneront bien avec les plateformes NetApp. Il n'y a aucune raison d'éviter NFS si c'est votre choix.

Si vous choisissez d'utiliser NFS avec le service de journalisation, vous devez définir la variable Ansible `openshift_enable_unsupported_configurations` sur `true` pour empêcher l'échec du programme d'installation.

Commencez

Le service de journalisation peut, éventuellement, être déployé pour les deux applications ainsi que pour les opérations de base du cluster OpenShift. Si vous choisissez de déployer la journalisation des opérations, en spécifiant la variable `openshift_logging_use_ops` comme `true`, deux instances du service seront créées. Les variables qui contrôlent l'instance de journalisation des opérations contiennent des "OPS", alors que l'instance des applications ne le fait pas.

Il est important de configurer les variables Ansible selon la méthode de déploiement afin de s'assurer que le stockage approprié est utilisé par les services sous-jacents. Examinons les options de chacune des méthodes de déploiement.

Les tableaux ci-dessous contiennent uniquement les variables pertinentes pour la configuration du stockage en ce qui concerne le service de journalisation. Vous trouverez d'autres options "Documentation de journalisation Red Hat OpenShift"qui doivent être vérifiées, configurées et utilisées en fonction de votre déploiement.

Les variables du tableau ci-dessous entraînent la création d'un volume persistant et de demande de volume persistant pour le service de journalisation à l'aide des informations fournies. Cette méthode est beaucoup moins flexible qu'avec le manuel d'installation des composants après l'installation d'OpenShift. Toutefois, si des volumes sont déjà disponibles, il s'agit d'une option.

Variable	Détails
`openshift_logging_storage_kind`	Définissez sur `nfs` pour que le programme d'installation crée un fichier PV NFS pour le service de journalisation.
`openshift_logging_storage_host`	Le nom d'hôte ou l'adresse IP de l'hôte NFS. Il doit être défini sur la LIF de données pour votre machine virtuelle.
`openshift_logging_storage_nfs_directory`	Chemin de montage pour l'exportation NFS. Par exemple, si le volume est relié par jonction à `/openshift_logging`, vous utiliseriez ce chemin pour cette variable.
`openshift_logging_storage_volume_name`	Le nom, par exemple `pv_ose_logs`, du volume persistant 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 doivent être configurées.

Variable	Détails
`openshift_logging_es_pvc_dynamic`	Définis sur true pour l'utilisation de volumes provisionnés dynamiquement.
`openshift_logging_es_pvc_storage_class_name`	Nom de la classe de stockage qui sera utilisée dans le PVC.
`openshift_logging_es_pvc_size`	Taille du volume demandé dans la demande de volume persistant.
`openshift_logging_es_pvc_prefix`	Préfixe pour les ESV utilisés par le service de journalisation.
`openshift_logging_es_ops_pvc_dynamic`	Définissez sur `true` pour utiliser les volumes provisionnés dynamiquement pour l'instance de journalisation des opérations.
`openshift_logging_es_ops_pvc_storage_class_name`	Nom de la classe de stockage de l'instance de journalisation OPS.
`openshift_logging_es_ops_pvc_size`	Taille de la demande de volume pour l'instance OPS.
`openshift_logging_es_ops_pvc_prefix`	Préfixe pour les ESV de l'instance OPS.

Déploiement de la pile de consignation

Si vous déployez la connexion dans le cadre du processus d'installation initiale d'OpenShift, il vous suffit de suivre le processus de déploiement standard. Ansible configure et déploie les services et les objets OpenShift nécessaires, de sorte que le service soit disponible dès qu'Ansible se termine.

Cependant, si vous déployez après l'installation initiale, vous devez utiliser le PlayBook des composants Ansible. Ce processus peut varier légèrement avec les différentes versions d'OpenShift. Assurez-vous de lire et de suivre "Documentation Red Hat OpenShift Container Platform 3.11"votre version.

Services de metrics

Le service de metrics fournit à l'administrateur des informations précieuses sur l'état, l'utilisation des ressources et la disponibilité du cluster OpenShift. Il est également nécessaire d'utiliser la fonctionnalité de montée en charge automatique des pods. De nombreuses entreprises utilisent les données issues du service de metrics pour leurs applications de refacturation et/ou de show-back.

Comme pour le service de journalisation, OpenShift dans son ensemble, Ansible est utilisé pour déployer le service de metrics. De même, tout comme le service de journalisation, le service de metrics peut être déployé lors de la configuration initiale du cluster ou après son fonctionnement à l'aide de la méthode d'installation des composants. Les tableaux suivants contiennent les variables importantes lors de la configuration du stockage persistant pour le service de metrics.

Les tableaux ci-dessous contiennent uniquement les variables pertinentes pour la configuration du stockage car elles concernent le service de metrics. De nombreuses autres options sont disponibles dans la documentation qui doit être examinée, configurée et utilisée en fonction de votre déploiement.

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

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

Variable	Détails
`openshift_metrics_cassandra_pvc_prefix`	Préfixe à utiliser pour les ESV de metrics.
`openshift_metrics_cassandra_pvc_size`	Taille des volumes à demander.

Variable	Détails
`openshift_metrics_cassandra_storage_type`	Le type de stockage à utiliser pour les metrics, doit être défini sur dynamique pour qu'Ansible crée des demandes de volume persistant avec la classe de stockage appropriée.
`openshift_metrics_cassanda_pvc_storage_class_name`	Nom de la classe de stockage à utiliser.

Déployez le service de metrics

Déployez le service à l'aide des variables Ansible appropriées définies dans votre fichier hôtes/d'inventaire. Si vous déployez au moment de l'installation d'OpenShift, le volume persistant est créé et utilisé automatiquement. Si vous déployez à l'aide des playbooks des composants après l'installation d'OpenShift, Ansible crée les demandes PVCS requises et, une fois que Trident a provisionné le stockage pour eux, déployez le service.

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

Protection des données et reprise d'activité

En savoir plus sur les options de protection et de restauration pour Trident et les volumes créés à l'aide de Trident. Vous devez disposer d'une stratégie de protection et de restauration des données pour chaque application ayant des exigences de persistance.

Réplication et restauration Trident

En cas d'incident, vous pouvez créer une sauvegarde pour restaurer Trident.

Réplication Trident

Trident utilise des CRD Kubernetes pour stocker et gérer son propre état ainsi que celui du cluster Kubernetes pour stocker ses métadonnées.

Étapes

1. Sauvegardez le cluster Kubernetes etcd à l'aide de "Kubernetes : sauvegarde d'un cluster ETCD".
2. Placez les artéfacts de sauvegarde sur une FlexVol.

> Nous vous recommandons de protéger la SVM où réside la FlexVol avec une relation SnapMirror vers une autre SVM.

Restauration Trident

Avec les CRD Kubernetes et le snapshot de type ETCD du cluster Kubernetes, vous pouvez restaurer Trident.

Étapes

1. Depuis le SVM de destination, monter le volume qui contient les fichiers de données et les certificats Kubernetes sur l'hôte qui sera configuré en tant que nœud maître.

2. Copiez tous les certificats requis en rapport avec le cluster Kubernetes sous `/etc/kubernetes/pki` et les fichiers membres ETCD sous `/var/lib/etcd`.
3. Restaurez le cluster Kubernetes à partir de la sauvegarde etcd à l'aide de "Kubernetes : restauration d'un cluster ETCD".
4. Exécutez `kubectl get crd` pour vérifier que toutes les ressources personnalisées Trident sont bien présentes et récupérez les objets Trident pour vérifier que toutes les données sont disponibles.

Réplication et restauration des SVM

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

En cas d'incident, vous pouvez activer la SVM de destination SnapMirror pour démarrer le service des données. Vous pouvez revenir au système principal lorsque les systèmes sont restaurés.

Description de la tâche

Tenir compte des points suivants lors de l'utilisation de la fonction de réplication SVM SnapMirror :

- Vous devez créer un back-end distinct pour chaque SVM lorsque la fonction SVM-DR est activée.
- Configurez les classes de stockage pour sélectionner les systèmes back-end répliqués uniquement en cas de besoin, afin d'éviter que des volumes ne nécessitant pas de réplication provisionnée vers les systèmes back-end qui prennent en charge la SVM-DR.
- Les administrateurs d'applications doivent comprendre les coûts et la complexité supplémentaires associés à la réplication et tenir compte de leur plan de reprise avant de commencer ce processus.

Réplication SVM

Utiliser "ONTAP : réplication SVM SnapMirror" pour créer la relation de réplication du SVM.

SnapMirror vous permet de définir des options pour contrôler ce qui doit être répliqué. Vous devez savoir quelles options vous avez sélectionnées lors de la préformation Restauration des SVM à l'aide de Trident.

- "-identité-préserver vrai" Réplique l'ensemble de la configuration du SVM.
- "-discard-configs réseau" Exclut les LIFs et les paramètres réseau associés.
- "-identity-preserve false" réplique uniquement les volumes et la configuration de sécurité.

Restauration des SVM à l'aide de Trident

Trident ne détecte pas automatiquement les défaillances des SVM. En cas d'incident, l'administrateur peut initier manuellement le basculement de Trident vers le nouveau SVM.

Étapes

1. Annuler les transferts SnapMirror planifiés et en cours, rompre la relation de réplication, arrêter la SVM source, puis activer la SVM de destination SnapMirror.
2. Si vous avez spécifié `-identity-preserve false` ou `-discard-config network` lors de la configuration de la réplication de votre SVM, mettez à jour les `managementLIF` et `dataLIF` dans le fichier de définition du back-end Trident.
3. Vérifiez que `storagePrefix` est présent dans le fichier de définition du back-end Trident. Ce paramètre ne peut pas être modifié. L'omission `storagePrefix` entraînera l'échec de la mise à jour du back-end.

4. Mettre à jour tous les systèmes back-end nécessaires pour indiquer le nom du nouveau SVM de destination à l'aide de :

```
./tridentctl update backend <backend-name> -f <backend-json-file> -n
<namespace>
```

5. Si vous avez spécifié `-identity-preserve false` ou `discard-config network`, vous devez rebondir tous les pods d'application.

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

Réplication et restauration de volume

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

Vous pouvez ensuite importer les volumes récupérés dans Trident à l'aide de "importation de volume tridentctl".

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

Protection des données Snapshot

Vous pouvez protéger et restaurer les données à l'aide des éléments suivants :

- Un contrôleur de snapshot externe et des CRD pour créer des copies Snapshot de volume Kubernetes de volumes persistants (PVS).

  "Snapshots de volume"

- Snapshots ONTAP pour restaurer le contenu complet d'un volume ou pour restaurer des fichiers individuels ou des LUN.

  "Snapshots ONTAP"

Sécurité

Sécurité

Suivez les recommandations ci-dessous pour vous assurer 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 d'assurer un stockage fiable

et de bloquer les activités malveillantes potentielles.

Pour séparer les autres applications et utilisateurs de Trident, installez toujours Trident dans son propre espace de noms Kubernetes (`trident`). Le placement de Trident dans son propre espace de noms permet de garantir que seules les équipes d'administration Kubernetes ont accès au pod Trident et aux artéfacts (comme les secrets back-end et CHAP, le cas échéant) stockés dans les objets CRD dont le nom a été donné. Vous devez vous assurer d'autoriser uniquement les administrateurs à accéder à l'espace de noms Trident et donc à l' `tridentctl`application.

Utilisez l'authentification CHAP avec les systèmes back-end ONTAP SAN

Trident prend en charge l'authentification CHAP pour les charges de travail SAN ONTAP (à l'aide `ontap-san` de pilotes et `ontap-san-economy`). NetApp recommande l'utilisation du protocole CHAP bidirectionnel avec Trident pour l'authentification entre un hôte et le back-end de stockage.

Pour les systèmes back-end ONTAP qui utilisent des pilotes de stockage SAN, Trident peut configurer le protocole CHAP bidirectionnel et gérer les noms d'utilisateur et les secrets CHAP via `tridentctl`. Reportez-vous à la section "Préparez la configuration du système back-end avec les pilotes SAN ONTAP" pour savoir comment Trident configure CHAP sur des systèmes back-end ONTAP.

Utilisez l'authentification CHAP avec les systèmes back-end NetApp HCI et SolidFire

NetApp recommande de déployer le protocole CHAP bidirectionnel pour garantir l'authentification entre l'hôte et les systèmes back-end NetApp HCI et SolidFire. 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 `tridentvolume` objet CR pour le PV correspondant. Lorsque vous créez un volume persistant, Trident utilise les secrets CHAP pour lancer 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 de volume.

Utilisez Trident avec NVE et NAE

NetApp ONTAP assure le chiffrement des données au repos pour protéger les données sensibles en cas de vol, de retour ou de reconversion d'un disque. Pour plus de détails, reportez-vous à "Configurer la présentation de NetApp Volume Encryption".

- Si NAE est activé sur le back-end, tout volume provisionné dans Trident est activé.
- Si NAE n'est pas activé sur le back-end, tout volume provisionné dans Trident est activé sur NVE, à moins que vous ne définiez l'indicateur de chiffrement NVE sur `false` dans la configuration back-end.

ⓘ Les volumes créés dans Trident sur un système back-end NAE doivent être chiffrés NVE ou NAE.

  - Vous pouvez définir l'indicateur de chiffrement NVE sur `true` dans la configuration back-end Trident pour remplacer le chiffrement NAE et utiliser une clé de chiffrement spécifique par volume.
  - La définition de l'indicateur de chiffrement NVE `false` sur un système back-end compatible NAE crée un volume compatible NAE. Vous ne pouvez pas désactiver le chiffrement NAE en configurant l'indicateur de chiffrement NVE sur `false`.

- Vous pouvez créer manuellement un volume NVE dans Trident en définissant explicitement l'indicateur de

chiffrement NVE sur `true`.

Pour plus d'informations sur les options de configuration du back-end, reportez-vous à :

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

Configuration de clé unifiée Linux (LUKS)

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

Dans Trident, les volumes chiffrés LUKS utilisent le cypher et le mode aes-xts-mclair 64, comme recommandé par "NIST".

Avant de commencer

- Les nœuds worker doivent avoir cryptsetup 2.1 ou supérieur (mais inférieur à 3.0) installé. Pour plus d'informations, visitez "Gitlab : cryptsetup".
- Pour des raisons de performances, nous recommandons aux nœuds workers de prendre en charge les nouvelles instructions AES-ni (Advanced Encryption Standard New instructions). Pour vérifier la prise en charge AES-ni, exécutez la commande suivante :

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

Si rien n'est renvoyé, votre processeur ne prend pas en charge AES-ni. Pour plus d'informations sur AES-ni, visitez le site : "Intel : instructions AES-ni (Advanced Encryption Standard instructions)".

Activez le cryptage LUKS

Vous pouvez activer le chiffrement côté hôte par volume en utilisant Linux Unified Key Setup (LUKS) pour SAN ONTAP et les volumes ÉCONOMIQUES SAN ONTAP.

Étapes

1. Définissez les attributs de cryptage LUKS dans la configuration back-end. Pour plus d'informations sur les options de configuration back-end pour le SAN ONTAP, reportez-vous à la section "Options de configuration du stockage SAN ONTAP".

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

2. `parameters.selector`Permet de définir les pools de stockage à l'aide du cryptage LUKS. Par exemple :

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

3. Créez un secret qui contient la phrase de passe LUKS. Par exemple :

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

Limites

Les volumes LUKS-chiffrés ne peuvent pas tirer parti de la déduplication et de la compression ONTAP.

Configuration back-end pour l'importation de volumes LUKS

Pour importer un volume LUKS, vous devez définir `luksEncryption` sur sur(`true` le back-end. L' `luksEncryption`option indique à Trident si le volume est conforme LUKS (`true`) ou non conforme LUKS) (`false`comme indiqué dans l'exemple suivant.

```
version: 1
storageDriverName: ontap-san
managementLIF: 10.0.0.1
dataLIF: 10.0.0.2
svm: trident_svm
username: admin
password: password
defaults:
  luksEncryption: 'true'
  spaceAllocation: 'false'
  snapshotPolicy: default
  snapshotReserve: '10'
```

Configuration PVC pour l'importation de volumes LUKS

Pour importer des volumes LUKS de façon dynamique, définissez l'annotation `trident.netapp.io/luksEncryption` sur `true` et incluez une classe de stockage LUKS activée dans la demande de volume virtuel, comme indiqué dans cet exemple.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: luks-sc
```

Faites pivoter une phrase de passe LUKS

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

N'oubliez pas une phrase de passe tant que vous n'avez pas vérifié qu'elle n'est plus référencée par un volume, un snapshot ou un secret. En cas de perte d'une phrase secrète référencée, vous risquez de ne pas pouvoir monter le volume et les données resteront cryptées et inaccessibles.

Description de la tâche

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

- Si la phrase de passe du volume ne correspond pas à la phrase de passe active dans le secret, la rotation se produit.
- Si la phrase de passe du volume correspond à la phrase de passe active du secret, le `previous-luks-passphrase` paramètre est ignoré.

Étapes

1. Ajoutez les `node-publish-secret-name` paramètres et `node-publish-secret-namespace` StorageClass. Par exemple :

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

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

Volumétrie

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

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

Snapshot

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

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

3. Mettez à jour le secret LUKS pour le volume afin de spécifier les phrases de passe nouvelles et précédentes. Assurez-vous que `previous-luke-passphrase-name` `previous-luks-passphrase`la phrase de passe précédente est identique.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Créez un nouveau pod qui monte le volume. Ceci est nécessaire pour lancer la rotation.
5. Vérifiez que la phrase de passe a été pivotée.

Volumétrie

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

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

Snapshot

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

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

Résultats

La phrase de passe a été pivotée lorsque seule la nouvelle phrase de passe est renvoyée sur le volume et le snapshot.

> Si deux phrases de passe sont renvoyées, par exemple `luksPassphraseNames: ["B", "A"]`, la rotation est incomplète. Vous pouvez déclencher un nouveau pod pour tenter de terminer la rotation.

Activer l'extension de volume

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

Étapes

1. Activez la `CSINodeExpandSecret` fonctionnalité Gate (bêta 1.25+). Voir "Kubernetes 1.25 : utilisez les secrets de l'extension des volumes CSI basée sur des nœuds" pour plus de détails.

2. Ajoutez les `node-expand-secret-name` paramètres et `node-expand-secret-namespace` StorageClass. Par exemple :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: csi.trident.netapp.io
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

Résultats

Lorsque vous initiez l'extension du stockage en ligne, le kubelet transmet les identifiants appropriés au pilote.

Chiffrement Kerberos à la volée

Avec le chiffrement à la volée Kerberos, vous pouvez améliorer la sécurité d'accès aux données en activant le chiffrement pour le trafic entre votre cluster géré et le back-end de stockage.

Trident prend en charge le chiffrement Kerberos pour ONTAP en tant que back-end de stockage :

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

Vous pouvez créer, supprimer, redimensionner, snapshot, cloner clone en lecture seule et importation des volumes qui utilisent le chiffrement NFS.

Configurez le chiffrement Kerberos à la volée avec les volumes ONTAP sur site

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

> Le chiffrement Kerberos pour le trafic NFS avec les systèmes back-end de stockage ONTAP sur site est uniquement pris en charge à l'aide du `ontap-nas` pilote de stockage.

Avant de commencer

- Vérifiez que vous avez accès à l' `tridentctl` utilitaire.
- Assurez-vous de disposer d'un accès administrateur au système back-end de stockage ONTAP.
- Assurez-vous de connaître le nom du ou des volumes que vous allez partager à partir du back-end de stockage ONTAP.

- Assurez-vous d'avoir préparé la machine virtuelle de stockage ONTAP à prendre en charge le chiffrement Kerberos pour les volumes NFS. Reportez-vous "Activez Kerberos sur une LIF donnée" à pour obtenir des instructions.
- Vérifiez que tous les volumes NFSv4 utilisés avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section Configuration du domaine NetApp NFSv4 (page 13) du "Guide des améliorations et des bonnes pratiques de NetApp NFSv4".

Ajoutez ou modifiez les règles d'export ONTAP

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

Protocoles d'accès

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

Accédez aux informations

Vous pouvez configurer l'une des trois versions différentes du cryptage Kerberos, en fonction de vos besoins pour le volume :

- **Kerberos 5** - (authentification et cryptage)
- **Kerberos 5i** - (authentification et chiffrement avec protection d'identité)
- **Kerberos 5p** - (authentification et chiffrement avec protection de l'identité et de la vie privée)

Configurez la règle d'export ONTAP avec les autorisations d'accès appropriées. Par exemple, si les clusters montant les volumes NFS avec un mélange de cryptage Kerberos 5i et Kerberos 5p, utilisez les paramètres d'accès suivants :

Type	Accès en lecture seule	Accès en lecture/écriture	Accès superutilisateur
UNIX	Activé	Activé	Activé
Kerberos 5i	Activé	Activé	Activé
Kerberos 5p	Activé	Activé	Activé

Pour plus d'informations sur la création de règles d'export ONTAP et de règles d'export-policy, reportez-vous à la documentation suivante :

- "Créer une export-policy"
- "Ajouter une règle à une export-policy"

Créer un back-end de stockage

Vous pouvez créer une configuration back-end de stockage Trident qui inclut une fonctionnalité de chiffrement Kerberos.

Description de la tâche

Lorsque vous créez un fichier de configuration du back-end de stockage qui configure le chiffrement Kerberos, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du

`spec.nfsMountOptions` paramètre :

- `spec.nfsMountOptions: sec=krb5` (authentification et chiffrement)
- `spec.nfsMountOptions: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `spec.nfsMountOptions: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la confidentialité)

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

Étapes

1. Sur le cluster géré, créez un fichier de configuration du back-end de stockage à l'aide de l'exemple suivant. Remplacez les valeurs entre parenthèses <> par les informations de votre environnement :

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

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

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

```
tridentctl logs
```

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

Créer une classe de stockage

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

Description de la tâche

Lorsque vous créez un objet classe de stockage, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du `mountOptions` paramètre :

- `mountOptions: sec=krb5` (authentification et chiffrement)
- `mountOptions: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `mountOptions: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la confidentialité)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de cryptage Kerberos dans la liste des paramètres, seule la première option est utilisée. Si le niveau de chiffrement que vous avez spécifié dans la configuration du back-end de stockage est différent du niveau que vous spécifiez dans l'objet classe de stockage, l'objet classe de stockage a priorité.

Étapes

1. Créez un objet StorageClass Kubernetes à l'aide de l'exemple suivant :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Créer la classe de stockage :

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Assurez-vous que la classe de stockage a été créée :

```
kubectl get sc ontap-nas-sc
```

Vous devez voir les résultats similaires à ce qui suit :

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

Provisionner les volumes

Une fois que vous avez créé un système back-end et une classe de stockage, vous pouvez provisionner un volume. Pour obtenir des instructions, reportez-vous à "Provisionner un volume" la .

Configurez le chiffrement Kerberos à la volée avec les volumes Azure NetApp Files

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un seul système back-end de stockage Azure NetApp Files ou un pool virtuel de systèmes back-end de stockage Azure NetApp Files.

Avant de commencer

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

Créer un back-end de stockage

Vous pouvez créer une configuration back-end de stockage Azure NetApp Files qui inclut une fonctionnalité de chiffrement Kerberos.

Description de la tâche

Lorsque vous créez un fichier de configuration du back-end de stockage qui configure le cryptage Kerberos, vous pouvez le définir de manière à ce qu'il soit appliqué à l'un des deux niveaux possibles :

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

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

À chaque niveau, vous pouvez spécifier l'une des trois versions différentes du cryptage Kerberos :

- `kerberos: sec=krb5` (authentification et chiffrement)

- `kerberos: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `kerberos: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la confidentialité)

Étapes

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

Exemple au niveau du back-end de stockage

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

Exemple de pool virtuel

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-secret
```

2. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

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

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

```
tridentctl logs
```

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

Créer une classe de stockage

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

Étapes

1. Créez un objet StorageClass Kubernetes à l'aide de l'exemple suivant :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Créer la classe de stockage :

```
kubectl create -f sample-input/storage-class-sc-nfs.yaml
```

3. Assurez-vous que la classe de stockage a été créée :

```
kubectl get sc -sc-nfs
```

Vous devez voir les résultats similaires à ce qui suit :

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

Provisionner les volumes

Une fois que vous avez créé un système back-end et une classe de stockage, vous pouvez provisionner un volume. Pour obtenir des instructions, reportez-vous à "Provisionner un volume" la .