Meilleures pratiques et recommandations

Astra Trident

NetApp
November 20, 2023

Sommaire

Meilleures pratiques et recommandations

Déploiement

Utilisez les recommandations indiquées ici pour déployer Astra Trident.

Déploiement dans un namespace dédié

"Espaces de noms" séparation des tâches administratives entre les différentes applications et barrière au partage des ressources. Par exemple, un volume persistant ne peut pas être consommé depuis un autre espace de noms. Astra Trident fournit des ressources PV à tous les namespaces du cluster Kubernetes et exploite par conséquent un compte de service avec des privilèges élevés.

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

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

Kubernetes dispose de deux fonctionnalités qui, lorsqu'elles sont combinées, fournissent un mécanisme puissant pour limiter la consommation des ressources par les applications. Le "mécanisme de quotas de stockage" permet à l'administrateur d'implémenter des limites d'utilisation globales et spécifiques aux classes de stockage, à la capacité et au nombre d'objets, sur la base de chaque espace de noms. En outre, à l'aide d'un "limite de plage" Veille à ce que les demandes de volume persistant se situent dans une valeur minimale et maximale avant que la requête ne soit transférée au mécanisme de provisionnement.

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. Trident fonctionne avec chacune des principales plateformes : ONTAP, Element et E-Series. 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. Indépendamment de la situation, le LIF de gestion doit être accessible via DNS pour faciliter une flexibilité maximale "SVM-DR" Utilisation en association 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. Voir "NetApp Hardware Universe" Pour votre plateforme et votre version ONTAP afin de déterminer les limites exactes. Lorsque le nombre de volumes est épuisé, les opérations de provisionnement échouent non seulement pour Trident, mais pour l'ensemble des requêtes de stockage.

Trident `ontap-nas` et `ontap-san` Des pilotes provisionnent un volume flexible pour chaque volume persistant Kubernetes créé. Le `ontap-nas-economy` Le pilote crée environ un FlexVolume pour chaque 200 PVS (configurable entre 50 et 300). Le `ontap-san-economy` Le pilote crée environ un FlexVolume pour chaque 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 pour `max-volumes` varie en fonction de plusieurs critères spécifiques à votre environnement :

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

Le `max-volumes` Valeur est le volume total provisionné 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. Cependant, si seulement "64 bits" Depuis un nœud

est attribué à la SVM, ou 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 alors la cible de tous les volumes provisionnés par Trident. Cela signifie que le volume peut être atteint en limite pour ce nœud avant le `max-volumes` La valeur est atteinte, ce qui affecte Trident et les autres opérations de volume utilisant 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 la `limitVolumeSize` dans votre `backend.json` définition.

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

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. À l'aide du `useCHAP` Paramètre dans votre configuration back-end, Trident authentifie les connexions iSCSI pour les systèmes back-end ONTAP avec CHAP. La prise en charge CHAP bidirectionnelle est disponible avec Trident 20.04 et versions ultérieures.

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 de "évitez un tyran" Ou un conteneur hors contrôle de affectant les charges de travail en dehors du 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 la QoS, voir "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 le `qosPolicy` saisissez 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 « policy Groups » de QoS, reportez-vous à la section "Commandes QoS de ONTAP 9.8".

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 éviter 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. Par défaut, ces dernières ne sont pas refusées. Veillez donc à désactiver cette fonctionnalité en utilisant "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 qui disposent de nœuds d'infrastructure dédiés (OpenShift, par exemple) ou d'autres nœuds ne pouvant pas être planificateurs pour les applications utilisateur, il est recommandé d'utiliser des règles d'exportation distinctes 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'exportation depuis la version 20.04. 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 :

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

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

Désactiver `showmount` Pour le SVM applicatif

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 lancer le `showmount -e` Commande au niveau de la LIF de données et reçoit la liste des montages disponibles, y compris ceux auxquels elle 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.

Vous devez désactiver `showmount` En utilisant 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	Minimum valeur	Valeur par défaut	Capacité Valeur (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. Voir "Qualité de service SolidFire" Pour plus d'informations sur la qualité de service et les performances.

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.

Meilleures pratiques des E-Series

Découvrez les bonnes pratiques pour la configuration du stockage E-Series pour Trident.

Pools de disques et groupes de volumes E-Series

Créez des pools de disques et des groupes de volumes en fonction de vos besoins et déterminez comment la capacité de stockage totale doit être organisée en volumes et partagée entre les hôtes. Le pool de disques et le groupe de volumes se composent d'un ensemble de disques regroupés de manière logique pour fournir un ou plusieurs volumes à un hôte d'application. Tous les lecteurs d'un pool de disques ou d'un groupe de volumes doivent être du même type de support.

Groupes d'hôtes E-Series

Trident utilise des groupes d'hôtes pour accéder aux volumes (LUN) qu'il provisionne. Par défaut, Trident utilise le groupe hôte appelé `trident` sauf si vous spécifiez un autre nom de groupe d'hôtes dans la configuration. Trident, ne crée ni ne gère en aucun cas les groupes d'hôtes. Vous devez créer le groupe hôte avant que le système back-end de stockage E-Series ne soit configuré sur Trident. Assurez-vous que tous les noms IQN iSCSI des nœuds workers Kubernetes sont mis à jour dans le groupe d'hôtes.

Planification Snapshot des E-Series

Créer un planning de snapshots et affecter le volume créé par Trident à un planning de snapshots afin de réaliser des sauvegardes de volume à l'intervalle requis. En fonction des snapshots pris conformément à la règle de snapshots, les opérations de restauration peuvent être réalisées sur les volumes en restaurant une image Snapshot sur le volume de base. Vous devez utiliser SANtricity System Manager pour créer la planification de snapshots.

Groupes de cohérence Snapshot

La configuration de groupes de cohérence de snapshots est également idéale pour les applications qui s'étendent sur plusieurs volumes. L'objectif d'un groupe de cohérence est de prendre simultanément des snapshots de plusieurs volumes, ce qui garantit des copies cohérentes d'une collection de volumes à un moment donné. Vous devez utiliser SANtricity System Manager pour créer des groupes de cohérence.

Bonnes pratiques Cloud Volumes Service pour AWS

Découvrez les bonnes pratiques pour la configuration d'Cloud Volumes Service sur AWS pour Trident.

Créer une export-policy

Pour vous assurer que seul l'ensemble de nœuds autorisé a accès au volume provisionné via Cloud Volumes Service, définissez les règles appropriées pour l'export policy lors de la création d'un Cloud Volumes Service. Lorsque vous provisionnez des volumes sur Cloud Volume Services via Trident, veillez à utiliser le `exportRule` Paramètre dans le fichier back-end pour donner l'accès aux nœuds Kubernetes requis.

Création d'une règle de snapshots

Créez une règle de snapshots pour les volumes provisionnés via Cloud Volume Service afin de garantir que les snapshots sont réalisés à intervalles réguliers. Les données sont ainsi sauvegardées à intervalles réguliers et peuvent être restaurées en cas de perte ou de corruption. Vous pouvez définir la stratégie de snapshot pour les volumes hébergés par Cloud Volume Service en sélectionnant la planification appropriée sur la page de détails des volumes.

Choisissez le niveau de service, la capacité de stockage et la bande passante de stockage appropriés

Les services Cloud volumes pour AWS proposent différents niveaux de service : standard, premium et extrême. Ces niveaux de service répondent aux besoins différents en capacité de stockage et bande passante de stockage. Assurez-vous de sélectionner le niveau de service approprié en fonction des besoins de votre entreprise.

Vous devez sélectionner la taille de stockage allouée au cours de la création du volume en fonction des besoins spécifiques de l'application. Deux facteurs doivent être pris en considération lors de la décision sur le stockage alloué :

- Besoins de stockage de l'application concernée
- La bande passante dont vous avez besoin au maximum ou à la périphérie

La bande passante de stockage dépend de la combinaison du niveau de service et de la capacité allouée que vous avez sélectionnée. Par conséquent, sélectionnez le niveau de service approprié et la capacité allouée en gardant à l'esprit la bande passante requise.

Limitez la taille maximale des volumes créés par Trident

Il est possible de limiter la taille maximale des volumes créés par Trident sur les services Cloud volumes pour AWS en utilisant la `limitVolumeSize` paramètre dans le fichier de configuration back-end. La définition de ce paramètre garantit que le provisionnement échoue si la taille du volume demandé est supérieure à la valeur définie.

Où trouver plus d'informations ?

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

ONTAP

- "Guide des meilleures pratiques et de mise en œuvre de NFS"
- "Guide d'administration DU 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"

E-Series

- "Installation et configuration pour Linux"

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 d'instructions spécifiques, il est important de collaborer avec votre équipe NetApp et d'utiliser le "Bibliothèque NetApp" pour trouver la documentation la plus récente.

Intégrez Astra Trident

Pour intégrer Astra Trident, les éléments de conception et d'architecture suivants nécessitent l'intégration : sélection des pilotes et déploiement, conception de la classe de stockage, conception de pool de stockage virtuel, impact de la demande de volume persistant sur le provisionnement du stockage, les opérations de volumes et le déploiement de services OpenShift avec Astra Trident.

Choix et déploiement du conducteur

Choisir un pilote back-end pour ONTAP

Les systèmes ONTAP intègrent quatre pilotes de système back-end différents. Ces pilotes sont différenciés par le protocole utilisé et le mode de provisionnement des volumes sur le système de stockage. Par conséquent, prenez garde à prendre en compte le pilote 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 cinq pilotes des systèmes ONTAP back-end sont répertoriés ci-dessous :

- `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 qtrees 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 un LUN au sein de son propre volume FlexVolume.
- `ontap-san-economy`: Chaque volume persistant provisionné est une LUN, avec un nombre configurable de LUN par FlexVolume (la valeur par défaut est 100).

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

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

Pilotes NAS ONTAP	Snapshots	Clones	Règles d'exportation dynamiques	Multi-attacher	La QoS	Redimensionner	La réplication
`ontap-nas`	Oui.	Oui.	Yes [5]	Oui.	Yes [1]	Oui.	Yes [1]
`ontap-nas-economy`	Yes [3]	Yes [3]	Yes [5]	Oui.	Yes [3]	Oui.	Yes [3]
`ontap-nas-flexgroup`	Yes [1]	Non	Yes [5]	Oui.	Yes [1]	Oui.	Yes [1]

Astra Trident propose 2 pilotes SAN pour ONTAP dont les fonctionnalités sont présentées ci-dessous.

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

> Note de bas de page pour les tableaux ci-dessus : Yes [1]: Non géré par Astra Trident Yes [2]: Géré par Astra Trident, mais pas PV granulaire Yes [3]: Non géré par Astra Trident et non PV granulaire Yes [4]: Supporté par 5 Trident pour les volumes en mode bloc brut[]: 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 on peut le voir dans les tableaux ci-dessus, une grande partie des fonctionnalités entre `ontap-nas` et `ontap-nas-economy` est identique. Cependant, parce que le `ontap-nas-economy` Le pilote limite la capacité à contrôler la planification à la granularité par volume persistant, ce qui peut affecter en particulier la

reprise après incident et la planification des sauvegardes. Pour les équipes de développement qui souhaitent exploiter la fonctionnalité de clonage PVC sur le stockage ONTAP, ce n'est possible que lorsque vous utilisez le `ontap-nas`, `ontap-san` ou `ontap-san-economy` pilotes.

> Le `solidfire-san` Le pilote est également capable de cloner des demandes de volume persistant.

Choisir un pilote back-end pour Cloud Volumes ONTAP

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 les `ontap-nas`, `ontap-nas-economy`, `ontap-san` et `ontap-san-economy`. Applicable à Cloud volumes ONTAP pour AWS, Cloud Volume ONTAP pour Azure et Cloud Volume ONTAP pour GCP.

Choisissez un pilote back-end pour Amazon FSX pour ONTAP

Avec Amazon FSX pour ONTAP, les clients peuvent exploiter les fonctions, les performances et les fonctionnalités d'administration NetApp qu'ils connaissent bien, tout en bénéficiant de la simplicité, de l'agilité, de la sécurité et de l'évolutivité du stockage de données sur AWS. FSX pour ONTAP prend en charge de nombreuses fonctionnalités de système de fichiers et API d'administration d'ONTAP. Les pilotes compatibles avec Cloud Volume ONTAP sont les `ontap-nas`, `ontap-nas-economy`, `ontap-nas-flexgroup`, `ontap-san` et `ontap-san-economy`.

Choisissez un pilote back-end pour NetApp HCI/SolidFire

Le `solidfire-san` Pilote utilisé avec les plateformes NetApp HCI/SolidFire pour aider l'administrateur à configurer un back-end Element pour Trident sur la base des limites de QoS. Si vous voulez concevoir votre système back-end pour définir les limites de QoS spécifiques sur les volumes provisionnés par Trident, utilisez la `type` paramètre dans le fichier backend. L'administrateur peut également restreindre la taille du volume pouvant être créé sur le stockage à l'aide de `limitVolumeSize` paramètre. Pour le moment, les fonctionnalités de stockage Element telles que le redimensionnement des volumes et la réplication des volumes ne sont pas prises en charge via le `solidfire-san` conducteur. 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.	Yes [2]	Oui.	Oui.	Oui.	Yes [1]

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

Choisir un pilote back-end pour Azure NetApp Files

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

Vous trouverez plus d'informations sur ce pilote et sa configuration dans le "Configuration back-end d'Astra Trident pour Azure NetApp Files".

Pilote Azure NetApp Files	Snapshots	Clones	Multi-attacher	La QoS	Développement	La réplication
`azure-netapp-files`	Oui.	Oui.	Oui.	Oui.	Oui.	Yes [1]

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

Choisir un pilote back-end pour Cloud Volumes Service avec AWS

Astra Trident utilise le `aws-cvs` Pilote pour la liaison avec le Cloud Volumes Service sur le back-end AWS. Pour configurer le back-end AWS sur Trident, vous devez spécifier `apiRegion`, `apiURL`, `apiKey`, et le `secretKey` dans le fichier backend. Ces valeurs se trouvent sur le portail Web CVS dans Paramètres de compte/accès API. Les niveaux de service pris en charge sont alignés sur CVS et comprennent `standard`, `premium`, et `extreme`. Actuellement, la taille minimale du volume à provisionner est de 100 G. Les futures versions de CVS peuvent supprimer cette restriction.

Pilote CVS pour AWS	Snapshots	Clones	Multi-attacher	La QoS	Développement	La réplication
`aws-cvs`	Oui.	Oui.	Oui.	Oui.	Oui.	Yes [1]

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

Le `aws-cvs` le pilote utilise des pools de stockage virtuel. Les pools de stockage virtuel extraient le système back-end afin que Trident décide du placement des volumes. L'administrateur définit les pools de stockage virtuels dans le(s) fichier(s) backend(s).json. Les classes de stockage identifient les pools de stockage virtuels à l'aide d'étiquettes.

Choisir un pilote back-end pour Cloud Volumes Service avec GCP

Astra Trident utilise le `gcp-cvs` Pilote à lier à Cloud Volumes Service sur le back-end GCP. Pour configurer le back-end GCP sur Trident, vous devez spécifier `projectNumber`, `apiRegion`, et `apiKey` dans le fichier backend. Le numéro de projet est disponible sur le portail Web GCP, tandis que la clé d'API doit être prise depuis le fichier de clé privée du compte de service que vous avez créé lors de la configuration de l'accès aux API pour Cloud volumes sur GCP. Astra Trident peut créer des volumes CVS dans un des deux "types de service":

1. **CVS**: Le type de service CVS de base, qui fournit une haute disponibilité zonale avec des niveaux de performance limités/modérés.
2. **CVS-Performance** : le type de service optimisé pour les performances est le mieux adapté aux charges de travail de production qui exigent des performances élevées. Choisissez parmi trois niveaux de service uniques [`standard`, `premium`, et `extreme`]. Actuellement, la taille minimale du volume CVS-Performance est de 100 Gio, tandis que les volumes CVS doivent être au moins 300 Gio. Les futures versions de CVS peuvent supprimer cette restriction.

> Lors du déploiement des systèmes back-end avec le type de service CVS par défaut [`storageClass=software`], les utilisateurs **doivent obtenir un accès** à la fonctionnalité de volumes de sous-Tio dans GCP pour le(s) numéro(s) de projet et ID de projet en question. Il est nécessaire que Trident provisionne les volumes de sous-Tio. Si ce n'est pas le cas, les créations de volume **échoueront** pour les ESV de <600 Gio. Utiliser "ce formulaire" Pour obtenir l'accès aux volumes de sous-Tio.

Pilote CVS pour GCP	Snapshots	Clones	Multi-attacher	La QoS	Développement	La réplication
`gcp-cvs`	Oui.	Oui.	Oui.	Oui.	Oui.	Yes [1]

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

Le `gcp-cvs` le pilote utilise des pools de stockage virtuel. Avec les pools de stockage virtuel, Astra Trident peut extraire le système back-end et décider du placement des volumes. L'administrateur définit les pools de stockage virtuels dans le(s) fichier(s) backend(s).json. Les classes de stockage identifient les pools de stockage virtuels à l'aide d'étiquettes.

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.

Conception de la classe de stockage pour une utilisation 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 ensembles 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 tous les attributs spécifiés. Le `additionalStoragePools` Le paramètre est utilisé pour étendre l'ensemble de pools qu'Astra Trident utilisera pour le provisionnement ainsi que l'ensemble de 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` le paramètre est utilisé pour exclure spécifiquement l'ensemble de pools répertoriés qui correspondent aux attributs.

Conception de classe de stockage pour émuler les règles de QoS

Si vous souhaitez concevoir des classes de stockage pour émuler les règles de qualité de service, créez une classe de stockage avec le `media` attribut en tant que `hdd` ou `ssd`. Basé sur `media` Attribut mentionné dans la classe de stockage, Trident sélectionne le back-end approprié qui sert `hdd` ou `ssd` les agrégats correspondent à l'attribut du support, puis dirigent le provisionnement des volumes sur l'agrégat spécifique. Nous pouvons donc créer une PRIME de classe de stockage qui aurait été nécessaire `media` attribut défini comme `ssd` Qui peuvent être classées comme politique DE qualité de service 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.

La conception des classes de stockage permettant d'utiliser le 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.

Conception de la classe de stockage pour les pools de stockage virtuel

Tous les systèmes back-end Trident utilisent des pools de stockage virtuel. Vous pouvez définir des pools de stockage virtuel pour tout système back-end, à l'aide de tout pilote fourni par Astra Trident.

Les pools de stockage virtuel permettent à un administrateur de créer un niveau d'abstraction sur les systèmes back-end, que l'on peut référencer 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, plusieurs pools de stockage peuvent être créés sur le même back-end, mais avec des caractéristiques différentes. Lorsqu'une classe de stockage est configurée avec un sélecteur portant les étiquettes spécifiques, Astra Trident choisit un système back-end correspondant à toutes les étiquettes de sélection pour placer le volume. Si les étiquettes de sélection de classe de stockage correspondent à plusieurs pools de stockage, Astra Trident choisira l'un d'entre eux pour provisionner le volume.

Conception du pool de stockage 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 Virtual Storage pools, ce problème a été résolu. Les pools de stockage virtuel sont une abstraction de niveau introduit entre le back-end et la classe de stockage Kubernetes. L'administrateur peut ainsi définir des paramètres et des étiquettes qui peuvent être référencés par les classes de stockage Kubernetes comme sélecteur, de façon indépendante du back-end. Il est possible de définir des pools de stockage virtuel pour tous les systèmes back-end NetApp pris en charge avec Astra Trident. Il s'agit notamment des systèmes SolidFire/NetApp HCI, ONTAP, Cloud Volumes Service sur AWS, GCP et Azure NetApp Files.

Lors de la définition des pools de stockage virtuel, 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.

Concevoir des pools de stockage virtuel pour émuler différents niveaux de services/QoS

Il est possible de concevoir des pools de stockage virtuel pour émuler des classes de service. Grâce à l'implémentation des pools virtuels pour Cloud volumes Service pour AWS, examinons comment nous pouvons configurer différentes classes de service. Configurez le back-end AWS-CVS avec plusieurs étiquettes représentant différents niveaux de performance. Réglez `servicelevel` aspect au niveau de performance approprié et ajouter d'autres aspects requis sous chaque étiquette. Créez désormais différentes classes de stockage Kubernetes qui seraient mappées sur différents pools de stockage virtuels. À l'aide du `parameters.selector` Chaque classe de stockage indique quel(s) pool(s) virtuel(s) peut(s) être utilisé(s) pour héberger un volume.

Concevoir des pools virtuels pour l'attribution d'un ensemble spécifique d'aspects

Il est possible de concevoir plusieurs pools de stockage virtuel comprenant un ensemble spécifique d'aspects 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 désormais des classes de stockage Kubernetes différentes avec le `parameters.selector` Champ correspondant aux différents pools de stockage virtuel. Les volumes provisionnés sur le back-end possèdent les aspects définis dans le pool de stockage virtuel choisi.

Caractéristiques des PVC qui affectent le provisionnement du stockage

Certains paramètres au-delà de la classe de stockage demandée peuvent affecter le processus de décision d'approvisionnement d'Astra Trident lors de la création d'un volume persistant.

Mode d'accès

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

Astra Trident tentera de correspondre au protocole de stockage utilisé avec la méthode d'accès spécifiée dans la matrice suivante. Cette technologie est indépendante de la plateforme de stockage sous-jacente.

	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, cela n'empêche pas la modification de certains aspects du volume en dehors de Kubernetes. Vous pouvez ainsi personnaliser le volume pour des applications spécifiques, en veillant à ce que la capacité ne soit pas accidentellement consommée ou tout simplement pour déplacer le volume vers un autre contrôleur de stockage pour n'importe quelle raison.

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

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

Création de copies Snapshot de volume à la demande

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

Créer des volumes à partir de copies Snapshot

Astra Trident prend également en charge la création de volumes persistant à partir des snapshots de volume. Pour ce faire, il suffit de créer une demande de volume persistant et de mentionner le `datasource` l'instantané requis à partir duquel le volume doit être créé. Astra Trident va gérer ce volume de volume persistant en créant un volume dont les données sont présentes sur le snapshot. Grâce à cette fonctionnalité, il est possible de dupliquer des données entre régions, de créer des environnements de test, de remplacer un

volume de production endommagé ou corrompu dans son intégralité, ou de récupérer des fichiers et des répertoires spécifiques et de les transférer vers un autre volume attaché.

Déplacement des volumes dans le cluster

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

Néanmoins, Astra Trident ne prend pas automatiquement en charge le déplacement des volumes entre les systèmes back-end. Il s'agit notamment d'étendre les SVM au sein d'un même cluster, entre plusieurs clusters ou sur une autre plateforme de stockage (même si ce système est un SVM connecté à Astra Trident).

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

Développement des volumes

Astra Trident prend en charge le redimensionnement des volumes NFS et iSCSI PVS. Les utilisateurs peuvent ainsi redimensionner leurs volumes directement via la couche Kubernetes. L'extension de volume est possible pour toutes les principales plateformes de stockage NetApp, y compris ONTAP, SolidFire/NetApp HCI et les systèmes back-end Cloud Volumes Service. Pour permettre une extension possible ultérieurement, définissez `allowVolumeExpansion` à `true` Dans votre classe de stockage associée au volume. Lorsque le volume persistant doit être redimensionné, modifiez le `spec.resources.requests.storage` Annotation dans la demande de volume persistant vers 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. Cette opération est actuellement prise en charge par `ontap-nas`, `ontap-nas-flexgroup`, `solidfire-san`, `azure-netapp-files`, `aws-cvs`, et `gcp-cvs` pilotes. 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` pilotes, utilisez la commande `tridentctl import volume <backend-name> <volume-name> -f /path/pvc.yaml` Pour importer un volume existant dans Kubernetes et le gérer par Astra Trident. Le fichier PVC YAML ou JSON utilisé dans la commande de volume d'importation pointe vers une classe de stockage qui identifie Astra Trident comme provisionneur. Si vous utilisez un système back-end NetApp HCI/SolidFire, assurez-vous que les noms des volumes sont uniques. Si les noms des volumes sont dupliqués, cloner le volume en un nom unique afin que la fonctionnalité d'importation des volumes puisse les distinguer.

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

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

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

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

Le déploiement des services OpenShift

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

Service de registre

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

Service de journalisation

Comme les autres services OpenShift, le service de journalisation est déployé avec Ansible, avec les paramètres de configuration fournis par le fichier d'inventaire, également appelé hôtes, fournis avec le manuel de vente. 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 d'ONTAP ne présente pas ces problèmes et peut facilement être à nouveau déployé en environnements 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` à `true` pour éviter que le programme d'installation ne tombe en panne.

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.

La configuration des variables Ansible selon la méthode de déploiement est importante 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 car elles concernent le service de journalisation. Vous trouverez d'autres options dans "Documentation de journalisation Red Hat OpenShift" quels domaines doivent être examinés, configurés et utilisés 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`	Réglez 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. 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 `/openshift_logging`, vous utiliserez ce chemin pour cette variable.
`openshift_logging_storage_volume_name`	Le nom, par exemple `pv_ose_logs`, De la PV à créer.
`openshift_logging_storage_volume_size`	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`	Réglez sur `true` utilisation de 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 légèrement évoluer avec différentes versions d'OpenShift, c'est pourquoi nous vous invitons à le lire et à le suivre "Documentation Red Hat OpenShift Container Platform 3.11" pour 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 mise à l'échelle automatique des pods et de nombreuses entreprises utilisent les données du service de metrics pour leurs applications de refacturation et/ou de démonstration.

Comme pour le service de journalisation, OpenShift dans son ensemble, Ansible est utilisé pour déployer le service de metrics. De même, comme le service de journalisation, le service de metrics peut être déployé lors d'une configuration initiale du cluster ou après son fonctionnement à l'aide de la méthode d'installation du composant. 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`	Réglez 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. 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 `/openshift_metrics`, vous utiliserez ce chemin pour cette variable.
`openshift_metrics_storage_volume_name`	Le nom, par exemple `pv_ose_metrics`, De la PV à créer.
`openshift_metrics_storage_volume_size`	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.

Variable	Détails
`openshift_metrics_cassandra_pvc_size`	Taille des volumes à demander.
`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 l'utilisation des playbooks, après l'installation d'OpenShift, Ansible crée toutes les demandes de volume persistant nécessaires et, après que Astra 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. Vérifiez et suivez "Guide de déploiement OpenShift de Red Hat" pour votre version afin qu'elle soit configurée pour votre environnement.

Protection des données

Découvrez les options de protection des données et de restauration fournies par les plateformes de stockage NetApp. Astra Trident peut provisionner des volumes qui peuvent bénéficier de certaines de ces fonctionnalités. Vous devez disposer d'une stratégie de protection et de restauration des données pour chaque application ayant des exigences de persistance.

Sauvegardez le `etcd` données de cluster

Astra Trident stocke ses métadonnées dans le cluster Kubernetes `etcd` base de données. Sauvegarder régulièrement le `etcd` Les données en cluster sont importantes pour la restauration de clusters Kubernetes en cas d'incident.

Étapes

1. Le `etcdctl snapshot save` vous permet de créer un snapshot instantané de l' `etcd` cluster :

```
sudo docker run --rm -v /backup:/backup \
  --network host \
  -v /etc/kubernetes/pki/etcd:/etc/kubernetes/pki/etcd \
  --env ETCDCTL_API=3 \
  k8s.gcr.io/etcd-amd64:3.2.18 \
  etcdctl --endpoints=https://127.0.0.1:2379 \
  --cacert=/etc/kubernetes/pki/etcd/ca.crt \
  --cert=/etc/kubernetes/pki/etcd/healthcheck-client.crt \
  --key=/etc/kubernetes/pki/etcd/healthcheck-client.key \
  snapshot save /backup/etcd-snapshot.db
```

Cette commande crée un snapshot ETCD en faisant tourner un conteneur ETCD et le sauvegarde dans le `/backup` répertoire.

2. En cas d'incident, vous pouvez activer un cluster Kubernetes à l'aide des snapshots ETCD. Utilisez le `etcdctl snapshot restore` commande permettant de restaurer un snapshot spécifique pris sur le `/var/lib/etcd` dossier. Après la restauration, vérifiez si `/var/lib/etcd` le dossier a été rempli avec le `member` dossier. Voici un exemple de `etcdctl snapshot restore` commande :

```
# etcdctl snapshot restore '/backup/etcd-snapshot-latest.db' ; mv
/default.etcd/member/ /var/lib/etcd/
```

3. Avant d'initialiser le cluster Kubernetes, copiez tous les certificats nécessaires.
4. Créez le cluster avec le `--ignore-preflight-errors=DirAvailable—var-lib-etcd` drapeau.
5. Une fois le cluster lancé, assurez-vous que les modules du système kube ont démarré.
6. Utilisez le `kubectl get crd` Commande pour vérifier si les ressources personnalisées créées par Trident sont présentes et récupérer des objets Trident afin de s'assurer que toutes les données sont disponibles.

Récupérer les données à l'aide des snapshots ONTAP

Les snapshots jouent un rôle important en proposant des options de restauration ponctuelles pour les données d'application. Toutefois, les snapshots ne sont pas des sauvegardes en elles-mêmes, elles ne protègent pas contre les défaillances du système de stockage ou autres catastrophes. Cependant, ils constituent un moyen pratique, rapide et simple de restaurer des données dans la plupart des scénarios. Découvrez comment utiliser la technologie Snapshot de ONTAP pour sauvegarder les volumes et les restaurer.

- Si la politique de snapshot n'a pas été définie dans le backend, elle utilise par défaut le `none` politique. Résultat : ONTAP ne prend pas de snapshots automatiques. Toutefois, l'administrateur du stockage peut effectuer manuellement des snapshots ou modifier la règle Snapshot via l'interface de gestion ONTAP. Cela n'affecte pas le fonctionnement de Trident.
- Le répertoire de snapshot est masqué par défaut. Cela facilite une compatibilité maximale des volumes provisionnés à l'aide de `ontap-nas` et `ontap-nas-economy` pilotes. Activez le `.snapshot` répertoire lors de l'utilisation du `ontap-nas` et `ontap-nas-economy` pilotes permettant aux applications de récupérer directement les données à partir des snapshots.
- Restaurer un volume à un état enregistré dans un instantané précédent à l'aide du `volume snapshot restore` Commande CLI ONTAP. Lorsque vous restaurez une copie snapshot, l'opération de restauration écrase la configuration de volume existante. Toute modification apportée aux données du volume après la création de la copie Snapshot est perdue.

```
cluster1::*> volume snapshot restore -vserver vs0 -volume vol3 -snapshot
vol3_snap_archive
```

Réplication des données à l'aide de ONTAP

La réplication des données peut jouer un rôle important dans la protection contre les pertes de données dues à une défaillance de la baie de stockage.

Pour en savoir plus sur les technologies de réplication ONTAP, consultez "Documentation ONTAP".

Réplication des machines virtuelles de stockage (SVM) SnapMirror

Vous pouvez utiliser "SnapMirror" Pour répliquer un SVM complet, qui inclut ses paramètres de configuration et ses volumes. En cas d'incident, vous pouvez activer la SVM de destination SnapMirror pour démarrer le service des données. Vous pouvez revenir au primaire lorsque les systèmes sont restaurés.

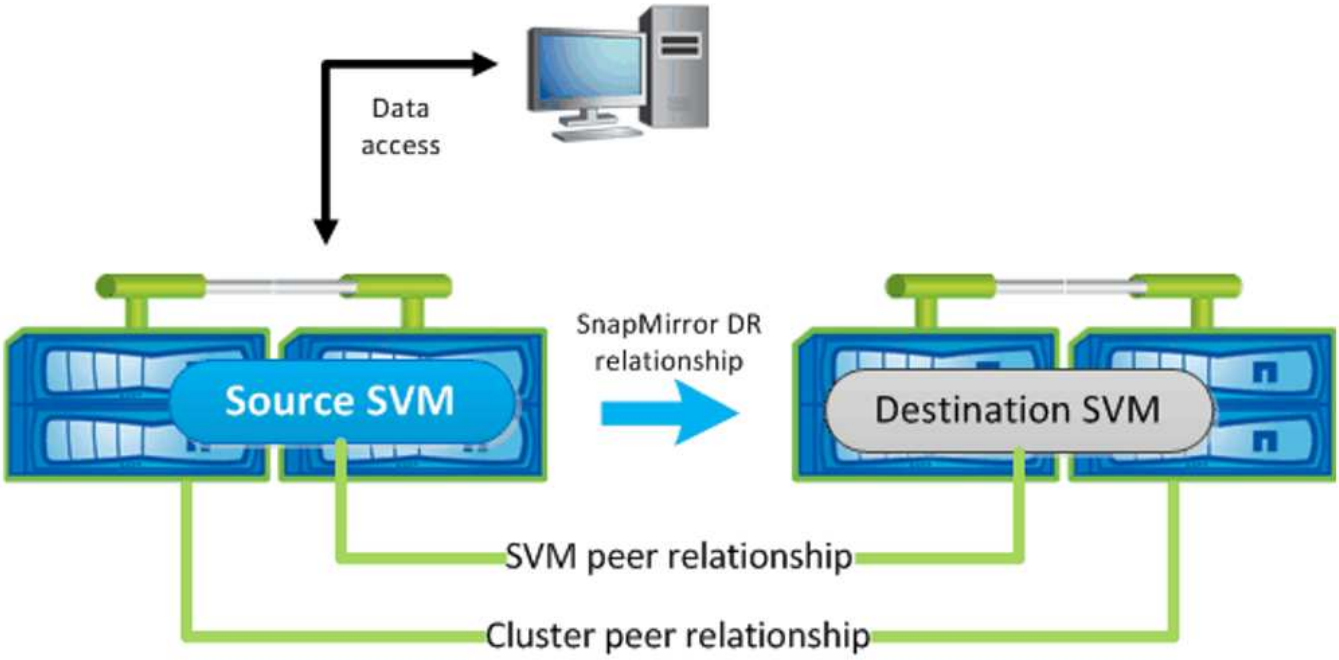
Astra Trident ne peut pas configurer lui-même les relations de réplication. L'administrateur du stockage peut donc utiliser la fonctionnalité de réplication du SVM SnapMirror d'ONTAP pour répliquer automatiquement les volumes vers une destination de reprise après incident.

Envisagez la commande suivante si vous prévoyez d'utiliser la fonctionnalité de réplication SVM SnapMirror ou si vous utilisez actuellement la fonctionnalité :

- Vous devez créer un système back-end distinct pour chaque SVM, sur lequel SVM-DR est activé.
- Vous devez configurer les classes de stockage de manière à ne pas sélectionner les systèmes back-end répliqués, sauf lorsque cela est nécessaire. Cela est important pour éviter la mise en service des volumes qui ne nécessitent pas de protection de la relation de réplication sur les back-end compatibles avec SVM-DR.
- Les administrateurs d'applications doivent comprendre les coûts et la complexité supplémentaires liés à la réplication des données, et un plan de restauration doit être déterminé avant d'exploiter la réplication des données.
- Avant d'activer la SVM de destination SnapMirror, arrêter tous les transferts SnapMirror planifiés, abandonner tous les transferts SnapMirror en cours, interrompre la relation de réplication, arrêter la SVM source puis démarrer la SVM de destination SnapMirror.
- Astra Trident ne détecte pas automatiquement les défaillances du SVM. Par conséquent, en cas d'échec, l'administrateur doit exécuter le `tridentctl backend update` Commande permettant de déclencher le basculement de Trident vers le nouveau back-end.

Voici une présentation des étapes de configuration des SVM :

- Configurer le peering entre le cluster source et destination et SVM
- Créer le SVM de destination à l'aide de l' `-subtype dp-destination` option.
- Créez une planification de tâches de réplication afin de vous assurer que la réplication se déroule aux intervalles requis.
- Créer une réplication SnapMirror depuis le SVM de destination vers le SVM source à l'aide de `-identity -preserve true` Option pour s'assurer que les configurations du SVM source et les interfaces du SVM source sont copiées vers la destination. Depuis le SVM de destination, initialiser la relation de réplication SVM SnapMirror



Workflow de reprise d'activité pour Trident

Astra Trident 19.07 et les versions ultérieures utilisent des CRD Kubernetes pour stocker et gérer son propre état. Elle utilise celle du cluster Kubernetes `etcd` pour stocker ses métadonnées. On suppose ici que Kubernetes `etcd` Les fichiers de données et les certificats sont stockés sur NetApp FlexVolume. Ce FlexVolume réside dans un SVM, qui dispose d'une relation SVM-DR SnapMirror avec un SVM de destination sur le site secondaire.

La procédure suivante décrit comment restaurer un cluster Kubernetes maître avec Astra Trident en cas d'incident :

1. En cas de défaillance du SVM source, activer le SVM de destination SnapMirror Pour cela, il faut arrêter des transferts SnapMirror planifiés, abandonner les transferts SnapMirror en cours, interrompre la relation de réplication, arrêter la SVM source et démarrer la SVM de destination.
2. Depuis le SVM de destination, montez le volume qui contient l'environnement Kubernetes `etcd` fichiers de données et certificats sur l'hôte qui seront configurés en tant que nœud maître.
3. Copiez tous les certificats requis se rapportant au cluster Kubernetes sous `/etc/kubernetes/pki` et le etcd `member` fichiers sous `/var/lib/etcd`.
4. Créez un cluster Kubernetes en utilisant le `kubeadm init` commande avec `--ignore-preflight -errors=DirAvailable—var-lib-etcd` drapeau. Les noms d'hôte utilisés pour les nœuds Kubernetes doivent être identiques au cluster Kubernetes source.
5. Exécutez le `kubectl get crd` Commande pour vérifier si toutes les ressources personnalisées Trident ont été extraites et récupérer les objets Trident pour vérifier que toutes les données sont disponibles.
6. Mise à jour de tous les systèmes back-end requis pour refléter le nouveau nom de SVM de destination en exécutant la `./tridentctl update backend <backend-name> -f <backend-json-file> -n <namespace>` commande.

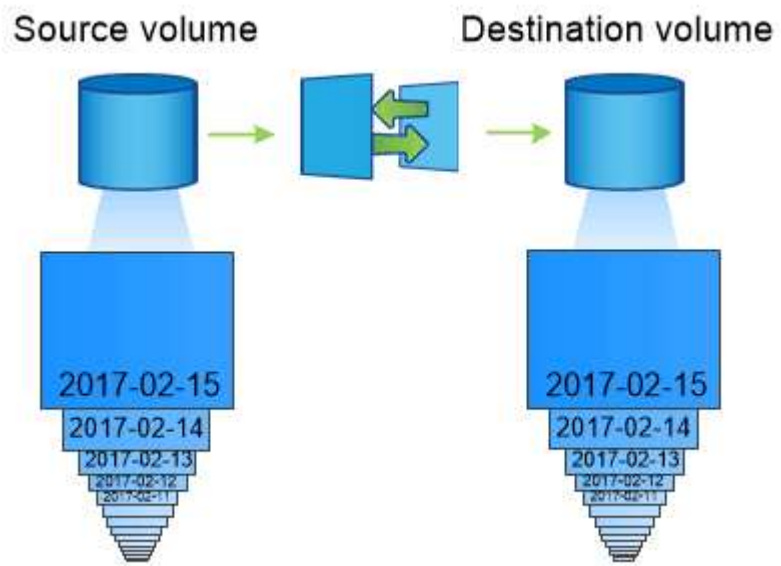
Lorsque le SVM de destination est activé pour les volumes persistants des applications, tous les volumes provisionnés par Trident commencent à transmettre les données. Une fois le cluster Kubernetes configuré sur le système de destination conformément aux étapes décrites ci-dessus, tous les déploiements et les pods sont démarrés et les applications conteneurisées doivent s'exécuter sans aucun problème.

Réplication de volume SnapMirror

La réplication de volume ONTAP SnapMirror est une fonctionnalité de reprise d'activité qui permet le basculement vers le stockage de destination à partir d'un stockage primaire au niveau des volumes. SnapMirror crée une réplique de volume ou un miroir du stockage primaire sur le stockage secondaire en synchronisant les snapshots.

Voici une synthèse des étapes de configuration de la réplication de volume ONTAP SnapMirror :

- Configurez le peering entre les clusters dans lesquels les volumes résident et les SVM qui fournissent les données des volumes.
- Créer une règle SnapMirror, qui contrôle le comportement de la relation et spécifie les attributs de configuration pour cette relation.
- Créer une relation SnapMirror entre le volume de destination et le volume source à l'aide de la[`snapmirror create` Commande^] et affecter la règle SnapMirror appropriée.
- Une fois la relation SnapMirror créée, initialisez la relation pour qu'un transfert de base du volume source vers le volume de destination soit terminé.



Workflow de reprise d'activité de volumes SnapMirror pour Trident

La procédure suivante décrit comment restaurer un cluster Kubernetes maître avec Astra Trident.

1. En cas d'incident, arrêter tous les transferts SnapMirror programmés et abandonner tous les transferts SnapMirror en cours. Rompez la relation de réplication entre les volumes de destination et source de sorte que le volume de destination soit lu/écrit.
2. Depuis le SVM de destination, montez le volume qui contient l'environnement Kubernetes `etcd` fichiers de données et certificats sur l'hôte, qui sera configuré en tant que nœud maître.

3. Copiez tous les certificats requis se rapportant au cluster Kubernetes sous `/etc/kubernetes/pki` et le etcd `member` fichiers sous `/var/lib/etcd`.
4. Créez un cluster Kubernetes en exécutant le `kubeadm init` commande avec `--ignore-preflight -errors=DirAvailable—var-lib-etcd` drapeau. Les noms d'hôte doivent être identiques au cluster Kubernetes source.
5. Exécutez le `kubectl get crd` Commande pour vérifier si toutes les ressources personnalisées Trident ont été extraites et récupérer des objets Trident pour s'assurer que toutes les données sont disponibles.
6. Nettoyez les systèmes back-end précédents et créez de nouveaux systèmes back-end sur Trident. Préciser la nouvelle LIF de gestion et de données, le nouveau nom du SVM et le mot de passe du SVM de destination.

Workflow de reprise d'activité pour les volumes persistants des applications

Les étapes suivantes décrivent comment mettre à disposition les volumes de destination SnapMirror pour les workloads conteneurisés en cas d'incident :

1. Arrêt de tous les transferts SnapMirror programmés et abandon de tous les transferts SnapMirror en cours. Rompez la relation de réplication entre le volume de destination et le volume source pour que le volume de destination devienne read/write. Nettoyer les déploiements qui consomtaient du volume persistant lié aux volumes sur la SVM source.
2. Une fois le cluster Kubernetes configuré sur le côté destination, suivez les étapes décrites ci-dessus pour nettoyer les déploiements, les demandes de volume persistant et le volume persistant à partir du cluster Kubernetes.
3. Créer de nouveaux systèmes back-end sur Trident en spécifiant la nouvelle LIF de gestion et de données, un nouveau nom de SVM et un nouveau mot de passe du SVM de destination.
4. Importez les volumes requis en tant que volume persistant lié à une nouvelle demande de volume persistant à l'aide de la fonctionnalité d'importation Trident.
5. Redéployez les déploiements d'applications avec les demandes de volume nouvellement créées.

Restaurez les données à l'aide des snapshots Element

Sauvegardez les données sur un volume Element en définissant une planification Snapshot pour le volume. Vous pouvez ainsi vérifier que les snapshots sont effectués à intervalles réguliers. Vous devez définir la planification des snapshots à l'aide de l'interface utilisateur ou des API d'Element. Actuellement, il n'est pas possible de définir un planning de snapshots sur un volume via la `solidfire-san` conducteur.

En cas de corruption des données, vous pouvez choisir un snapshot en particulier et restaurer manuellement le volume vers le Snapshot à l'aide de l'interface utilisateur ou des API Element. Cette opération rétablit les modifications apportées au volume depuis la création du snapshot.

Sécurité

Suivez les recommandations indiquées ici pour vous assurer que votre installation d'Astra Trident est sécurisée.

Exécutez Astra Trident dans son propre espace de noms

Il est important d'empêcher les applications, les administrateurs d'applications, les utilisateurs et les applications de gestion d'accéder aux définitions d'objets Astra Trident ou aux pods pour assurer un stockage fiable et bloquer tout risque d'activité malveillante.

Pour séparer les autres applications et utilisateurs d'Astra Trident, installez toujours Astra Trident dans son propre espace de noms Kubernetes (`trident`). L'utilisation d'Astra Trident dans son propre espace de noms garantit que seul le personnel d'administration Kubernetes a accès au pod Trident Astra et aux artéfacts (tels que les secrets d'arrière-plan et CHAP le cas échéant) stockés dans les objets CRD devant être namestes. Vous devez vous assurer que seuls les administrateurs ont accès à l'espace de noms Astra Trident et y ont donc accès `tridentctl` client supplémentaire.

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

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

Pour les systèmes ONTAP back-end qui utilisent les pilotes de stockage SAN, Astra Trident peut configurer le protocole CHAP bidirectionnel et gérer les noms d'utilisateur et les secrets CHAP via `tridentctl`. Voir "ici" Pour comprendre comment Astra Trident configure le protocole CHAP sur les systèmes back-end ONTAP.

> La prise en charge CHAP pour les systèmes back-end ONTAP est disponible avec Trident 20.04 et versions ultérieures.

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

NetApp recommande de déployer le protocole CHAP bidirectionnel pour garantir l'authentification entre l'hôte et les systèmes back-end NetApp HCI et SolidFire. Astra Trident utilise un objet secret qui inclut deux mots de passe CHAP par locataire. Lorsque Trident est installé en tant que fournisseur CSI, il gère les secrets CHAP et les stocke dans un `tridentvolume` Objet CR pour la PV correspondante. Lorsque vous créez un volume persistant, CSI 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 CSI Trident ne sont associés à aucun groupe d'accès de volume.

Sur le système front-end non CSI, la connexion de volumes en tant que périphériques sur les nœuds workers est gérée par Kubernetes. Après la création de volumes, Astra Trident effectue un appel d'API vers le système NetApp HCI/SolidFire pour récupérer les secrets de ce locataire n'existe pas encore. Astra Trident transmet ensuite les secrets de Kubernetes. Le kubelet situé sur chaque nœud accède aux secrets de l'API Kubernetes et les utilise pour exécuter/activer CHAP entre chaque nœud accédant au volume et le système NetApp HCI/SolidFire où se trouvent les volumes.

Informations sur le copyright

Informations sur les marques commerciales