Protégez vos applications avec Trident Protect

Trident

NetApp
January 15, 2026

Sommaire

Protégez vos applications avec Trident Protect

Découvrez Trident Protect

NetApp Trident Protect offre des fonctionnalités avancées de gestion des données d'application qui améliorent la fonctionnalité et la disponibilité des applications Kubernetes avec état, prises en charge par les systèmes de stockage NetApp ONTAP et le provisionneur de stockage NetApp Trident CSI. Trident Protect simplifie la gestion, la protection et le déplacement des charges de travail conteneurisées entre les clouds publics et les environnements sur site. Il offre également des capacités d'automatisation via son API et sa CLI.

Vous pouvez protéger les applications avec Trident Protect en créant des ressources personnalisées (CR) ou en utilisant l'interface de ligne de commande (CLI) de Trident Protect.

Quelle est la prochaine étape ?

Vous pouvez vous renseigner sur les exigences de Trident Protect avant de l'installer :

- "Exigences de Trident Protect"

Installer Trident Protect

Exigences de Trident Protect

Commencez par vérifier l'état de préparation de votre environnement opérationnel, de vos clusters d'applications, de vos applications et de vos licences. Assurez-vous que votre environnement répond à ces exigences pour déployer et utiliser Trident Protect.

Compatibilité avec les clusters Kubernetes de Trident Protect

Trident Protect est compatible avec une large gamme d'offres Kubernetes entièrement gérées et autogérées, notamment :

- Amazon Elastic Kubernetes Service (EKS)
- Moteur Google Kubernetes (GKE)
- Service Kubernetes Microsoft Azure (AKS)
- Red Hat OpenShift
- SUSE Rancher
- Portefeuille VMware Tanzu
- Kubernetes en amont

- Les sauvegardes Trident Protect sont prises en charge uniquement sur les nœuds de calcul Linux. Les nœuds de calcul Windows ne sont pas pris en charge pour les opérations de sauvegarde.
- Assurez-vous que le cluster sur lequel vous installez Trident Protect est configuré avec un contrôleur de snapshots en cours d'exécution et les CRD associés. Pour installer un contrôleur de snapshots, reportez-vous à la documentation. "ces instructions" .

Compatibilité du système de stockage Trident Protect

Trident Protect prend en charge les systèmes de stockage suivants :

- Amazon FSx for NetApp ONTAP
- Cloud Volumes ONTAP
- baies de stockage ONTAP
- Google Cloud NetApp Volumes
- Azure NetApp Files

Assurez-vous que votre système de stockage réponde aux exigences suivantes :

- Assurez-vous que le stockage NetApp connecté au cluster utilise Trident 24.02 ou une version plus récente (Trident 24.10 est recommandé).
- Assurez-vous de disposer d'un système de stockage NetApp ONTAP .
- Assurez-vous d'avoir configuré un compartiment de stockage d'objets pour stocker les sauvegardes.
- Créez les espaces de noms d'application que vous prévoyez d'utiliser pour les applications ou les opérations de gestion des données d'application. Trident Protect ne crée pas ces espaces de noms pour vous ; si vous spécifiez un espace de noms inexistant dans une ressource personnalisée, l'opération échouera.

Exigences pour les volumes de l'économie NAS

Trident Protect prend en charge les opérations de sauvegarde et de restauration sur les volumes NAS économiques. Les snapshots, les clones et la réplication SnapMirror vers des volumes nas-economy ne sont actuellement pas pris en charge. Vous devez activer un répertoire de snapshots pour chaque volume nas-economy que vous prévoyez d'utiliser avec Trident Protect.

Certaines applications ne sont pas compatibles avec les volumes qui utilisent un répertoire de snapshots. Pour ces applications, vous devez masquer le répertoire des instantanés en exécutant la commande suivante sur le système de stockage ONTAP :

```
nfs modify -vserver <svm> -v3-hide-snapshot enabled
```

Vous pouvez activer le répertoire de snapshots en exécutant la commande suivante pour chaque volume nas-economy, en remplaçant `<volume-UUID>` avec l'UUID du volume que vous souhaitez modifier :

```
tridentctl update volume <volume-UUID> --snapshot-dir=true --pool-level
=true -n trident
```

Vous pouvez activer par défaut les répertoires de snapshots pour les nouveaux volumes en configurant l'option de configuration du backend Trident . `snapshotDir` à `true` . Les volumes existants ne sont pas affectés.

Protection des données avec les machines virtuelles KubeVirt

Trident Protect 24.10 et 24.10.1 et versions ultérieures ont un comportement différent lorsque vous protégez des applications exécutées sur des machines virtuelles KubeVirt. Pour les deux versions, vous pouvez activer ou désactiver le gel et le dégel du système de fichiers pendant les opérations de protection des données.

Lors des opérations de restauration, tout `VirtualMachineSnapshots` Les éléments créés pour une machine virtuelle (VM) ne sont pas restaurés.

Trident Protect 24.10

Trident Protect 24.10 ne garantit pas automatiquement un état cohérent pour les systèmes de fichiers de machines virtuelles KubeVirt lors des opérations de protection des données. Si vous souhaitez protéger les données de votre machine virtuelle KubeVirt à l'aide de Trident Protect 24.10, vous devez activer manuellement la fonctionnalité de gel/dégel des systèmes de fichiers avant l'opération de protection des données. Cela garantit que les systèmes de fichiers sont dans un état cohérent.

Vous pouvez configurer Trident Protect 24.10 pour gérer le gel et le dégel du système de fichiers de la machine virtuelle lors des opérations de protection des données."configuration de la virtualisation" puis en utilisant la commande suivante :

```
kubectl set env deployment/trident-protect-controller-manager
NEPTUNE_VM_FREEZE=true -n trident-protect
```

Trident Protect 24.10.1 et versions ultérieures

À partir de Trident Protect 24.10.1, Trident Protect gèle et débloque automatiquement les systèmes de fichiers KubeVirt lors des opérations de protection des données. Vous pouvez désactiver ce comportement automatique à l'aide de la commande suivante :

```
kubectl set env deployment/trident-protect-controller-manager
NEPTUNE_VM_FREEZE=false -n trident-protect
```

Exigences pour la réplication SnapMirror

La réplication NetApp SnapMirror est disponible pour une utilisation avec Trident Protect pour les solutions ONTAP suivantes :

- Clusters NetApp FAS, AFF et ASA sur site
- ONTAP Select NetApp ONTAP
- NetApp Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP

Configuration requise pour la réplication SnapMirror dans un cluster ONTAP

Assurez-vous que votre cluster ONTAP répond aux exigences suivantes si vous prévoyez d'utiliser la réplication SnapMirror :

- * NetApp Trident* : NetApp Trident doit exister à la fois sur les clusters Kubernetes source et de destination qui utilisent ONTAP comme backend. Trident Protect prend en charge la réplication avec la technologie NetApp SnapMirror utilisant des classes de stockage reposant sur les pilotes suivants :
  - `ontap-nas`: NFS
  - `ontap-san`: iSCSI
  - `ontap-san`: FC
  - `ontap-san`: NVMe/TCP (nécessite au minimum la version ONTAP 9.15.1)
- **Licences** : Les licences asynchrones ONTAP SnapMirror utilisant le module de protection des données doivent être activées sur les clusters ONTAP source et de destination. Se référer à "Présentation des licences SnapMirror dans ONTAP" pour plus d'informations.

  À partir d' ONTAP 9.10.1, toutes les licences sont fournies sous forme de fichier de licence NetApp (NLF), qui est un fichier unique permettant d'activer plusieurs fonctionnalités. Se référer à"Licences incluses avec ONTAP One" pour plus d'informations.

  > Seule la protection asynchrone SnapMirror est prise en charge.

Considérations relatives au peering pour la réplication SnapMirror

Si vous prévoyez d'utiliser le peering de stockage backend, assurez-vous que votre environnement réponde aux exigences suivantes :

- **Cluster et SVM** : Les backends de stockage ONTAP doivent être appariés. Se référer à "Aperçu du peering de clusters et de SVM" pour plus d'informations.

  > Assurez-vous que les noms SVM utilisés dans la relation de réplication entre deux clusters ONTAP sont uniques.

- * NetApp Trident et SVM * : Les SVM distants appariés doivent être disponibles pour NetApp Trident sur le cluster de destination.
- **Systèmes de stockage backend gérés** : Vous devez ajouter et gérer des systèmes de stockage backend ONTAP dans Trident Protect pour créer une relation de réplication.

Configuration Trident / ONTAP pour la réplication SnapMirror

Trident Protect exige que vous configuriez au moins un système de stockage dorsal prenant en charge la réplication pour les clusters source et de destination. Si les clusters source et de destination sont identiques, l'application de destination doit utiliser un système de stockage différent de celui de l'application source pour une résilience optimale.

Configuration requise pour la réplication SnapMirror dans un cluster Kubernetes

Assurez-vous que vos clusters Kubernetes répondent aux exigences suivantes :

- **Accessibilité à AppVault** : Les clusters source et de destination doivent avoir un accès réseau pour lire et

écrire dans AppVault pour la réplication des objets d'application.

- **Connectivité réseau** : Configurez les règles de pare-feu, les autorisations de compartiment et les listes d'adresses IP autorisées pour permettre la communication entre les deux clusters et AppVault via les réseaux WAN.

> De nombreux environnements d'entreprise mettent en œuvre des politiques de pare-feu strictes sur les connexions WAN. Vérifiez ces exigences réseau auprès de votre équipe d'infrastructure avant de configurer la réplication.

Installez et configurez Trident Protect.

Si votre environnement répond aux exigences de Trident Protect, vous pouvez suivre ces étapes pour installer Trident Protect sur votre cluster. Vous pouvez obtenir Trident Protect auprès de NetApp ou l'installer à partir de votre propre registre privé. L'installation à partir d'un registre privé est utile si votre cluster ne peut pas accéder à Internet.

Installer Trident Protect

Installez Trident Protect de NetApp

Étapes

1. Ajouter le dépôt Trident Helm :

```
helm repo add netapp-trident-protect
https://netapp.github.io/trident-protect-helm-chart
```

2. Utilisez Helm pour installer Trident Protect. Remplacer `<name-of-cluster>` avec un nom de cluster, qui sera attribué au cluster et utilisé pour identifier les sauvegardes et les instantanés du cluster :

```
helm install trident-protect netapp-trident-protect/trident-protect
--set clusterName=<name-of-cluster> --version 100.2506.0 --create
-namespace --namespace trident-protect
```

Installez Trident Protect à partir d'un registre privé

Vous pouvez installer Trident Protect à partir d'un registre d'images privé si votre cluster Kubernetes ne peut pas accéder à Internet. Dans ces exemples, remplacez les valeurs entre crochets par les informations provenant de votre environnement :

Étapes

1. Téléchargez les images suivantes sur votre machine locale, mettez à jour les étiquettes, puis envoyez-les vers votre registre privé :

```
netapp/controller:25.06.0
netapp/restic:25.06.0
netapp/kopia:25.06.0
netapp/trident-autosupport:25.06.0
netapp/exechook:25.06.0
netapp/resourcebackup:25.06.0
netapp/resourcerestore:25.06.0
netapp/resourcedelete:25.06.0
bitnami/kubectl:1.30.2
kubebuilder/kube-rbac-proxy:v0.16.0
```

Par exemple:

```
docker pull netapp/controller:25.06.0
```

```
docker tag netapp/controller:25.06.0 <private-registry-
url>/controller:25.06.0
```

```
docker push <private-registry-url>/controller:25.06.0
```

2. Créez l'espace de noms système Trident Protect :

```
kubectl create ns trident-protect
```

3. Connectez-vous au registre :

```
helm registry login <private-registry-url> -u <account-id> -p <api-token>
```

4. Créez un secret d'extraction à utiliser pour l'authentification du registre privé :

```
kubectl create secret docker-registry regcred --docker-username=<registry-username> --docker-password=<api-token> -n trident-protect --docker-server=<private-registry-url>
```

5. Ajouter le dépôt Trident Helm :

```
helm repo add netapp-trident-protect https://netapp.github.io/trident-protect-helm-chart
```

6. Créez un fichier nommé `protectValues.yaml` . Assurez-vous qu'il contienne les paramètres Trident Protect suivants :

```
---
image:
  registry: <private-registry-url>
imagePullSecrets:
  - name: regcred
controller:
  image:
    registry: <private-registry-url>
rbacProxy:
  image:
    registry: <private-registry-url>
crCleanup:
  imagePullSecrets:
    - name: regcred
webhooksCleanup:
  imagePullSecrets:
    - name: regcred
```

7. Utilisez Helm pour installer Trident Protect. Remplacer `<name_of_cluster>` avec un nom de cluster, qui sera attribué au cluster et utilisé pour identifier les sauvegardes et les instantanés du cluster :

```
helm install trident-protect netapp-trident-protect/trident-protect
--set clusterName=<name_of_cluster> --version 100.2506.0 --create
-namespace --namespace trident-protect -f protectValues.yaml
```

Installez le plugin CLI Trident Protect

Vous pouvez utiliser le plugin en ligne de commande Trident Protect, qui est une extension de Trident. `tridentctl` utilitaire, pour créer et interagir avec les ressources personnalisées (CR) de Trident Protect.

Installez le plugin CLI Trident Protect

Avant d'utiliser l'utilitaire en ligne de commande, vous devez l'installer sur la machine que vous utilisez pour accéder à votre cluster. Suivez ces étapes, selon que votre machine utilise un processeur x64 ou ARM .

Télécharger le plugin pour les processeurs Linux AMD64

Étapes

1. Téléchargez le plugin CLI Trident Protect :

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.06.0/tridentctl-protect-linux-amd64
```

Télécharger le plugin pour les processeurs Linux ARM64

Étapes

1. Téléchargez le plugin CLI Trident Protect :

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.06.0/tridentctl-protect-linux-arm64
```

Télécharger le plugin pour les processeurs Mac AMD64

Étapes

1. Téléchargez le plugin CLI Trident Protect :

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.06.0/tridentctl-protect-macos-amd64
```

Télécharger le plugin pour les processeurs Mac ARM64

Étapes

1. Téléchargez le plugin CLI Trident Protect :

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.06.0/tridentctl-protect-macos-arm64
```

1. Activer les permissions d'exécution pour le fichier binaire du plugin :

```
chmod +x tridentctl-protect
```

2. Copiez le fichier binaire du plugin à un emplacement défini dans votre variable PATH. Par exemple, `/usr/bin` ou `/usr/local/bin` (Vous pourriez avoir besoin de privilèges élevés) :

```
cp ./tridentctl-protect /usr/local/bin/
```

3. Vous pouvez également copier le fichier binaire du plugin dans un emplacement de votre répertoire personnel. Dans ce cas, il est recommandé de s'assurer que l'emplacement fait partie de votre variable PATH :

```
cp ./tridentctl-protect ~/bin/
```

Copier le plugin dans un emplacement figurant dans votre variable PATH vous permet de l'utiliser en tapant : `tridentctl-protect` ou `tridentctl protect` de n'importe quel endroit.

Consultez l'aide du plugin Trident CLI

Vous pouvez utiliser les fonctionnalités d'aide intégrées au plugin pour obtenir une aide détaillée sur ses capacités :

Étapes

1. Utilisez la fonction d'aide pour consulter les instructions d'utilisation :

```
tridentctl-protect help
```

Activer la saisie semi-automatique des commandes

Une fois le plugin CLI Trident Protect installé, vous pouvez activer la saisie semi-automatique pour certaines commandes.

Activer la saisie semi-automatique pour le shell Bash

Étapes

1. Télécharger le script de complétion :

```
curl -L -O https://github.com/NetApp/tridentctl-
protect/releases/download/25.06.0/tridentctl-completion.bash
```

2. Créez un nouveau répertoire dans votre répertoire personnel pour y placer le script :

```
mkdir -p ~/.bash/completions
```

3. Déplacez le script téléchargé vers le `~/.bash/completions` annuaire:

```
mv tridentctl-completion.bash ~/.bash/completions/
```

4. Ajoutez la ligne suivante à la `~/.bashrc` fichier dans votre répertoire personnel :

```
source ~/.bash/completions/tridentctl-completion.bash
```

Activer la saisie semi-automatique pour le shell Z

Étapes

1. Télécharger le script de complétion :

```
curl -L -O https://github.com/NetApp/tridentctl-
protect/releases/download/25.06.0/tridentctl-completion.zsh
```

2. Créez un nouveau répertoire dans votre répertoire personnel pour y placer le script :

```
mkdir -p ~/.zsh/completions
```

3. Déplacez le script téléchargé vers le `~/.zsh/completions` annuaire:

```
mv tridentctl-completion.zsh ~/.zsh/completions/
```

4. Ajoutez la ligne suivante à la `~/.zprofile` fichier dans votre répertoire personnel :

```
source ~/.zsh/completions/tridentctl-completion.zsh
```

Résultat

Lors de votre prochaine connexion à l'interpréteur de commandes, vous pourrez utiliser la saisie semi-automatique des commandes grâce au plugin tridentctl-protect.

Personnaliser l'installation de Trident Protect

Vous pouvez personnaliser la configuration par défaut de Trident Protect pour répondre aux exigences spécifiques de votre environnement.

Spécifiez les limites de ressources du conteneur Trident Protect

Vous pouvez utiliser un fichier de configuration pour spécifier les limites de ressources des conteneurs Trident Protect après l'installation de Trident Protect. La définition de limites de ressources vous permet de contrôler la quantité de ressources du cluster consommées par les opérations de Trident Protect.

Étapes

1. Créez un fichier nommé `resourceLimits.yaml` .
2. Renseignez le fichier avec les options de limite de ressources pour les conteneurs Trident Protect en fonction des besoins de votre environnement.

   Le fichier de configuration d'exemple suivant présente les paramètres disponibles et contient les valeurs par défaut pour chaque limite de ressources :

```
---
jobResources:
  defaults:
    limits:
      cpu: 8000m
      memory: 10000Mi
      ephemeralStorage: ""
    requests:
      cpu: 100m
      memory: 100Mi
      ephemeralStorage: ""
  resticVolumeBackup:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
  resticVolumeRestore:
    limits:
      cpu: ""
      memory: ""
```

```
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
  kopiaVolumeBackup:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
  kopiaVolumeRestore:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
```

3. Appliquez les valeurs de `resourceLimits.yaml` déposer:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect -f resourceLimits.yaml --reuse-values
```

Personnaliser les contraintes de contexte de sécurité

Vous pouvez utiliser un fichier de configuration pour modifier les contraintes de contexte de sécurité OpenShift (SCC) pour les conteneurs Trident Protect après avoir installé Trident Protect. Ces contraintes définissent les restrictions de sécurité des pods dans un cluster Red Hat OpenShift.

Étapes

1. Créez un fichier nommé `sccconfig.yaml` .
2. Ajoutez l'option SCC au fichier et modifiez les paramètres en fonction des besoins de votre environnement.

   L'exemple suivant illustre les valeurs par défaut des paramètres de l'option SCC :

```
scc:
  create: true
  name: trident-protect-job
  priority: 1
```

Ce tableau décrit les paramètres de l'option SCC :

Paramètre	Description	Défaut
créer	Détermine si une ressource SCC peut être créée. Une ressource SCC ne sera créée que si `scc.create` est réglé sur `true` et le processus d'installation de Helm identifie un environnement OpenShift. Si vous n'utilisez pas OpenShift, ou si `scc.create` est réglé sur `false` Aucune ressource SCC ne sera créée.	true
nom	Spécifie le nom du SCC.	trident-protect-emploi
priorité	Définit la priorité du SCC. Les SCC ayant des valeurs de priorité plus élevées sont évaluées avant celles ayant des valeurs plus faibles.	1

3. Appliquez les valeurs de `sccconfig.yaml` déposer:

```
helm upgrade trident-protect netapp-trident-protect/trident-protect -f
sccconfig.yaml --reuse-values
```

Cela remplacera les valeurs par défaut par celles spécifiées dans le `sccconfig.yaml` déposer.

Configurer les paramètres supplémentaires du graphique de barre de Trident Protect

Vous pouvez personnaliser les paramètres AutoSupport et le filtrage des espaces de noms pour répondre à vos besoins spécifiques. Le tableau suivant décrit les paramètres de configuration disponibles :

Paramètre	Type	Description
autoSupport.proxy	chaîne	Configure une URL proxy pour les connexions NetApp AutoSupport . Utilisez ceci pour acheminer les téléchargements de bundles de support via un serveur proxy. Exemple: `http://my.proxy.url` .

Paramètre	Type	Description
autoSupport.insecure	booléen	Ignore la vérification TLS pour les connexions proxy AutoSupport lorsque cette option est activée. `true` . À utiliser uniquement pour les connexions proxy non sécurisées. (défaut: `false`)
autoSupport.activé	booléen	Active ou désactive les téléchargements quotidiens des modules Trident Protect AutoSupport . Lorsqu'il est réglé sur `false` Les téléchargements quotidiens programmés sont désactivés, mais vous pouvez toujours générer manuellement des ensembles de support. (défaut: `true`)
restaurerSkipNamespaceAnnotations	chaîne	Liste séparée par des virgules d'annotations d'espace de noms à exclure des opérations de sauvegarde et de restauration. Vous permet de filtrer les espaces de noms en fonction des annotations.
restaurerSkipNamespaceLabels	chaîne	Liste séparée par des virgules d'étiquettes d'espace de noms à exclure des opérations de sauvegarde et de restauration. Vous permet de filtrer les espaces de noms en fonction des étiquettes.

Vous pouvez configurer ces options à l'aide d'un fichier de configuration YAML ou d'indicateurs de ligne de commande :

Utiliser le fichier YAML

Étapes

1. Créez un fichier de configuration et nommez-le `values.yaml` .
2. Dans le fichier que vous avez créé, ajoutez les options de configuration que vous souhaitez personnaliser.

```
autoSupport:
  enabled: false
  proxy: http://my.proxy.url
  insecure: true
restoreSkipNamespaceAnnotations: "annotation1,annotation2"
restoreSkipNamespaceLabels: "label1,label2"
```

3. Après avoir rempli le `values.yaml` Fichier contenant les valeurs correctes, appliquez le fichier de configuration :

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect -f values.yaml --reuse-values
```

Utiliser l'indicateur CLI

Étapes

1. Utilisez la commande suivante avec le `--set` indicateur permettant de spécifier des paramètres individuels :

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set autoSupport.enabled=false \
  --set autoSupport.proxy=http://my.proxy.url \
  --set restoreSkipNamespaceAnnotations="annotation1,annotation2" \
  --set restoreSkipNamespaceLabels="label1,label2" \
  --reuse-values
```

Limiter les pods Trident Protect à des nœuds spécifiques

Vous pouvez utiliser la contrainte de sélection de nœuds nodeSelector de Kubernetes pour contrôler quels nœuds sont éligibles pour exécuter des pods Trident Protect, en fonction des étiquettes de nœud. Par défaut, Trident Protect est limité aux nœuds exécutant Linux. Vous pouvez personnaliser davantage ces contraintes en fonction de vos besoins.

Étapes

1. Créez un fichier nommé `nodeSelectorConfig.yaml` .

2. Ajoutez l'option nodeSelector au fichier et modifiez ce dernier pour ajouter ou modifier les étiquettes des nœuds afin de les adapter aux besoins de votre environnement. Par exemple, le fichier suivant contient la restriction par défaut du système d'exploitation, mais cible également une région et un nom d'application spécifiques :

```
nodeSelector:
  kubernetes.io/os: linux
  region: us-west
  app.kubernetes.io/name: mysql
```

3. Appliquez les valeurs de `nodeSelectorConfig.yaml` déposer:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect -f nodeSelectorConfig.yaml --reuse-values
```

Cela remplace les restrictions par défaut par celles que vous avez spécifiées dans le `nodeSelectorConfig.yaml` déposer.

Gérer Trident Protect

Gérer l'autorisation et le contrôle d'accès de Trident Protect

Trident Protect utilise le modèle Kubernetes de contrôle d'accès basé sur les rôles (RBAC). Par défaut, Trident Protect fournit un seul espace de noms système et son compte de service par défaut associé. Si votre organisation compte de nombreux utilisateurs ou des besoins de sécurité spécifiques, vous pouvez utiliser les fonctionnalités RBAC de Trident Protect pour obtenir un contrôle plus précis sur l'accès aux ressources et aux espaces de noms.

L'administrateur du cluster a toujours accès aux ressources par défaut `trident-protect` espace de noms, et peut également accéder aux ressources de tous les autres espaces de noms. Pour contrôler l'accès aux ressources et aux applications, vous devez créer des espaces de noms supplémentaires et y ajouter des ressources et des applications.

Notez qu'aucun utilisateur ne peut créer de demandes de changement (CR) de gestion des données d'application par défaut. `trident-protect` espace de noms. Vous devez créer des CR de gestion des données d'application dans un espace de noms d'application (il est recommandé de créer les CR de gestion des données d'application dans le même espace de noms que leur application associée).

Seuls les administrateurs devraient avoir accès aux objets de ressources personnalisés privilégiés de Trident Protect, notamment :

- **AppVault** : Nécessite des données d'identification de compartiment
- **AutoSupportBundle** : Collecte les métriques, les journaux et autres données sensibles de Trident Protect
- **AutoSupportBundleSchedule** : Gère les planifications de collecte des journaux

Il est recommandé d'utiliser le contrôle d'accès basé sur les rôles (RBAC) pour limiter l'accès aux objets privilégiés aux seuls administrateurs.

Pour plus d'informations sur la manière dont le RBAC régule l'accès aux ressources et aux espaces de noms, consultez la documentation. "Documentation RBAC Kubernetes" .

Pour plus d'informations sur les comptes de service, veuillez consulter le "Documentation des comptes de service Kubernetes" .

Exemple : Gérer l'accès pour deux groupes d'utilisateurs

Par exemple, une organisation possède un administrateur de cluster, un groupe d'utilisateurs ingénieurs et un groupe d'utilisateurs marketing. L'administrateur du cluster effectuerait les tâches suivantes pour créer un environnement où le groupe d'ingénierie et le groupe marketing n'auraient accès qu'aux ressources attribuées à leurs espaces de noms respectifs.

Étape 1 : Créer un espace de noms pour contenir les ressources de chaque groupe

La création d'un espace de noms vous permet de séparer logiquement les ressources et de mieux contrôler qui y a accès.

Étapes

1. Créez un espace de noms pour le groupe d'ingénierie :

```
kubectl create ns engineering-ns
```

2. Créez un espace de noms pour le groupe marketing :

```
kubectl create ns marketing-ns
```

Étape 2 : Créez de nouveaux comptes de service pour interagir avec les ressources de chaque espace de noms

Chaque nouvel espace de noms que vous créez est fourni avec un compte de service par défaut, mais vous devriez créer un compte de service pour chaque groupe d'utilisateurs afin de pouvoir répartir davantage les privilèges entre les groupes à l'avenir si nécessaire.

Étapes

1. Créer un compte de service pour le groupe d'ingénierie :

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: eng-user
  namespace: engineering-ns
```

2. Créer un compte de service pour le groupe marketing :

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: mkt-user
  namespace: marketing-ns
```

Étape 3 : Créez un secret pour chaque nouveau compte de service

Un secret de compte de service est utilisé pour s'authentifier auprès du compte de service et peut être facilement supprimé et recréé en cas de compromission.

Étapes

1. Créez un secret pour le compte du service d'ingénierie :

```
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: eng-user
  name: eng-user-secret
  namespace: engineering-ns
type: kubernetes.io/service-account-token
```

2. Créez un secret pour le compte du service marketing :

```
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: mkt-user
  name: mkt-user-secret
  namespace: marketing-ns
type: kubernetes.io/service-account-token
```

Étape 4 : Créez un objet RoleBinding pour lier l'objet ClusterRole à chaque nouveau compte de service.

Un objet ClusterRole par défaut est créé lors de l'installation de Trident Protect. Vous pouvez lier ce ClusterRole au compte de service en créant et en appliquant un objet RoleBinding.

Étapes

1. Associez le rôle ClusterRole au compte de service d'ingénierie :

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: engineering-ns-tenant-rolebinding
  namespace: engineering-ns
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-protect-tenant-cluster-role
subjects:
- kind: ServiceAccount
  name: eng-user
  namespace: engineering-ns
```

2. Associez le rôle ClusterRole au compte de service marketing :

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: marketing-ns-tenant-rolebinding
  namespace: marketing-ns
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-protect-tenant-cluster-role
subjects:
- kind: ServiceAccount
  name: mkt-user
  namespace: marketing-ns
```

Étape 5 : Tester les autorisations

Vérifiez que les autorisations sont correctes.

Étapes

1. Confirmer que les utilisateurs ingénieurs peuvent accéder aux ressources d'ingénierie :

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get applications.protect.trident.netapp.io -n engineering-ns
```

2. Confirmer que les utilisateurs ingénieurs n'ont pas accès aux ressources marketing :

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get applications.protect.trident.netapp.io -n marketing-ns
```

Étape 6 : Accorder l'accès aux objets AppVault

Pour effectuer des tâches de gestion des données telles que les sauvegardes et les instantanés, l'administrateur du cluster doit accorder l'accès aux objets AppVault aux utilisateurs individuels.

Étapes

1. Créez et appliquez un fichier YAML combinant AppVault et secret, qui accorde à un utilisateur l'accès à un AppVault. Par exemple, la demande de changement suivante accorde à l'utilisateur l'accès à un AppVault `eng-user` :

```
apiVersion: v1
data:
  accessKeyID: <ID_value>
  secretAccessKey: <key_value>
kind: Secret
metadata:
  name: appvault-for-eng-user-only-secret
  namespace: trident-protect
type: Opaque
---
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: appvault-for-eng-user-only
  namespace: trident-protect # Trident Protect system namespace
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: testbucket
      endpoint: 192.168.0.1:30000
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-for-eng-user-only-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-for-eng-user-only-secret
  providerType: GenericS3
```

2. Créez et appliquez un rôle CR pour permettre aux administrateurs de cluster d'accorder l'accès à des ressources spécifiques dans un espace de noms. Par exemple:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: eng-user-appvault-reader
  namespace: trident-protect
rules:
- apiGroups:
  - protect.trident.netapp.io
  resourceNames:
  - appvault-for-enguser-only
  resources:
  - appvaults
  verbs:
  - get
```

3. Créez et appliquez une ressource personnalisée RoleBinding pour lier les autorisations à l'utilisateur eng-user. Par exemple:

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: eng-user-read-appvault-binding
  namespace: trident-protect
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: eng-user-appvault-reader
subjects:
- kind: ServiceAccount
  name: eng-user
  namespace: engineering-ns
```

4. Vérifiez que les autorisations sont correctes.

   a. Tentative de récupération des informations des objets AppVault pour tous les espaces de noms :

   ```
   kubectl get appvaults -n trident-protect
   --as=system:serviceaccount:engineering-ns:eng-user
   ```

   Vous devriez obtenir un résultat similaire à celui-ci :

```
Error from server (Forbidden): appvaults.protect.trident.netapp.io is
forbidden: User "system:serviceaccount:engineering-ns:eng-user"
cannot list resource "appvaults" in API group
"protect.trident.netapp.io" in the namespace "trident-protect"
```

b. Vérifiez si l'utilisateur peut accéder aux informations AppVault auxquelles il est désormais autorisé à accéder :

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get appvaults.protect.trident.netapp.io/appvault-for-eng-user-only -n
trident-protect
```

Vous devriez obtenir un résultat similaire à celui-ci :

```
yes
```

Résultat

Les utilisateurs auxquels vous avez accordé des autorisations AppVault doivent pouvoir utiliser les objets AppVault autorisés pour les opérations de gestion des données d'application, et ne doivent pas pouvoir accéder à des ressources en dehors des espaces de noms attribués ni créer de nouvelles ressources auxquelles ils n'ont pas accès.

Surveiller les ressources de Trident Protect

Vous pouvez utiliser les outils open source kube-state-metrics, Prometheus et Alertmanager pour surveiller l'état des ressources protégées par Trident Protect.

Le service kube-state-metrics génère des métriques à partir des communications de l'API Kubernetes. Son utilisation conjointe avec Trident Protect permet d'obtenir des informations utiles sur l'état des ressources de votre environnement.

Prometheus est une boîte à outils capable d'ingérer les données générées par kube-state-metrics et de les présenter sous forme d'informations facilement lisibles sur ces objets. Ensemble, kube-state-metrics et Prometheus vous permettent de surveiller l'état et la santé des ressources que vous gérez avec Trident Protect.

Alertmanager est un service qui ingère les alertes envoyées par des outils tels que Prometheus et les achemine vers des destinations que vous configurez.

> Les configurations et les conseils inclus dans ces étapes ne sont que des exemples ; vous devez les personnaliser en fonction de votre environnement. Veuillez vous référer à la documentation officielle suivante pour obtenir des instructions et une assistance spécifiques :
>
> - "documentation kube-state-metrics"
> - "Documentation Prometheus"
> - "Documentation d'Alertmanager"

Étape 1 : Installer les outils de surveillance

Pour activer la surveillance des ressources dans Trident Protect, vous devez installer et configurer kube-state-metrics, Promethus et Alertmanager.

Installer kube-state-metrics

Vous pouvez installer kube-state-metrics à l'aide de Helm.

Étapes

1. Ajoutez le graphique Helm kube-state-metrics. Par exemple:

```
helm repo add prometheus-community https://prometheus-
community.github.io/helm-charts
helm repo update
```

2. Appliquez le CRD Prometheus ServiceMonitor au cluster :

```
kubectl apply -f https://raw.githubusercontent.com/prometheus-
operator/prometheus-operator/main/example/prometheus-operator-
crd/monitoring.coreos.com_servicemonitors.yaml
```

3. Créez un fichier de configuration pour le graphique Helm (par exemple, `metrics-config.yaml`). Vous pouvez personnaliser la configuration d'exemple suivante pour l'adapter à votre environnement :

metrics-config.yaml : configuration du graphique Helm kube-state-metrics

```
---
extraArgs:
  # Collect only custom metrics
  - --custom-resource-state-only=true

customResourceState:
  enabled: true
  config:
    kind: CustomResourceStateMetrics
    spec:
      resources:
      - groupVersionKind:
          group: protect.trident.netapp.io
          kind: "Backup"
          version: "v1"
        labelsFromPath:
          backup_uid: [metadata, uid]
          backup_name: [metadata, name]
          creation_time: [metadata, creationTimestamp]
        metrics:
        - name: backup_info
          help: "Exposes details about the Backup state"
          each:
            type: Info
            info:
              labelsFromPath:
                appVaultReference: ["spec", "appVaultRef"]
                appReference: ["spec", "applicationRef"]
rbac:
  extraRules:
  - apiGroups: ["protect.trident.netapp.io"]
    resources: ["backups"]
    verbs: ["list", "watch"]

# Collect metrics from all namespaces
namespaces: ""

# Ensure that the metrics are collected by Prometheus
prometheus:
  monitor:
    enabled: true
```

4. Installez kube-state-metrics en déployant le graphique Helm. Par exemple:

```
helm install custom-resource -f metrics-config.yaml prometheus-
community/kube-state-metrics --version 5.21.0
```

5. Configurez kube-state-metrics pour générer des métriques pour les ressources personnalisées utilisées par Trident Protect en suivant les instructions du guide. "Documentation sur la ressource personnalisée kube-state-metrics" .

Installer Prometheus

Vous pouvez installer Prometheus en suivant les instructions du "Documentation Prometheus" .

Installer Alertmanager

Vous pouvez installer Alertmanager en suivant les instructions du "Documentation d'Alertmanager" .

Étape 2 : Configurer les outils de surveillance pour qu'ils fonctionnent ensemble

Après avoir installé les outils de surveillance, vous devez les configurer pour qu'ils fonctionnent ensemble.

Étapes

1. Intégrer kube-state-metrics avec Prometheus. Modifier le fichier de configuration Prometheus(`prometheus.yaml`) et ajoutez les informations du service kube-state-metrics. Par exemple:

prometheus.yaml : intégration du service kube-state-metrics avec Prometheus

```
---
apiVersion: v1
kind: ConfigMap
metadata:
  name: prometheus-config
  namespace: trident-protect
data:
  prometheus.yaml: |
    global:
      scrape_interval: 15s
    scrape_configs:
      - job_name: 'kube-state-metrics'
        static_configs:
          - targets: ['kube-state-metrics.trident-protect.svc:8080']
```

2. Configurez Prometheus pour acheminer les alertes vers Alertmanager. Modifier le fichier de configuration Prometheus(`prometheus.yaml`) et ajoutez la section suivante :

prometheus.yaml : Envoyer des alertes à Alertmanager

```
alerting:
  alertmanagers:
    - static_configs:
        - targets:
            - alertmanager.trident-protect.svc:9093
```

Résultat

Prometheus peut désormais collecter des métriques à partir de kube-state-metrics et envoyer des alertes à Alertmanager. Vous êtes maintenant prêt à configurer les conditions qui déclenchent une alerte et les destinations de ces alertes.

Étape 3 : Configurer les alertes et leurs destinations

Une fois les outils configurés pour fonctionner ensemble, vous devez configurer le type d'informations qui déclenchent les alertes et l'endroit où ces alertes doivent être envoyées.

Exemple d'alerte : échec de la sauvegarde

L'exemple suivant définit une alerte critique qui se déclenche lorsque l'état de la ressource personnalisée de sauvegarde est défini sur `Error` pendant 5 secondes ou plus. Vous pouvez personnaliser cet exemple pour qu'il corresponde à votre environnement et inclure cet extrait YAML dans votre fichier. `prometheus.yaml` fichier de configuration :

rules.yaml : Définir une alerte Prometheus pour les sauvegardes ayant échoué

```
rules.yaml: |
  groups:
    - name: fail-backup
        rules:
          - alert: BackupFailed
            expr: kube_customresource_backup_info{status="Error"}
            for: 5s
            labels:
              severity: critical
            annotations:
              summary: "Backup failed"
              description: "A backup has failed."
```

Configurez Alertmanager pour envoyer des alertes vers d'autres canaux.

Vous pouvez configurer Alertmanager pour envoyer des notifications vers d'autres canaux, tels que le courrier électronique, PagerDuty, Microsoft Teams ou d'autres services de notification, en spécifiant la configuration correspondante dans le `alertmanager.yaml` déposer.

L'exemple suivant configure Alertmanager pour envoyer des notifications à un canal Slack. Pour adapter cet exemple à votre environnement, remplacez la valeur de `api_url` clé avec l'URL du webhook Slack utilisée dans votre environnement :

alertmanager.yaml : Envoyer les alertes à un canal Slack

```
data:
  alertmanager.yaml: |
    global:
      resolve_timeout: 5m
    route:
      receiver: 'slack-notifications'
    receivers:
      - name: 'slack-notifications'
        slack_configs:
          - api_url: '<your-slack-webhook-url>'
            channel: '#failed-backups-channel'
            send_resolved: false
```

Générer un ensemble de support Trident Protect

Trident Protect permet aux administrateurs de générer des ensembles contenant des informations utiles au support NetApp , notamment des journaux, des métriques et des informations de topologie sur les clusters et les applications gérés. Si vous êtes connecté à Internet, vous pouvez télécharger des bundles de support sur le site de support NetApp (NSS) à l'aide d'un fichier de ressources personnalisé (CR).

Créez un ensemble de support à l'aide d'une demande de changement.

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-support-bundle.yaml`).
2. Configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.triggerType**: (*Obligatoire*) Détermine si le bundle de support est généré immédiatement ou planifié. La génération des paquets est programmée à minuit UTC. Valeurs possibles :
     - Programmé
     - Manuel
   - **spec.uploadEnabled** : (*Optionnel*) Contrôle si le bundle de support doit être téléchargé sur le site de support NetApp après sa génération. Si non spécifié, la valeur par défaut est `false` . Valeurs possibles :
     - true
     - faux (par défaut)
   - **spec.dataWindowStart**: (*Optionnel*) Une chaîne de date au format RFC 3339 qui spécifie la date et l'heure auxquelles la fenêtre de données incluses dans le bundle de support doit commencer. Si aucune valeur n'est spécifiée, la date par défaut est celle d'il y a 24 heures. La date la plus ancienne que vous pouvez spécifier remonte à 7 jours.

     Exemple de YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: AutoSupportBundle
metadata:
  name: trident-protect-support-bundle
spec:
  triggerType: Manual
  uploadEnabled: true
  dataWindowStart: 2024-05-05T12:30:00Z
```

3. Après avoir rempli le `trident-protect-support-bundle.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-support-bundle.yaml -n trident-protect
```

Créez un ensemble de support à l'aide de l'interface de ligne de commande (CLI).

Étapes

1. Créez le paquet de support en remplaçant les valeurs entre crochets par les informations provenant

de votre environnement. Le `trigger-type` détermine si le lot est créé immédiatement ou si le délai de création est dicté par la planification, et peut être `Manual` ou `Scheduled` . Le paramètre par défaut est `Manual` .

Par exemple:

```
tridentctl-protect create autosupportbundle <my-bundle-name>
--trigger-type <trigger-type> -n trident-protect
```

Surveiller et récupérer le pack de support

Après avoir créé un bundle de support à l'aide de l'une ou l'autre méthode, vous pouvez surveiller sa progression de génération et le récupérer sur votre système local.

Étapes

1. Attendez le `status.generationState` atteindre `Completed` État. Vous pouvez surveiller la progression de la génération avec la commande suivante :

   ```
   kubectl get autosupportbundle trident-protect-support-bundle -n trident-
   protect
   ```

2. Récupérez le pack de support sur votre système local. Obtenez la commande de copie à partir du bundle AutoSupport terminé :

   ```
   kubectl describe autosupportbundle trident-protect-support-bundle -n
   trident-protect
   ```

   Trouvez le `kubectl cp` Copiez la commande affichée dans le résultat et exécutez-la en remplaçant l'argument de destination par votre répertoire local préféré.

Amélioration de Trident Protect

Vous pouvez mettre à jour Trident Protect vers la dernière version pour bénéficier des nouvelles fonctionnalités ou des correctifs de bugs.

> Lors de la mise à niveau depuis la version 24.10, les instantanés exécutés pendant la mise à niveau peuvent échouer. Cette défaillance n'empêche pas la création de futurs instantanés, qu'ils soient manuels ou planifiés. Si la création d'un instantané échoue lors de la mise à niveau, vous pouvez en créer manuellement un nouveau pour garantir la protection de votre application.
>
> Pour éviter d'éventuelles défaillances, vous pouvez désactiver toutes les planifications de capture d'instantanés avant la mise à niveau et les réactiver après. Cependant, cela a pour conséquence de manquer toutes les captures d'écran planifiées pendant la période de mise à niveau.

Pour mettre à niveau Trident Protect, procédez comme suit.

Étapes

1. Mettre à jour le dépôt Trident Helm :

```
helm repo update
```

2. Mettez à niveau les CRD Trident Protect :

> Cette étape est nécessaire si vous effectuez une mise à niveau depuis une version antérieure à la 25.06, car les CRD sont désormais inclus dans le tableau Trident Protect Helm.

a. Exécutez cette commande pour transférer la gestion des CRD depuis `trident-protect-crds` à `trident-protect` :

```
kubectl get crd | grep protect.trident.netapp.io | awk '{print $1}' |
xargs -I {} kubectl patch crd {} --type merge -p '{"metadata":
{"annotations":{"meta.helm.sh/release-name": "trident-protect"}}}'
```

b. Exécutez cette commande pour supprimer le secret Helm pour le `trident-protect-crds` graphique:

> Ne désinstallez pas le `trident-protect-crds` Utilisez Helm pour créer un graphique, car cela pourrait supprimer vos CRD et toutes les données associées.

```
kubectl delete secret -n trident-protect -l name=trident-protect-
crds,owner=helm
```

3. Mise à niveau de Trident Protect :

```
helm upgrade trident-protect netapp-trident-protect/trident-protect
--version 100.2506.0 --namespace trident-protect
```

Gérer et protéger les applications

Utilisez les objets Trident Protect AppVault pour gérer les compartiments.

La ressource personnalisée (CR) du compartiment pour Trident Protect est connue sous le nom d'AppVault. Les objets AppVault sont la représentation déclarative du flux de travail Kubernetes d'un bucket de stockage. Un AppVault CR contient les configurations nécessaires pour qu'un bucket soit utilisé dans les opérations de protection, telles que les sauvegardes, les snapshots, les opérations de restauration et la réplication SnapMirror .

Seuls les administrateurs peuvent créer des AppVaults.

Vous devez créer une CR AppVault manuellement ou depuis la ligne de commande lorsque vous effectuez des opérations de protection des données sur une application. La CR AppVault est spécifique à votre environnement et vous pouvez vous inspirer des exemples de cette page pour créer des CR AppVault.

Assurez-vous que le fichier CR d'AppVault se trouve sur le cluster où Trident Protect est installé. Si le CR AppVault n'existe pas ou si vous ne pouvez pas y accéder, la ligne de commande affiche une erreur.

Configurer l'authentification et les mots de passe AppVault

Avant de créer un AppVault CR, assurez-vous que l'AppVault et le dispositif de transfert de données que vous choisissez peuvent s'authentifier auprès du fournisseur et de toutes les ressources associées.

Mots de passe du référentiel de déplacement de données

Lorsque vous créez des objets AppVault à l'aide de CR ou du plugin CLI Trident Protect, vous pouvez spécifier un secret Kubernetes avec des mots de passe personnalisés pour le chiffrement Restic et Kopia. Si vous ne spécifiez pas de mot de passe secret, Trident Protect utilise un mot de passe par défaut.

- Lors de la création manuelle de demandes de changement AppVault, utilisez le champ **spec.dataMoverPasswordSecretRef** pour spécifier le secret.
- Lors de la création d'objets AppVault à l'aide de l'interface de ligne de commande Trident Protect, utilisez le `--data-mover-password-secret-ref` argument permettant de préciser le secret.

Créer un mot de passe secret pour le référentiel de déplacement de données

Utilisez les exemples suivants pour créer le mot de passe secret. Lorsque vous créez des objets AppVault, vous pouvez indiquer à Trident Protect d'utiliser ce secret pour s'authentifier auprès du référentiel de transfert de données.

- Selon le logiciel de transfert de données que vous utilisez, il vous suffit d'indiquer le mot de passe correspondant. Par exemple, si vous utilisez Restic et que vous ne prévoyez pas d'utiliser Kopia à l'avenir, vous pouvez inclure uniquement le mot de passe Restic lors de la création du secret.
- Conservez le mot de passe en lieu sûr. Vous en aurez besoin pour restaurer les données sur le même cluster ou sur un autre. Si le cluster ou le `trident-protect` L'espace de noms a été supprimé ; vous ne pourrez pas restaurer vos sauvegardes ou vos instantanés sans le mot de passe.

Utilisez un CR

```
---
apiVersion: v1
data:
  KOPIA_PASSWORD: <base64-encoded-password>
  RESTIC_PASSWORD: <base64-encoded-password>
kind: Secret
metadata:
  name: my-optional-data-mover-secret
  namespace: trident-protect
type: Opaque
```

Utiliser la CLI

```
kubectl create secret generic my-optional-data-mover-secret \
--from-literal=KOPIA_PASSWORD=<plain-text-password> \
--from-literal=RESTIC_PASSWORD=<plain-text-password> \
-n trident-protect
```

Autorisations IAM de stockage compatibles S3

Lorsque vous accédez à un stockage compatible S3 tel qu'Amazon S3, Generic S3, "StorageGrid S3" , ou "ONTAP S3" Lors de l'utilisation de Trident Protect, vous devez vous assurer que les informations d'identification de l'utilisateur que vous fournissez disposent des autorisations nécessaires pour accéder au compartiment. Voici un exemple de politique accordant les autorisations minimales requises pour l'accès avec Trident Protect. Vous pouvez appliquer cette politique à l'utilisateur qui gère les politiques de compartiment compatibles S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    }
  ]
}
```

Pour plus d'informations sur les politiques Amazon S3, reportez-vous aux exemples dans la documentation. "Documentation Amazon S3" .

Identité du pod EKS pour l'authentification Amazon S3 (AWS)

Trident Protect prend en charge EKS Pod Identity pour les opérations de déplacement de données Kopia. Cette fonctionnalité permet un accès sécurisé aux buckets S3 sans stocker les informations d'identification AWS dans les secrets Kubernetes.

Configuration requise pour l'identification du pod EKS avec Trident Protect

Avant d'utiliser EKS Pod Identity avec Trident Protect, assurez-vous des points suivants :

- L'identité de pod est activée sur votre cluster EKS.
- Vous avez créé un rôle IAM avec les autorisations de compartiment S3 nécessaires. Pour en savoir plus, consultez "Autorisations IAM de stockage compatibles S3".
- Le rôle IAM est associé aux comptes de service Trident Protect suivants :
  - `<trident-protect>-controller-manager`
  - `<trident-protect>-resource-backup`
  - `<trident-protect>-resource-restore`
  - `<trident-protect>-resource-delete`

Pour obtenir des instructions détaillées sur l'activation de Pod Identity et l'association des rôles IAM aux comptes de service, veuillez consulter la documentation. "Documentation sur l'identité des pods AWS EKS" .

Configuration d'AppVault Lorsque vous utilisez EKS Pod Identity, configurez votre ressource personnalisée AppVault avec le `useIAM: true` drapeau au lieu d'identifiants explicites :

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: eks-protect-vault
  namespace: trident-protect
spec:
  providerType: AWS
  providerConfig:
    s3:
      bucketName: trident-protect-aws
      endpoint: s3.example.com
      useIAM: true
```

Exemples de génération de clés AppVault pour les fournisseurs de cloud

Lors de la définition d'un AppVault CR, vous devez inclure des informations d'identification pour accéder aux ressources hébergées par le fournisseur, sauf si vous utilisez l'authentification IAM. La manière dont vous générez les clés pour les informations d'identification varie selon le fournisseur. Voici des exemples de génération de clés en ligne de commande pour plusieurs fournisseurs. Vous pouvez utiliser les exemples suivants pour créer des clés pour les informations d'identification de chaque fournisseur de cloud.

Google Cloud

```
kubectl create secret generic <secret-name> \
--from-file=credentials=<mycreds-file.json> \
-n trident-protect
```

Amazon S3 (AWS)

```
kubectl create secret generic <secret-name> \
--from-literal=accessKeyID=<objectstorage-accesskey> \
--from-literal=secretAccessKey=<amazon-s3-trident-protect-src-bucket
-secret> \
-n trident-protect
```

Microsoft Azure

```
kubectl create secret generic <secret-name> \
--from-literal=accountKey=<secret-name> \
-n trident-protect
```

S3 générique

```
kubectl create secret generic <secret-name> \
--from-literal=accessKeyID=<objectstorage-accesskey> \
--from-literal=secretAccessKey=<generic-s3-trident-protect-src-bucket
-secret> \
-n trident-protect
```

ONTAP S3

```
kubectl create secret generic <secret-name> \
--from-literal=accessKeyID=<objectstorage-accesskey> \
--from-literal=secretAccessKey=<ontap-s3-trident-protect-src-bucket
-secret> \
-n trident-protect
```

StorageGrid S3

```
kubectl create secret generic <secret-name> \
--from-literal=accessKeyID=<objectstorage-accesskey> \
--from-literal=secretAccessKey=<storagegrid-s3-trident-protect-src
-bucket-secret> \
-n trident-protect
```

Exemples de création d'AppVault

Vous trouverez ci-dessous des exemples de définitions AppVault pour chaque fournisseur.

Exemples de CR AppVault

Vous pouvez utiliser les exemples de CR suivants pour créer des objets AppVault pour chaque fournisseur de cloud.

- Vous pouvez éventuellement spécifier un secret Kubernetes contenant des mots de passe personnalisés pour le chiffrement des référentiels Restic et Kopia. Se référer àMots de passe du référentiel de déplacement de données pour plus d'informations.
- Pour les objets Amazon S3 (AWS) AppVault, vous pouvez éventuellement spécifier un jeton de session, ce qui est utile si vous utilisez l'authentification unique (SSO). Ce jeton est créé lorsque vous générez des clés pour le fournisseur dansExemples de génération de clés AppVault pour les fournisseurs de cloud .
- Pour les objets S3 AppVault, vous pouvez éventuellement spécifier une URL de proxy de sortie pour le trafic S3 sortant à l'aide de `spec.providerConfig.S3.proxyURL` clé.

Google Cloud

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: gcp-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: GCP
  providerConfig:
    gcp:
      bucketName: trident-protect-src-bucket
      projectID: project-id
  providerCredentials:
    credentials:
      valueFromSecret:
        key: credentials
        name: gcp-trident-protect-src-bucket-secret
```

Amazon S3 (AWS)

```
---
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: amazon-s3-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: AWS
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
      proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret
    sessionToken:
      valueFromSecret:
        key: sessionToken
        name: s3-secret
```

Pour les environnements EKS utilisant Pod Identity avec Kopia Data Mover, vous pouvez supprimer le `providerCredentials` section et ajouter `useIAM: true` sous le `s3` plutôt une configuration.

Microsoft Azure

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: azure-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: Azure
  providerConfig:
    azure:
      accountName: account-name
      bucketName: trident-protect-src-bucket
  providerCredentials:
    accountKey:
      valueFromSecret:
        key: accountKey
        name: azure-trident-protect-src-bucket-secret
```

S3 générique

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: generic-s3-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: GenericS3
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
      proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret
```

ONTAP S3

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: OntapS3
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
      proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret
```

StorageGrid S3

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: storagegrid-s3-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: StorageGridS3
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
      proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret
```

Exemples de création d'AppVault à l'aide de l'interface de ligne de commande Trident Protect

Vous pouvez utiliser les exemples de commandes CLI suivants pour créer des demandes de changement AppVault pour chaque fournisseur.

- Vous pouvez éventuellement spécifier un secret Kubernetes contenant des mots de passe personnalisés pour le chiffrement des référentiels Restic et Kopia. Se référer àMots de passe du référentiel de déplacement de données pour plus d'informations.
- Pour les objets S3 AppVault, vous pouvez éventuellement spécifier une URL de proxy de sortie pour le trafic S3 sortant à l'aide de `--proxy-url <ip_address:port>` argument.

Google Cloud

```
tridentctl-protect create vault GCP <vault-name> \
--bucket <mybucket> \
--project <my-gcp-project> \
--secret <secret-name>/credentials \
--data-mover-password-secret-ref <my-optional-data-mover-secret> \
-n trident-protect
```

Amazon S3 (AWS)

```
tridentctl-protect create vault AWS <vault-name> \
--bucket <bucket-name> \
--secret  <secret-name>  \
--endpoint <s3-endpoint> \
--data-mover-password-secret-ref <my-optional-data-mover-secret> \
-n trident-protect
```

Microsoft Azure

```
tridentctl-protect create vault Azure <vault-name> \
--account <account-name> \
--bucket <bucket-name> \
--secret <secret-name> \
--data-mover-password-secret-ref <my-optional-data-mover-secret> \
-n trident-protect
```

S3 générique

```
tridentctl-protect create vault GenericS3 <vault-name> \
--bucket <bucket-name> \
--secret  <secret-name>  \
--endpoint <s3-endpoint> \
--data-mover-password-secret-ref <my-optional-data-mover-secret> \
-n trident-protect
```

ONTAP S3

```
tridentctl-protect create vault OntapS3 <vault-name> \
--bucket <bucket-name> \
--secret  <secret-name>  \
--endpoint <s3-endpoint> \
--data-mover-password-secret-ref <my-optional-data-mover-secret> \
-n trident-protect
```

StorageGrid S3

```
tridentctl-protect create vault StorageGridS3 <vault-name> \
--bucket <bucket-name> \
--secret  <secret-name>  \
--endpoint <s3-endpoint> \
--data-mover-password-secret-ref <my-optional-data-mover-secret> \
-n trident-protect
```

Consultez les informations d'AppVault

Vous pouvez utiliser le plugin CLI Trident Protect pour consulter les informations relatives aux objets AppVault que vous avez créés sur le cluster.

Étapes

1. Afficher le contenu d'un objet AppVault :

```
tridentctl-protect get appvaultcontent gcp-vault \
--show-resources all \
-n trident-protect
```

Exemple de résultat :

```
+-------------+-------+----------+-----------------------------
+---------------------------+
|   CLUSTER   |  APP  |   TYPE   |            NAME             |
TIMESTAMP         |
+-------------+-------+----------+-----------------------------
+---------------------------+
|             | mysql | snapshot | mysnap                      | 2024-
08-09 21:02:11 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815180300 | 2024-
08-15 18:03:06 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815190300 | 2024-
08-15 19:03:06 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815200300 | 2024-
08-15 20:03:06 (UTC) |
| production1 | mysql | backup   | hourly-e7db6-20240815180300 | 2024-
08-15 18:04:25 (UTC) |
| production1 | mysql | backup   | hourly-e7db6-20240815190300 | 2024-
08-15 19:03:30 (UTC) |
| production1 | mysql | backup   | hourly-e7db6-20240815200300 | 2024-
08-15 20:04:21 (UTC) |
| production1 | mysql | backup   | mybackup5                   | 2024-
08-09 22:25:13 (UTC) |
|             | mysql | backup   | mybackup                    | 2024-
08-09 21:02:52 (UTC) |
+-------------+-------+----------+-----------------------------
+---------------------------+
```

2. Pour afficher le chemin AppVaultPath de chaque ressource, vous pouvez également utiliser l'indicateur. `--show-paths` .

   Le nom du cluster dans la première colonne du tableau n'est disponible que si un nom de cluster a été spécifié dans l'installation Helm de Trident Protect. Par exemple: `--set clusterName=production1` .

Supprimer un AppVault

Vous pouvez supprimer un objet AppVault à tout moment.

> Ne retirez pas le `finalizers` Saisissez la clé dans la ressource personnalisée AppVault avant de supprimer l'objet AppVault. Si vous procédez ainsi, cela peut entraîner la présence de données résiduelles dans le compartiment AppVault et de ressources orphelines dans le cluster.

Avant de commencer

Assurez-vous d'avoir supprimé toutes les ressources de configuration (CR) de snapshot et de sauvegarde utilisées par l'AppVault que vous souhaitez supprimer.

Supprimer un AppVault à l'aide de l'interface de ligne de commande Kubernetes

1. Supprimez l'objet AppVault, en le remplaçant `appvault-name` avec le nom de l'objet AppVault à supprimer :

```
kubectl delete appvault <appvault-name> \
-n trident-protect
```

Supprimer un AppVault à l'aide de l'interface de ligne de commande Trident Protect

1. Supprimez l'objet AppVault, en le remplaçant `appvault-name` avec le nom de l'objet AppVault à supprimer :

```
tridentctl-protect delete appvault <appvault-name> \
-n trident-protect
```

Définissez une application de gestion avec Trident Protect

Vous pouvez définir une application que vous souhaitez gérer avec Trident Protect en créant une demande de changement d'application et une demande de changement AppVault associée.

Créer une demande de changement AppVault

Vous devez créer une ressource personnalisée AppVault qui sera utilisée lors des opérations de protection des données sur l'application, et cette ressource personnalisée AppVault doit résider sur le cluster où Trident Protect est installé. La demande de changement (CR) AppVault est spécifique à votre environnement ; pour des exemples de CR AppVault, reportez-vous à"Ressources personnalisées AppVault."

Définir une application

Vous devez définir chaque application que vous souhaitez gérer avec Trident Protect. Vous pouvez définir une application de gestion soit en créant manuellement une demande de changement d'application, soit en utilisant l'interface de ligne de commande (CLI) de Trident Protect.

Ajouter une application utilisant un CR

Étapes

1. Créez le fichier CR de l'application de destination :
   a. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `maria-app.yaml`).
   b. Configurez les attributs suivants :
      - **metadata.name**: (*Obligatoire*) Le nom de la ressource personnalisée de l'application. Notez le nom que vous choisissez, car d'autres fichiers CR nécessaires aux opérations de protection font référence à cette valeur.
      - **spec.includedNamespaces**: (*Obligatoire*) Utilisez le sélecteur d'espace de noms et d'étiquette pour spécifier les espaces de noms et les ressources utilisés par l'application. L'espace de noms de l'application doit figurer dans cette liste. Le sélecteur d'étiquettes est facultatif et peut être utilisé pour filtrer les ressources au sein de chaque espace de noms spécifié.
      - **spec.includedClusterScopedResources**: (*Optionnel*) Utilisez cet attribut pour spécifier les ressources à portée de cluster à inclure dans la définition de l'application. Cet attribut vous permet de sélectionner ces ressources en fonction de leur groupe, de leur version, de leur type et de leurs étiquettes.
        - **groupVersionKind**: (*Obligatoire*) Spécifie le groupe d'API, la version et le type de la ressource à portée de cluster.
        - **labelSelector**: (*Optionnel*) Filtre les ressources à portée de cluster en fonction de leurs étiquettes.
      - **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**: (*Optional*) Cette annotation s'applique uniquement aux applications définies à partir de machines virtuelles, comme dans les environnements KubeVirt, où les gels du système de fichiers se produisent avant les instantanés. Indiquez si cette application peut écrire sur le système de fichiers lors d'un instantané. Si cette option est activée (true), l'application ignore le paramètre global et peut écrire sur le système de fichiers pendant la création d'un instantané. Si cette option est désactivée, l'application ignore le paramètre global et le système de fichiers est figé lors de la création d'un instantané. Si cette annotation est spécifiée mais que l'application ne comporte aucune machine virtuelle dans sa définition, elle est ignorée. Sauf indication contraire, la demande suit la procédure"Paramètre de gel global Trident Protect" .

Si vous devez appliquer cette annotation après la création d'une application, vous pouvez utiliser la commande suivante :

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
Exemple de YAML :

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (*Facultatif*) Ajouter un filtrage qui inclut ou exclut les ressources marquées avec des étiquettes particulières :

   - **resourceFilter.resourceSelectionCriteria** : (Requis pour le filtrage) Utiliser `Include` ou `Exclude` inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :

     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (groupe, type, version) correspondent selon une opération ET.
       - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
       - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
       - **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
       - **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.

- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Facultatif*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes, telle que définie dans le "Documentation Kubernetes" . Par exemple: `"trident.netapp.io/os=linux"` .

> ⓘ Lorsque les deux `resourceFilter` et `labelSelector` sont utilisés, `resourceFilter` court d'abord, puis ensuite `labelSelector` est appliquée aux ressources résultantes.

Par exemple:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. Après avoir créé la demande de changement (CR) d'application correspondant à votre environnement, appliquez-la. Par exemple:

```
kubectl apply -f maria-app.yaml
```

Étapes

1. Créez et appliquez la définition de l'application en utilisant l'un des exemples suivants, en remplaçant les valeurs entre crochets par les informations de votre environnement. Vous pouvez inclure des espaces de noms et des ressources dans la définition de l'application en utilisant des listes séparées par des virgules avec les arguments indiqués dans les exemples.

   Vous pouvez, si vous le souhaitez, utiliser une annotation lors de la création d'une application pour spécifier si celle-ci peut écrire sur le système de fichiers pendant la prise d'un instantané. Ceci ne s'applique qu'aux applications définies à partir de machines virtuelles, comme dans les environnements KubeVirt, où des blocages du système de fichiers se produisent avant la création des instantanés. Si vous définissez l'annotation sur `true` L'application ignore le paramètre global et peut écrire sur le système de fichiers pendant la création d'un instantané. Si vous le configurez à `false`

L'application ignore alors le paramètre global et le système de fichiers est figé lors de la prise d'un instantané. Si vous utilisez l'annotation mais que l'application ne comporte aucune machine virtuelle dans sa définition, l'annotation est ignorée. Si vous n'utilisez pas l'annotation, l'application suit le comportement attendu."Paramètre de gel global Trident Protect" .

Pour spécifier l'annotation lorsque vous utilisez l'interface de ligne de commande pour créer une application, vous pouvez utiliser la `--annotation` drapeau.

- Créez l'application et utilisez le paramètre global pour le comportement de gel du système de fichiers :

```
tridentctl-protect create application <my_new_app_cr_name>
--namespaces <namespaces_to_include> --csr
<cluster_scoped_resources_to_include> --namespace <my-app-
namespace>
```

- Créez l'application et configurez les paramètres locaux de l'application pour le comportement de gel du système de fichiers :

```
tridentctl-protect create application <my_new_app_cr_name>
--namespaces <namespaces_to_include> --csr
<cluster_scoped_resources_to_include> --namespace <my-app-
namespace> --annotation protect.trident.netapp.io/skip-vm-freeze
=<"true"|"false">
```

Vous pouvez utiliser `--resource-filter-include` et `--resource-filter-exclude` indicateurs permettant d'inclure ou d'exclure des ressources en fonction de `resourceSelectionCriteria` tels que le groupe, le type, la version, les étiquettes, les noms et les espaces de noms, comme illustré dans l'exemple suivant :

```
tridentctl-protect create application <my_new_app_cr_name>
--namespaces <namespaces_to_include> --csr
<cluster_scoped_resources_to_include> --namespace <my-app-namespace>
--resource-filter-include
'[{"Group":"apps","Kind":"Deployment","Version":"v1","Names":["my-
deployment"],"Namespaces":["my-
namespace"],"LabelSelectors":["app=my-app"]}]'
```

Protégez les applications à l'aide de Trident Protect

Vous pouvez protéger toutes les applications gérées par Trident Protect en prenant des instantanés et des sauvegardes à l'aide d'une politique de protection automatisée ou de manière ponctuelle.

Vous pouvez configurer Trident Protect pour geler et dégeler les systèmes de fichiers pendant les opérations de protection des données. "Apprenez-en davantage sur la configuration du gel du système de fichiers avec Trident Protect.".

Créer un instantané à la demande

Vous pouvez créer un instantané à la demande à tout moment.

Les ressources à portée de cluster sont incluses dans une sauvegarde, un instantané ou un clone si elles sont explicitement référencées dans la définition de l'application ou si elles font référence à l'un des espaces de noms de l'application.

Créez un instantané à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-snapshot-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.applicationRef** : Le nom Kubernetes de l'application à capturer.
   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où le contenu de l'instantané (métadonnées) doit être stocké.
   - **spec.reclaimPolicy**: (*Optionnel*) Définit ce qui arrive à l'AppArchive d'un instantané lorsque le CR de l'instantané est supprimé. Cela signifie que même lorsqu'il est réglé sur `Retain` , le cliché sera supprimé. Options valides :
     - `Retain`(défaut)
     - `Delete`

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: Snapshot
     metadata:
       namespace: my-app-namespace
       name: my-cr-name
     spec:
       applicationRef: my-application
       appVaultRef: appvault-name
       reclaimPolicy: Delete
     ```
3. Après avoir rempli le `trident-protect-snapshot-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

   ```
   kubectl apply -f trident-protect-snapshot-cr.yaml
   ```

Créez un instantané à l'aide de l'interface de ligne de commande (CLI).

Étapes

1. Créez l'instantané en remplaçant les valeurs entre crochets par les informations provenant de votre environnement. Par exemple:

   ```
   tridentctl-protect create snapshot <my_snapshot_name> --appvault
   <my_appvault_name> --app <name_of_app_to_snapshot> -n
   <application_namespace>
   ```

Créer une sauvegarde à la demande

Vous pouvez sauvegarder une application à tout moment.

> Les ressources à portée de cluster sont incluses dans une sauvegarde, un instantané ou un clone si elles sont explicitement référencées dans la définition de l'application ou si elles font référence à l'un des espaces de noms de l'application.

Avant de commencer

Assurez-vous que la durée de validité du jeton de session AWS est suffisante pour toute opération de sauvegarde S3 de longue durée. Si le jeton expire pendant l'opération de sauvegarde, l'opération peut échouer.

- Se référer à "Documentation AWS API" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Se référer à "Documentation AWS IAM" pour plus d'informations sur les identifiants avec les ressources AWS.

Créez une sauvegarde à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-backup-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.applicationRef**: (*Obligatoire*) Le nom Kubernetes de l'application à sauvegarder.
   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où le contenu de la sauvegarde doit être stocké.
   - **spec.dataMover**: (*Optionnel*) Une chaîne de caractères indiquant l'outil de sauvegarde à utiliser pour l'opération de sauvegarde. Valeurs possibles (sensible à la casse) :
     - `Restic`
     - `Kopia`(défaut)
   - **spec.reclaimPolicy**: (*Optional*) Définit ce qui arrive à une sauvegarde lorsqu'elle est libérée de sa revendication. Valeurs possibles :
     - `Delete`
     - `Retain`(défaut)
   - **spec.snapshotRef**: (*Optionnel*): Nom du snapshot à utiliser comme source de la sauvegarde. Si aucune information n'est fournie, un instantané temporaire sera créé et sauvegardé.
   - **metadata.annotations.protect.trident.netapp.io/full-backup** : (*Optionnel*) Cette annotation est utilisée pour spécifier si une sauvegarde doit être non incrémentale. Par défaut, toutes les sauvegardes sont incrémentielles. Toutefois, si cette annotation est définie sur `true` , la sauvegarde devient non incrémentale. Si aucune option n'est spécifiée, la sauvegarde suit le paramètre de sauvegarde incrémentielle par défaut. Il est recommandé d'effectuer périodiquement une sauvegarde complète, puis d'effectuer des sauvegardes incrémentales entre les sauvegardes complètes afin de minimiser les risques liés aux restaurations.

     Exemple de YAML :

```yaml
---
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
  annotations:
    protect.trident.netapp.io/full-backup: "true"
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: Kopia
```

3. Après avoir rempli le `trident-protect-backup-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-backup-cr.yaml
```

Créez une sauvegarde à l'aide de l'interface de ligne de commande (CLI).

Étapes

1. Créez la sauvegarde en remplaçant les valeurs entre crochets par les informations provenant de votre environnement. Par exemple:

```
tridentctl-protect create backup <my_backup_name> --appvault <my-
vault-name> --app <name_of_app_to_back_up> --data-mover
<Kopia_or_Restic> -n <application_namespace>
```

   Vous pouvez utiliser, si vous le souhaitez, le `--full-backup` indicateur permettant de spécifier si une sauvegarde doit être non incrémentale. Par défaut, toutes les sauvegardes sont incrémentielles. Lorsque cette option est utilisée, la sauvegarde devient non incrémentale. Il est recommandé d'effectuer périodiquement une sauvegarde complète, puis d'effectuer des sauvegardes incrémentales entre les sauvegardes complètes afin de minimiser les risques liés aux restaurations.

Élaborer un calendrier de protection des données

Une politique de protection protège une application en créant des instantanés, des sauvegardes ou les deux selon un calendrier défini. Vous pouvez choisir de créer des instantanés et des sauvegardes toutes les heures, tous les jours, toutes les semaines et tous les mois, et vous pouvez spécifier le nombre de copies à conserver. Vous pouvez planifier une sauvegarde complète non incrémentielle en utilisant l'annotation full-backup-rule. Par défaut, toutes les sauvegardes sont incrémentielles. L'exécution périodique d'une sauvegarde complète, ainsi que de sauvegardes incrémentielles entre les deux, permet de réduire le risque associé aux restaurations.

- Vous pouvez créer des planifications pour les instantanés uniquement en configurant `backupRetention` à zéro et `snapshotRetention` à une valeur supérieure à zéro. Paramètre `snapshotRetention` La valeur zéro signifie que les sauvegardes planifiées continueront à créer des instantanés, mais ceux-ci seront temporaires et supprimés immédiatement une fois la sauvegarde terminée.
- Les ressources à portée de cluster sont incluses dans une sauvegarde, un instantané ou un clone si elles sont explicitement référencées dans la définition de l'application ou si elles font référence à l'un des espaces de noms de l'application.

Créez un planning à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-schedule-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.dataMover**: (*Optionnel*) Une chaîne de caractères indiquant l'outil de sauvegarde à utiliser pour l'opération de sauvegarde. Valeurs possibles (sensible à la casse) :
     - `Restic`
     - `Kopia`(défaut)
   - **spec.applicationRef** : Nom Kubernetes de l'application à sauvegarder.
   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où le contenu de la sauvegarde doit être stocké.
   - **spec.backupRetention**: Le nombre de sauvegardes à conserver. Zéro indique qu'aucune sauvegarde ne doit être créée (instantanés uniquement).
   - **spec.snapshotRetention** : Le nombre d'instantanés à conserver. La valeur zéro indique qu'aucun instantané ne doit être créé.
   - **spec.granularity** : La fréquence à laquelle la planification doit s'exécuter. Valeurs possibles, ainsi que les champs associés obligatoires :
     - `Hourly`(nécessite que vous précisiez `spec.minute`)
     - `Daily`(nécessite que vous précisiez `spec.minute` et `spec.hour`)
     - `Weekly`(nécessite que vous précisiez `spec.minute, spec.hour` , et `spec.dayOfWeek`)
     - `Monthly`(nécessite que vous précisiez `spec.minute, spec.hour` , et `spec.dayOfMonth`)
     - `Custom`
   - **spec.dayOfMonth**: (*Facultatif*) Le jour du mois (1 - 31) auquel la planification doit s'exécuter. Ce champ est obligatoire si la granularité est définie sur `Monthly` . La valeur doit être fournie sous forme de chaîne.
   - **spec.dayOfWeek**: (*Facultatif*) Le jour de la semaine (0 - 7) pendant lequel la planification doit s'exécuter. Les valeurs de 0 ou 7 indiquent dimanche. Ce champ est obligatoire si la granularité est définie sur `Weekly` . La valeur doit être fournie sous forme de chaîne.
   - **spec.hour**: (*Facultatif*) L'heure de la journée (0 - 23) à laquelle le programme doit s'exécuter. Ce champ est obligatoire si la granularité est définie sur `Daily` , `Weekly` , ou `Monthly` . La valeur doit être fournie sous forme de chaîne.
   - **spec.minute**: (*Facultatif*) La minute de l'heure (0 - 59) à laquelle la planification doit s'exécuter. Ce champ est obligatoire si la granularité est définie sur `Hourly` , `Daily` , `Weekly` , ou `Monthly` . La valeur doit être fournie sous forme de chaîne.
   - **metadata.annotations.protect.trident.netapp.io/full-backup-rule**: (*Optionnel*) Cette annotation est utilisée pour spécifier la règle de planification de la sauvegarde complète. Vous pouvez le paramétrer pour `always` pour une sauvegarde complète et permanente ou personnalisez-la en fonction de vos besoins. Par exemple, si vous choisissez une granularité quotidienne, vous

pouvez spécifier les jours de la semaine où la sauvegarde complète doit avoir lieu.

Exemple de YAML pour la planification de sauvegarde et de snapshot :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  namespace: my-app-namespace
  name: my-cr-name
  annotations:
    protect.trident.netapp.io/full-backup-rule: "Monday,Thursday"
spec:
  dataMover: Kopia
  applicationRef: my-application
  appVaultRef: appvault-name
  backupRetention: "15"
  snapshotRetention: "15"
  granularity: Daily
  hour: "0"
  minute: "0"
```

Exemple de YAML pour la planification des instantanés uniquement :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  namespace: my-app-namespace
  name: my-snapshot-schedule
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  backupRetention: "0"
  snapshotRetention: "15"
  granularity: Daily
  hour: "2"
  minute: "0"
```

3. Après avoir rempli le `trident-protect-schedule-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-schedule-cr.yaml
```

Créez une planification à l'aide de l'interface de ligne de commande (CLI).

Étapes

1. Créez le calendrier de protection en remplaçant les valeurs entre parenthèses par les informations provenant de votre environnement. Par exemple:

   Vous pouvez utiliser `tridentctl-protect create schedule --help` pour afficher des informations d'aide détaillées sur cette commande.

   ```
   tridentctl-protect create schedule <my_schedule_name> --appvault
   <my_appvault_name> --app <name_of_app_to_snapshot> --backup
   -retention <how_many_backups_to_retain> --data-mover
   <Kopia_or_Restic> --day-of-month <day_of_month_to_run_schedule>
   --day-of-week <day_of_month_to_run_schedule> --granularity
   <frequency_to_run> --hour <hour_of_day_to_run> --minute
   <minute_of_hour_to_run> --recurrence-rule <recurrence> --snapshot
   -retention <how_many_snapshots_to_retain> -n <application_namespace>
   --full-backup-rule <string>
   ```

   Vous pouvez paramétrer le `--full-backup-rule` drapeau à `always` pour une sauvegarde complète et permanente ou personnalisez-la en fonction de vos besoins. Par exemple, si vous choisissez une granularité quotidienne, vous pouvez spécifier les jours de la semaine où la sauvegarde complète doit avoir lieu. Par exemple, utilisez `--full-backup-rule "Monday,Thursday"` programmer une sauvegarde complète les lundis et jeudis.

   Pour les planifications ne prenant en compte que les instantanés, définissez `--backup-retention 0` et spécifiez une valeur supérieure à 0 pour `--snapshot-retention` .

Supprimer un instantané

Supprimez les instantanés planifiés ou à la demande dont vous n'avez plus besoin.

Étapes

1. Supprimez la ressource personnalisée (CR) associée à l'instantané :

   ```
   kubectl delete snapshot <snapshot_name> -n my-app-namespace
   ```

Supprimer une sauvegarde

Supprimez les sauvegardes planifiées ou à la demande dont vous n'avez plus besoin.

Assurez-vous que la politique de réclamation est configurée pour `Delete` supprimer toutes les données de sauvegarde du stockage d'objets. Le paramètre par défaut de la politique est `Retain` pour éviter toute perte accidentelle de données. Si la politique n'est pas modifiée à `Delete` Les données de sauvegarde resteront stockées dans l'objet et devront être supprimées manuellement.

Étapes

1. Supprimez la CR de sauvegarde associée à la sauvegarde :

```
kubectl delete backup <backup_name> -n my-app-namespace
```

Vérifier l'état d'une opération de sauvegarde

Vous pouvez utiliser la ligne de commande pour vérifier l'état d'une opération de sauvegarde : en cours, terminée ou ayant échoué.

Étapes

1. Utilisez la commande suivante pour récupérer l'état de l'opération de sauvegarde, en remplaçant les valeurs entre parenthèses par les informations provenant de votre environnement :

```
kubectl get backup -n <namespace_name> <my_backup_cr_name> -o jsonpath
='{.status}'
```

Activer la sauvegarde et la restauration des opérations azure-netapp-files (ANF)

Si vous avez installé Trident Protect, vous pouvez activer une fonctionnalité de sauvegarde et de restauration économe en espace pour les backends de stockage qui utilisent la classe de stockage azure-netapp-files et qui ont été créés avant Trident 24.06. Cette fonctionnalité est compatible avec les volumes NFSv4 et ne consomme pas d'espace supplémentaire du pool de capacité.

Avant de commencer

Assurez-vous de ce qui suit :

- Vous avez installé Trident Protect.
- Vous avez défini une application dans Trident Protect. Cette application offrira des fonctionnalités de protection limitées jusqu'à ce que vous ayez terminé cette procédure.
- Tu as `azure-netapp-files` sélectionné comme classe de stockage par défaut pour votre système de stockage dorsal.

Développez pour afficher les étapes de configuration

1. Procédez comme suit dans Trident si le volume ANF a été créé avant la mise à niveau vers Trident 24.10 :

   a. Activez le répertoire de snapshots pour chaque PV basé sur azure-netapp-files et associé à l'application :

   ```
   tridentctl update volume <pv name> --snapshot-dir=true -n trident
   ```

   b. Vérifiez que le répertoire des instantanés a été activé pour chaque PV associé :

   ```
   tridentctl get volume <pv name> -n trident -o yaml | grep
   snapshotDir
   ```

   Réponse:

   ```
   snapshotDirectory: "true"
   ```

   +
   Lorsque le répertoire de snapshots n'est pas activé, le système choisit la fonctionnalité de sauvegarde standard, qui consomme temporairement de l'espace dans le pool de capacité pendant le processus de sauvegarde. Dans ce cas, assurez-vous de disposer d'un espace suffisant dans le pool de capacité pour créer un volume temporaire de la taille du volume sauvegardé.

Résultat

L'application est prête pour la sauvegarde et la restauration à l'aide de Trident Protect. Chaque PVC peut également être utilisé par d'autres applications pour les sauvegardes et les restaurations.

Restaurer les applications

Restaurez les applications à l'aide de Trident Protect

Vous pouvez utiliser Trident Protect pour restaurer votre application à partir d'un instantané ou d'une sauvegarde. La restauration à partir d'un instantané existant sera plus rapide lors de la restauration de l'application sur le même cluster.

- Lorsque vous restaurez une application, tous les points d'exécution configurés pour celle-ci sont restaurés avec elle. Si un point d'entrée d'exécution post-restauration est présent, il s'exécute automatiquement dans le cadre de l'opération de restauration.
- La restauration à partir d'une sauvegarde vers un espace de noms différent ou vers l'espace de noms d'origine est prise en charge pour les volumes qtree. Cependant, la restauration à partir d'un instantané vers un espace de noms différent ou vers l'espace de noms d'origine n'est pas prise en charge pour les volumes qtree.
- Vous pouvez utiliser des paramètres avancés pour personnaliser les opérations de restauration. Pour en savoir plus, consultez "Utilisez les paramètres de restauration avancés de Trident Protect".

Restaurer à partir d'une sauvegarde vers un espace de noms différent

Lorsque vous restaurez une sauvegarde dans un espace de noms différent à l'aide d'une ressource personnalisée BackupRestore, Trident Protect restaure l'application dans un nouvel espace de noms et crée une ressource personnalisée d'application pour l'application restaurée. Pour protéger l'application restaurée, créez des sauvegardes ou des instantanés à la demande, ou établissez un calendrier de protection.

La restauration d'une sauvegarde dans un espace de noms différent contenant des ressources existantes ne modifiera pas les ressources qui partagent les mêmes noms que celles de la sauvegarde. Pour restaurer toutes les ressources de la sauvegarde, supprimez et recréez l'espace de noms cible, ou restaurez la sauvegarde dans un nouvel espace de noms.

Avant de commencer

Assurez-vous que la durée d'expiration du jeton de session AWS est suffisante pour toute opération de restauration S3 de longue durée. Si le jeton expire pendant l'opération de restauration, celle-ci peut échouer.

- Se référer à "Documentation AWS API" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Se référer à "Documentation AWS IAM" pour plus d'informations sur les identifiants avec les ressources AWS.

Lorsque vous restaurez des sauvegardes à l'aide de Kopia comme outil de transfert de données, vous pouvez éventuellement spécifier des annotations dans le CR ou utiliser l'interface de ligne de commande pour contrôler le comportement du stockage temporaire utilisé par Kopia. Se référer à "Documentation Kopia" pour plus d'informations sur les options que vous pouvez configurer. Utilisez le `tridentctl-protect create --help` commande pour plus d'informations sur la spécification des annotations avec l'interface de ligne de commande Trident Protect.

Utilisez un CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-backup-restore-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appArchivePath** : Chemin d'accès dans AppVault où sont stockés les contenus de sauvegarde. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où sont stockés les contenus de sauvegarde.
   - **spec.namespaceMapping** : Le mappage de l'espace de noms source de l'opération de restauration vers l'espace de noms de destination. Remplacer `my-source-namespace` et `my-destination-namespace` avec des informations provenant de votre environnement.

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: my-cr-name
       namespace: my-destination-namespace
     spec:
       appArchivePath: my-backup-path
       appVaultRef: appvault-name
       namespaceMapping: [{"source": "my-source-namespace",
     "destination": "my-destination-namespace"}]
     ```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées par des étiquettes particulières :

   > Trident Protect sélectionne automatiquement certaines ressources en raison de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Requis pour le filtrage) Utiliser `Include` ou `Exclude` inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs

à l'intérieur de chaque élément (groupe, type, version) correspondent selon une opération ET.

- **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
- **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
- **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
- **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Facultatif*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes, telle que définie dans le "Documentation Kubernetes" . Par exemple: `"trident.netapp.io/os=linux"` .

  Par exemple:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le `trident-protect-backup-restore-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Utiliser la CLI

Étapes

1. Restaurez la sauvegarde dans un espace de noms différent, en remplaçant les valeurs entre crochets par les informations de votre environnement. Le `namespace-mapping` L'argument utilise des espaces de noms séparés par deux-points pour associer les espaces de noms source aux espaces de noms de destination corrects au format `source1:dest1,source2:dest2` . Par exemple:

```
tridentctl-protect create backuprestore <my_restore_name> \
--backup <backup_namespace>/<backup_to_restore> \
--namespace-mapping <source_to_destination_namespace_mapping> \
-n <application_namespace>
```

Restaurer à partir d'une sauvegarde vers l'espace de noms d'origine

Vous pouvez restaurer une sauvegarde dans l'espace de noms d'origine à tout moment.

Avant de commencer

Assurez-vous que la durée d'expiration du jeton de session AWS est suffisante pour toute opération de restauration S3 de longue durée. Si le jeton expire pendant l'opération de restauration, celle-ci peut échouer.

- Se référer à "Documentation AWS API" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Se référer à "Documentation AWS IAM" pour plus d'informations sur les identifiants avec les ressources AWS.

> Lorsque vous restaurez des sauvegardes à l'aide de Kopia comme outil de transfert de données, vous pouvez éventuellement spécifier des annotations dans le CR ou utiliser l'interface de ligne de commande pour contrôler le comportement du stockage temporaire utilisé par Kopia. Se référer à "Documentation Kopia" pour plus d'informations sur les options que vous pouvez configurer. Utilisez le `tridentctl-protect create --help` commande pour plus d'informations sur la spécification des annotations avec l'interface de ligne de commande Trident Protect.

Utilisez un CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-backup-ipr-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appArchivePath** : Chemin d'accès dans AppVault où sont stockés les contenus de sauvegarde. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où sont stockés les contenus de sauvegarde.

     Par exemple:

```
---
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées par des étiquettes particulières :

   Trident Protect sélectionne automatiquement certaines ressources en raison de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Requis pour le filtrage) Utiliser `Include` ou `Exclude` inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (groupe, type, version) correspondent selon une opération ET.
       - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
       - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.

- **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
- **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Facultatif*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes, telle que définie dans le "Documentation Kubernetes" . Par exemple: `"trident.netapp.io/os=linux"` .

  Par exemple:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le `trident-protect-backup-ipr-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

Utiliser la CLI

Étapes

1. Restaurez la sauvegarde dans l'espace de noms d'origine, en remplaçant les valeurs entre crochets par les informations de votre environnement. Le `backup` L'argument utilise un espace de noms et un nom de sauvegarde au format `<namespace>/<name>` . Par exemple:

```
tridentctl-protect create backupinplacerestore <my_restore_name> \
--backup <namespace/backup_to_restore> \
-n <application_namespace>
```

Restaurer à partir d'une sauvegarde vers un cluster différent

Vous pouvez restaurer une sauvegarde sur un autre cluster en cas de problème avec le cluster d'origine.

> Lorsque vous restaurez des sauvegardes à l'aide de Kopia comme outil de transfert de données, vous pouvez éventuellement spécifier des annotations dans le CR ou utiliser l'interface de ligne de commande pour contrôler le comportement du stockage temporaire utilisé par Kopia. Se référer à "Documentation Kopia" pour plus d'informations sur les options que vous pouvez configurer. Utilisez le `tridentctl-protect create --help` commande pour plus d'informations sur la spécification des annotations avec l'interface de ligne de commande Trident Protect.

Avant de commencer

Assurez-vous que les conditions préalables suivantes sont remplies :

- Le cluster de destination possède Trident Protect installé.
- Le cluster de destination a accès au chemin du compartiment du même AppVault que le cluster source, où la sauvegarde est stockée.
- Assurez-vous que votre environnement local peut se connecter au compartiment de stockage d'objets défini dans la ressource personnalisée AppVault lors de l'exécution. `tridentctl-protect get appvaultcontent` commande. Si des restrictions réseau empêchent l'accès, exécutez plutôt l'interface de ligne de commande Trident Protect depuis un pod sur le cluster de destination.
- Assurez-vous que la durée de validité du jeton de session AWS est suffisante pour toute opération de restauration de longue durée. Si le jeton expire pendant l'opération de restauration, celle-ci peut échouer.
  - Se référer à "Documentation AWS API" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
  - Se référer à "Documentation AWS" pour plus d'informations sur les identifiants avec les ressources AWS.

Étapes

1. Vérifiez la disponibilité de la ressource personnalisée AppVault sur le cluster de destination à l'aide du plugin CLI Trident Protect :

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

> Assurez-vous que l'espace de noms destiné à la restauration de l'application existe sur le cluster de destination.

2. Consultez le contenu de la sauvegarde de l'AppVault disponible sur le cluster de destination :

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

L'exécution de cette commande affiche les sauvegardes disponibles dans AppVault, y compris leurs clusters d'origine, les noms des applications correspondantes, les horodatages et les chemins d'accès aux

archives.

Exemple de résultat :

```
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |        TIMESTAMP
|    PATH     |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
```

3. Restaurez l’application sur le cluster de destination en utilisant le nom AppVault et le chemin d’accès à l’archive :

Utilisez un CR

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-backup-restore-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où sont stockés les contenus de sauvegarde.
   - **spec.appArchivePath** : Chemin d'accès dans AppVault où sont stockés les contenus de sauvegarde. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

     Si BackupRestore CR n'est pas disponible, vous pouvez utiliser la commande mentionnée à l'étape 2 pour afficher le contenu de la sauvegarde.

   - **spec.namespaceMapping** : Le mappage de l'espace de noms source de l'opération de restauration vers l'espace de noms de destination. Remplacer `my-source-namespace` et `my-destination-namespace` avec des informations provenant de votre environnement.

     Par exemple:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "
destination": "my-destination-namespace"}]
```

3. Après avoir rempli le `trident-protect-backup-restore-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Utiliser la CLI

1. Utilisez la commande suivante pour restaurer l'application, en remplaçant les valeurs entre crochets par les informations provenant de votre environnement. L'argument namespace-mapping utilise des

espaces de noms séparés par deux-points pour mapper les espaces de noms sources aux espaces de noms de destination corrects au format source1:dest1,source2:dest2. Par exemple:

```
tridentctl-protect create backuprestore <restore_name> \
--namespace-mapping <source_to_destination_namespace_mapping> \
--appvault <appvault_name> \
--path <backup_path> \
--context <destination_cluster_name> \
-n <application_namespace>
```

Restaurer à partir d'un instantané vers un espace de noms différent

Vous pouvez restaurer des données à partir d'un instantané à l'aide d'un fichier de ressources personnalisé (CR), soit dans un espace de noms différent, soit dans l'espace de noms source d'origine. Lorsque vous restaurez un instantané dans un espace de noms différent à l'aide d'une ressource personnalisée SnapshotRestore, Trident Protect restaure l'application dans un nouvel espace de noms et crée une ressource personnalisée d'application pour l'application restaurée. Pour protéger l'application restaurée, créez des sauvegardes ou des instantanés à la demande, ou établissez un calendrier de protection.

SnapshotRestore prend en charge `spec.storageClassMapping` cet attribut est valable uniquement lorsque les classes de stockage source et de destination utilisent le même système de stockage dorsal. Si vous tentez de restaurer un `StorageClass` Si le système de stockage utilisé est différent, l'opération de restauration échouera.

Avant de commencer

Assurez-vous que la durée d'expiration du jeton de session AWS est suffisante pour toute opération de restauration S3 de longue durée. Si le jeton expire pendant l'opération de restauration, celle-ci peut échouer.

- Se référer à "Documentation AWS API" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Se référer à "Documentation AWS IAM" pour plus d'informations sur les identifiants avec les ressources AWS.

Utilisez un CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-snapshot-restore-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où le contenu de l'instantané est stocké.
   - **spec.appArchivePath** : Le chemin d'accès dans AppVault où le contenu des instantanés est stocké. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
     ```

   - **spec.namespaceMapping** : Le mappage de l'espace de noms source de l'opération de restauration vers l'espace de noms de destination. Remplacer `my-source-namespace` et `my-destination-namespace` avec des informations provenant de votre environnement.

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
       appArchivePath: my-snapshot-path
       namespaceMapping: [{"source": "my-source-namespace",
     "destination": "my-destination-namespace"}]
     ```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées par des étiquettes particulières :

   > Trident Protect sélectionne automatiquement certaines ressources en raison de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Requis pour le filtrage) Utiliser `Include` ou `Exclude` inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (groupe, type, version) correspondent selon une opération ET.

- **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
- **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
- **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
- **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Facultatif*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes, telle que définie dans le "Documentation Kubernetes" . Par exemple: `"trident.netapp.io/os=linux"` .

  Par exemple:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le `trident-protect-snapshot-restore-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Utiliser la CLI

Étapes

1. Restaurez l'instantané dans un espace de noms différent, en remplaçant les valeurs entre crochets par les informations de votre environnement.

   - Le `snapshot` L'argument utilise un espace de noms et un nom d'instantané au format `<namespace>/<name>` .
   - Le `namespace-mapping` L'argument utilise des espaces de noms séparés par deux-points pour associer les espaces de noms source aux espaces de noms de destination corrects au format

`source1:dest1,source2:dest2`.

Par exemple:

```
tridentctl-protect create snapshotrestore <my_restore_name> \
--snapshot <namespace/snapshot_to_restore> \
--namespace-mapping <source_to_destination_namespace_mapping> \
-n <application_namespace>
```

Restaurer à partir d'un instantané vers l'espace de noms d'origine

Vous pouvez restaurer un instantané dans l'espace de noms d'origine à tout moment.

Avant de commencer

Assurez-vous que la durée d'expiration du jeton de session AWS est suffisante pour toute opération de restauration S3 de longue durée. Si le jeton expire pendant l'opération de restauration, celle-ci peut échouer.

- Se référer à "Documentation AWS API" pour plus d'informations sur la vérification de l'expiration du jeton de session actuel.
- Se référer à "Documentation AWS IAM" pour plus d'informations sur les identifiants avec les ressources AWS.

Utilisez un CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-snapshot-ipr-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où le contenu de l'instantané est stocké.
   - **spec.appArchivePath** : Le chemin d'accès dans AppVault où le contenu des instantanés est stocké. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
     ```

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotInplaceRestore
     metadata:
       name: my-cr-name
       namespace: my-app-namespace
     spec:
       appVaultRef: appvault-name
         appArchivePath: my-snapshot-path
     ```

3. (*Facultatif*) Si vous devez sélectionner uniquement certaines ressources de l'application à restaurer, ajoutez un filtrage qui inclut ou exclut les ressources marquées par des étiquettes particulières :

   > Trident Protect sélectionne automatiquement certaines ressources en raison de leur relation avec les ressources que vous sélectionnez. Par exemple, si vous sélectionnez une ressource de revendication de volume persistant et qu'elle possède un pod associé, Trident Protect restaurera également le pod associé.

   - **resourceFilter.resourceSelectionCriteria** : (Requis pour le filtrage) Utiliser `Include` ou `Exclude` inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (groupe, type, version) correspondent selon une opération ET.
       - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
       - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
       - **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
       - **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.

- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Facultatif*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes, telle que définie dans le "Documentation Kubernetes" . Par exemple: `"trident.netapp.io/os=linux"` .

  Par exemple:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le `trident-protect-snapshot-ipr-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

Utiliser la CLI

Étapes

1. Restaurez l'instantané dans l'espace de noms d'origine, en remplaçant les valeurs entre crochets par les informations de votre environnement. Par exemple:

```
tridentctl-protect create snapshotinplacerestore <my_restore_name> \
--snapshot <snapshot_to_restore> \
-n <application_namespace>
```

Vérifier l'état d'une opération de restauration

Vous pouvez utiliser la ligne de commande pour vérifier l'état d'une opération de restauration : en cours, terminée ou ayant échoué.

Étapes

1. Utilisez la commande suivante pour récupérer l'état de l'opération de restauration, en remplaçant les valeurs entre parenthèses par les informations provenant de votre environnement :

```
kubectl get backuprestore -n <namespace_name> <my_restore_cr_name> -o
jsonpath='{.status}'
```

Utilisez les paramètres de restauration avancés de Trident Protect

Vous pouvez personnaliser les opérations de restauration à l'aide de paramètres avancés tels que les annotations, les paramètres d'espace de noms et les options de stockage pour répondre à vos besoins spécifiques.

Annotations et étiquettes d'espace de noms lors des opérations de restauration et de basculement

Lors des opérations de restauration et de basculement, les étiquettes et annotations de l'espace de noms de destination sont mises en correspondance avec celles de l'espace de noms source. Les étiquettes ou annotations de l'espace de noms source qui n'existent pas dans l'espace de noms de destination sont ajoutées, et toutes les étiquettes ou annotations existantes sont écrasées pour correspondre à la valeur de l'espace de noms source. Les étiquettes ou annotations qui existent uniquement dans l'espace de noms de destination restent inchangées.

> Si vous utilisez Red Hat OpenShift, il est important de noter le rôle essentiel des annotations d'espace de noms dans les environnements OpenShift. Les annotations d'espace de noms garantissent que les pods restaurés adhèrent aux autorisations et aux configurations de sécurité appropriées définies par les contraintes de contexte de sécurité (SCC) OpenShift et peuvent accéder aux volumes sans problèmes d'autorisation. Pour plus d'informations, veuillez consulter le "Documentation sur les contraintes de contexte de sécurité d'OpenShift" .

Vous pouvez empêcher l'écrasement de certaines annotations dans l'espace de noms de destination en définissant la variable d'environnement Kubernetes. `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` avant d'effectuer l'opération de restauration ou de basculement. Par exemple:

```
helm upgrade trident-protect --set
restoreSkipNamespaceAnnotations=<annotation_key_to_skip_1>,<annotation_key
_to_skip_2> --reuse-values
```

> Lors d'une opération de restauration ou de basculement, toutes les annotations et étiquettes d'espace de noms spécifiées dans `restoreSkipNamespaceAnnotations` et `restoreSkipNamespaceLabels` sont exclues de l'opération de restauration ou de basculement. Assurez-vous que ces paramètres sont configurés lors de l'installation initiale de Helm. Pour en savoir plus, consultez "Configurer les options de filtrage AutoSupport et d'espace de noms".

Si vous avez installé l'application source à l'aide de Helm avec le `--create-namespace` Le drapeau, un traitement spécial est accordé au `name` Légende. Lors du processus de restauration ou de basculement, Trident Protect copie cette étiquette dans l'espace de noms de destination, mais met à jour la valeur avec la valeur de l'espace de noms de destination si la valeur de la source correspond à l'espace de noms source. Si

cette valeur ne correspond pas à l'espace de noms source, elle est copiée dans l'espace de noms de destination sans modification.

Exemple

L'exemple suivant présente un espace de noms source et un espace de noms de destination, chacun avec des annotations et des étiquettes différentes. Vous pouvez voir l'état de l'espace de noms de destination avant et après l'opération, et comment les annotations et les étiquettes sont combinées ou écrasées dans l'espace de noms de destination.

Avant l'opération de restauration ou de basculement

Le tableau suivant illustre l'état des espaces de noms source et de destination de l'exemple avant l'opération de restauration ou de basculement :

Espace de noms	Annotations	Étiquettes
Espace de noms ns-1 (source)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true"	• environnement=production • conformité=hippaa • nom=ns-1
Espace de noms ns-2 (destination)	• annotation.one/key: "true" • annotation.three/key: "false"	• rôle=base de données

Après l'opération de restauration

Le tableau suivant illustre l'état de l'espace de noms de destination d'exemple après l'opération de restauration ou de basculement. Des touches ont été ajoutées, d'autres ont été écrasées, et le `name` L'étiquette a été mise à jour pour correspondre à l'espace de noms de destination :

Espace de noms	Annotations	Étiquettes
Espace de noms ns-2 (destination)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true" • annotation.three/key: "false"	• nom=ns-2 • conformité=hippaa • environnement=production • rôle=base de données

Champs pris en charge

Cette section décrit les champs supplémentaires disponibles pour les opérations de restauration.

Mappage des classes de stockage

Le `spec.storageClassMapping` L'attribut définit un mappage entre une classe de stockage présente dans l'application source et une nouvelle classe de stockage sur le cluster cible. Vous pouvez l'utiliser lors de la migration d'applications entre des clusters avec différentes classes de stockage ou lors du changement du backend de stockage pour les opérations BackupRestore.

Exemple:

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

Annotations prises en charge

Cette section répertorie les annotations prises en charge pour configurer différents comportements du système. Si aucune annotation n'est explicitement définie par l'utilisateur, le système utilisera la valeur par défaut.

Annotation	Type	Description	Valeur par défaut
protect.trident.netapp.io/data-mover-timeout-sec	chaîne	Le temps maximal (en secondes) pendant lequel l'opération de déplacement de données peut être bloquée.	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	chaîne	La limite de taille maximale (en mégaoctets) pour le cache de contenu Kopia.	"1000"

Répliquez les applications à l'aide de NetApp SnapMirror et Trident Protect.

Avec Trident Protect, vous pouvez utiliser les capacités de réplication asynchrone de la technologie NetApp SnapMirror pour répliquer les données et les modifications d'applications d'un système de stockage à un autre, sur le même cluster ou entre différents clusters.

Annotations et étiquettes d'espace de noms lors des opérations de restauration et de basculement

Lors des opérations de restauration et de basculement, les étiquettes et annotations de l'espace de noms de destination sont mises en correspondance avec celles de l'espace de noms source. Les étiquettes ou annotations de l'espace de noms source qui n'existent pas dans l'espace de noms de destination sont ajoutées, et toutes les étiquettes ou annotations existantes sont écrasées pour correspondre à la valeur de l'espace de noms source. Les étiquettes ou annotations qui existent uniquement dans l'espace de noms de destination restent inchangées.

> Si vous utilisez Red Hat OpenShift, il est important de noter le rôle essentiel des annotations d'espace de noms dans les environnements OpenShift. Les annotations d'espace de noms garantissent que les pods restaurés adhèrent aux autorisations et aux configurations de sécurité appropriées définies par les contraintes de contexte de sécurité (SCC) OpenShift et peuvent accéder aux volumes sans problèmes d'autorisation. Pour plus d'informations, veuillez consulter le "Documentation sur les contraintes de contexte de sécurité d'OpenShift" .

Vous pouvez empêcher l'écrasement de certaines annotations dans l'espace de noms de destination en définissant la variable d'environnement Kubernetes. `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` avant

d'effectuer l'opération de restauration ou de basculement. Par exemple:

```
helm upgrade trident-protect --set
restoreSkipNamespaceAnnotations=<annotation_key_to_skip_1>,<annotation_key
_to_skip_2> --reuse-values
```

> Lors d'une opération de restauration ou de basculement, toutes les annotations et étiquettes d'espace de noms spécifiées dans `restoreSkipNamespaceAnnotations` et `restoreSkipNamespaceLabels` sont exclues de l'opération de restauration ou de basculement. Assurez-vous que ces paramètres sont configurés lors de l'installation initiale de Helm. Pour en savoir plus, consultez "Configurer les options de filtrage AutoSupport et d'espace de noms".

Si vous avez installé l'application source à l'aide de Helm avec le `--create-namespace` Le drapeau, un traitement spécial est accordé au `name` Légende. Lors du processus de restauration ou de basculement, Trident Protect copie cette étiquette dans l'espace de noms de destination, mais met à jour la valeur avec la valeur de l'espace de noms de destination si la valeur de la source correspond à l'espace de noms source. Si cette valeur ne correspond pas à l'espace de noms source, elle est copiée dans l'espace de noms de destination sans modification.

Exemple

L'exemple suivant présente un espace de noms source et un espace de noms de destination, chacun avec des annotations et des étiquettes différentes. Vous pouvez voir l'état de l'espace de noms de destination avant et après l'opération, et comment les annotations et les étiquettes sont combinées ou écrasées dans l'espace de noms de destination.

Avant l'opération de restauration ou de basculement

Le tableau suivant illustre l'état des espaces de noms source et de destination de l'exemple avant l'opération de restauration ou de basculement :

Espace de noms	Annotations	Étiquettes
Espace de noms ns-1 (source)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true"	• environnement=production • conformité=hippaa • nom=ns-1
Espace de noms ns-2 (destination)	• annotation.one/key: "true" • annotation.three/key: "false"	• rôle=base de données

Après l'opération de restauration

Le tableau suivant illustre l'état de l'espace de noms de destination d'exemple après l'opération de restauration ou de basculement. Des touches ont été ajoutées, d'autres ont été écrasées, et le `name` L'étiquette a été mise à jour pour correspondre à l'espace de noms de destination :

Espace de noms	Annotations	Étiquettes
Espace de noms ns-2 (destination)	• annotation.one/key: "updatedvalue" • annotation.two/key: "true" • annotation.three/key: "false"	• nom=ns-2 • conformité=hippaa • environnement=production • rôle=base de données

Vous pouvez configurer Trident Protect pour geler et dégeler les systèmes de fichiers pendant les opérations de protection des données. "Apprenez-en davantage sur la configuration du gel du système de fichiers avec Trident Protect.".

Points d'exécution lors des opérations de basculement et d'inversion

Lorsque vous utilisez la relation AppMirror pour protéger votre application, il existe des comportements spécifiques liés aux points d'exécution dont vous devez tenir compte lors des opérations de basculement et de restauration.

- Lors d'un basculement, les points d'entrée d'exécution sont automatiquement copiés du cluster source vers le cluster de destination. Vous n'avez pas besoin de les recréer manuellement. Après le basculement, des points d'entrée d'exécution sont présents dans l'application et s'exécuteront lors de toute action pertinente.
- Lors d'une opération inverse ou d'une resynchronisation inverse, tous les points d'entrée d'exécution existants sur l'application sont supprimés. Lorsque l'application source devient l'application de destination, ces points d'ancrage d'exécution ne sont plus valides et sont supprimés pour empêcher leur exécution.

Pour en savoir plus sur les hooks d'exécution, consultez"Gérer les hooks d'exécution de Trident Protect" .

Établir une relation de réplication

La mise en place d'une relation de réplication implique les éléments suivants :

- Choisir la fréquence à laquelle Trident Protect doit prendre un instantané de l'application (qui inclut les ressources Kubernetes de l'application ainsi que les instantanés de volume pour chacun des volumes de l'application).
- Choix du calendrier de réplication (incluant les ressources Kubernetes ainsi que les données de volume persistant)
- Définir l'heure de la prise de vue

Étapes

1. Sur le cluster source, créez un AppVault pour l'application source. Selon votre fournisseur de stockage, modifiez un exemple dans"Ressources personnalisées AppVault" pour s'adapter à votre environnement :

Créez un AppVault à l'aide d'une demande de changement.

a. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-appvault-primary-source.yaml`).

b. Configurez les attributs suivants :

- **metadata.name**: (*Obligatoire*) Le nom de la ressource personnalisée AppVault. Notez bien le nom que vous choisissez, car d'autres fichiers CR nécessaires à une relation de réplication font référence à cette valeur.
- **spec.providerConfig**: (*Obligatoire*) Stocke la configuration nécessaire pour accéder à AppVault à l'aide du fournisseur spécifié. Choisissez un nom de compartiment et toutes autres informations nécessaires pour votre fournisseur. Notez les valeurs que vous choisissez, car d'autres fichiers CR nécessaires à une relation de réplication font référence à ces valeurs. Se référer à"Ressources personnalisées AppVault" pour des exemples de demandes de changement AppVault avec d'autres fournisseurs.
- **spec.providerCredentials**: (*Obligatoire*) Stocke les références à toutes les informations d'identification requises pour accéder à AppVault à l'aide du fournisseur spécifié.
  - **spec.providerCredentials.valueFromSecret**: (*Obligatoire*) Indique que la valeur d'identification doit provenir d'un secret.
    - **clé**: (*Obligatoire*) La clé valide du secret à sélectionner.
    - **nom** : (*Obligatoire*) Nom du secret contenant la valeur de ce champ. Doit se trouver dans le même espace de noms.
  - **spec.providerCredentials.secretAccessKey**: (*Obligatoire*) La clé d'accès utilisée pour accéder au fournisseur. Le **nom** doit correspondre à **spec.providerCredentials.valueFromSecret.name**.
- **spec.providerType**: (*Obligatoire*) Détermine ce qui fournit la sauvegarde ; par exemple, NetApp ONTAP S3, S3 générique, Google Cloud ou Microsoft Azure. Valeurs possibles :
  - aws
  - azuré
  - GCP
  - générique-s3
  - ontap-s3
  - storagegrid-s3

c. Après avoir rempli le `trident-protect-appvault-primary-source.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-appvault-primary-source.yaml -n
trident-protect
```

Créez un AppVault à l'aide de l'interface de ligne de commande (CLI).

a. Créez l'AppVault en remplaçant les valeurs entre crochets par les informations provenant de votre environnement :

```
tridentctl-protect create vault Azure <vault-name> --account
<account-name> --bucket <bucket-name> --secret <secret-name> -n
trident-protect
```

2. Sur le cluster source, créez l'application source CR :

Créez l'application source à l'aide d'une CR

a. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-app-source.yaml`).

b. Configurez les attributs suivants :

- **metadata.name**: (*Obligatoire*) Le nom de la ressource personnalisée de l'application. Notez bien le nom que vous choisissez, car d'autres fichiers CR nécessaires à une relation de réplication font référence à cette valeur.
- **spec.includedNamespaces**: (*Obligatoire*) Un tableau d'espaces de noms et d'étiquettes associées. Utilisez les noms d'espaces de noms et, éventuellement, restreignez la portée des espaces de noms à l'aide d'étiquettes pour spécifier les ressources qui existent dans les espaces de noms listés ici. L'espace de noms de l'application doit faire partie de ce tableau.

  Exemple de fichier YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: my-app-namespace
      labelSelector: {}
```

c. Après avoir rempli le `trident-protect-app-source.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-app-source.yaml -n my-app-namespace
```

Créez l'application source à l'aide de l'interface de ligne de commande (CLI).

a. Créez l'application source. Par exemple:

```
tridentctl-protect create app <my-app-name> --namespaces
<namespaces-to-be-included> -n <my-app-namespace>
```

3. Vous pouvez également, si vous le souhaitez, prendre un instantané de l'application source sur le cluster source. Cet instantané sert de base à l'application sur le cluster de destination. Si vous ignorez cette étape, vous devrez attendre la prochaine capture d'écran planifiée pour obtenir une version récente. Pour créer un instantané à la demande, reportez-vous à "Créer un instantané à la demande".

4. Sur le cluster source, créez la ressource personnalisée (CR) de planification de réplication :

En plus du calendrier fourni ci-dessous, il est recommandé de créer un calendrier de capture instantanée quotidienne distinct avec une période de conservation de 7 jours afin de maintenir une capture instantanée commune entre les clusters ONTAP appariés. Cela garantit la disponibilité des instantanés pendant une durée maximale de 7 jours, mais cette période de conservation peut être personnalisée en fonction des besoins de l'utilisateur.

En cas de basculement, le système peut utiliser ces instantanés pendant une durée maximale de 7 jours pour les opérations inverses. Cette approche rend le processus inverse plus rapide et plus efficace car seules les modifications apportées depuis le dernier instantané seront transférées, et non la totalité des données.

Si un calendrier existant pour la demande répond déjà aux exigences de conservation souhaitées, aucun calendrier supplémentaire n'est requis.

Créez la planification de réplication à l'aide d'une ressource personnalisée (CR).

a. Créez une planification de réplication pour l'application source :

i. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-schedule.yaml`).

ii. Configurez les attributs suivants :

- **metadata.name**: (*Obligatoire*) Le nom de la ressource personnalisée de planification.
- **spec.appVaultRef** : (*Obligatoire*) Cette valeur doit correspondre au champ metadata.name de l'AppVault pour l'application source.
- **spec.applicationRef**: (*Obligatoire*) Cette valeur doit correspondre au champ metadata.name de la ressource personnalisée (CR) de l'application source.
- **spec.backupRetention**: (*Obligatoire*) Ce champ est obligatoire et sa valeur doit être définie sur 0.
- **spec.enabled** : Doit être défini sur true.
- **spec.granularity** : Doit être défini sur `Custom` .
- **spec.recurrenceRule** : Définissez une date de début en temps UTC et un intervalle de récurrence.
- **spec.snapshotRetention** : Doit être défini sur 2.

Exemple de YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  name: appmirror-schedule
  namespace: my-app-namespace
spec:
  appVaultRef: my-appvault-name
  applicationRef: my-app-name
  backupRetention: "0"
  enabled: true
  granularity: Custom
  recurrenceRule: |-
    DTSTART:20220101T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  snapshotRetention: "2"
```

i. Après avoir rempli le `trident-protect-schedule.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-schedule.yaml -n my-app-
namespace
```

Créez la planification de réplication à l'aide de l'interface de ligne de commande (CLI).

a. Créez la planification de réplication en remplaçant les valeurs entre crochets par les informations provenant de votre environnement :

```
tridentctl-protect create schedule --name appmirror-schedule
--app <my_app_name> --appvault <my_app_vault> --granularity
Custom --recurrence-rule <rule> --snapshot-retention
<snapshot_retention_count> -n <my_app_namespace>
```

Exemple:

```
tridentctl-protect create schedule --name appmirror-schedule
--app <my_app_name> --appvault <my_app_vault> --granularity
Custom --recurrence-rule  "DTSTART:20220101T000200Z
\nRRULE:FREQ=MINUTELY;INTERVAL=5" --snapshot-retention 2 -n
<my_app_namespace>
```

5. Sur le cluster de destination, créez une demande de changement (CR) AppVault d'application source identique à celle que vous avez appliquée sur le cluster source et nommez-la (par exemple, `trident-protect-appvault-primary-destination.yaml`).
6. Appliquer le CR :

```
kubectl apply -f trident-protect-appvault-primary-destination.yaml -n
trident-protect
```

7. Créez une ressource personnalisée AppVault de destination pour l'application de destination sur le cluster de destination. Selon votre fournisseur de stockage, modifiez un exemple dans"Ressources personnalisées AppVault" pour s'adapter à votre environnement :
   a. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-appvault-secondary-destination.yaml`).
   b. Configurez les attributs suivants :
      - **metadata.name**: (*Obligatoire*) Le nom de la ressource personnalisée AppVault. Notez bien le nom que vous choisissez, car d'autres fichiers CR nécessaires à une relation de réplication font référence à cette valeur.
      - **spec.providerConfig**: (*Obligatoire*) Stocke la configuration nécessaire pour accéder à AppVault à l'aide du fournisseur spécifié. Choisissez un `bucketName` et toute autre information nécessaire à votre fournisseur. Notez les valeurs que vous choisissez, car d'autres fichiers CR nécessaires à une relation de réplication font référence à ces valeurs. Se référer à"Ressources personnalisées

AppVault" pour des exemples de demandes de changement AppVault avec d'autres fournisseurs.

- **spec.providerCredentials**: (*Obligatoire*) Stocke les références à toutes les informations d'identification requises pour accéder à AppVault à l'aide du fournisseur spécifié.
  - **spec.providerCredentials.valueFromSecret**: (*Obligatoire*) Indique que la valeur d'identification doit provenir d'un secret.
    - **clé**: (*Obligatoire*) La clé valide du secret à sélectionner.
    - **nom** : (*Obligatoire*) Nom du secret contenant la valeur de ce champ. Doit se trouver dans le même espace de noms.
  - **spec.providerCredentials.secretAccessKey**: (*Obligatoire*) La clé d'accès utilisée pour accéder au fournisseur. Le **nom** doit correspondre à **spec.providerCredentials.valueFromSecret.name**.
- **spec.providerType**: (*Obligatoire*) Détermine ce qui fournit la sauvegarde ; par exemple, NetApp ONTAP S3, S3 générique, Google Cloud ou Microsoft Azure. Valeurs possibles :
  - aws
  - azuré
  - GCP
  - générique-s3
  - ontap-s3
  - storagegrid-s3

c. Après avoir rempli le `trident-protect-appvault-secondary-destination.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-appvault-secondary-destination.yaml
-n trident-protect
```

8. Sur le cluster de destination, créez un fichier CR AppMirrorRelationship :

Créez une relation AppMirror à l'aide d'un CR

a. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-relationship.yaml`).

b. Configurez les attributs suivants :

- **metadata.name:** (Obligatoire) Le nom de la ressource personnalisée AppMirrorRelationship.
- **spec.destinationAppVaultRef** : (*Obligatoire*) Cette valeur doit correspondre au nom de l'AppVault pour l'application de destination sur le cluster de destination.
- **spec.namespaceMapping**: (*Obligatoire*) Les espaces de noms de destination et source doivent correspondre à l'espace de noms de l'application défini dans la CR de l'application respective.
- **spec.sourceAppVaultRef** : (*Obligatoire*) Cette valeur doit correspondre au nom de l'AppVault pour l'application source.
- **spec.sourceApplicationName** : (*Obligatoire*) Cette valeur doit correspondre au nom de l'application source que vous avez définie dans la ressource personnalisée de l'application source.
- **spec.sourceApplicationUID** : (Obligatoire) Cette valeur doit correspondre à l'UID de l'application source que vous avez définie dans la CR de l'application source.
- **spec.storageClassName**: (*Optionnel*) Choisissez le nom d'une classe de stockage valide sur le cluster. La classe de stockage doit être liée à une machine virtuelle de stockage ONTAP qui est appariée avec l'environnement source. Si la classe de stockage n'est pas spécifiée, la classe de stockage par défaut du cluster sera utilisée.
- **spec.recurrenceRule** : Définissez une date de début en temps UTC et un intervalle de récurrence.

  Exemple de YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: AppMirrorRelationship
metadata:
  name: amr-16061e80-1b05-4e80-9d26-d326dc1953d8
  namespace: my-app-namespace
spec:
  desiredState: Established
  destinationAppVaultRef: generic-s3-trident-protect-dst-bucket-
8fe0b902-f369-4317-93d1-ad7f2edc02b5
  namespaceMapping:
    - destination: my-app-namespace
      source: my-app-namespace
  recurrenceRule: |-
    DTSTART:20220101T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  sourceAppVaultRef: generic-s3-trident-protect-src-bucket-
b643cc50-0429-4ad5-971f-ac4a83621922
  sourceApplicationName: my-app-name
  sourceApplicationUID: 7498d32c-328e-4ddd-9029-122540866aeb
  storageClassName: sc-vsim-2
```

c. Après avoir rempli le `trident-protect-relationship.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-
namespace
```

Créez une relation AppMirror à l'aide de l'interface de ligne de commande (CLI).

a. Créez et appliquez l'objet AppMirrorRelationship en remplaçant les valeurs entre crochets par les informations provenant de votre environnement :

```
tridentctl-protect create appmirrorrelationship
<name_of_appmirorrelationship> --destination-app-vault
<my_vault_name> --source-app-vault <my_vault_name> --recurrence
-rule <rule> --namespace-mapping <ns_mapping> --source-app-id
<source_app_UID> --source-app <my_source_app_name> --storage
-class <storage_class_name> -n <application_namespace>
```

Exemple:

```
tridentctl-protect create appmirrorrelationship my-amr
--destination-app-vault appvault2 --source-app-vault appvault1
--recurrence-rule
"DTSTART:20220101T000200Z\nRRULE:FREQ=MINUTELY;INTERVAL=5"
--source-app my-app --namespace-mapping "my-source-ns1:my-dest-
ns1,my-source-ns2:my-dest-ns2" --source-app-id 373f24c1-5769-
404c-93c3-5538af6ccc36 --storage-class my-storage-class -n my-
dest-ns1
```

9. (*Facultatif*) Sur le cluster de destination, vérifiez l'état et le statut de la relation de réplication :

```
kubectl get amr -n my-app-namespace <relationship name> -o=jsonpath
='{.status}' | jq
```

Basculement vers le cluster de destination

Avec Trident Protect, vous pouvez basculer les applications répliquées vers un cluster de destination. Cette procédure interrompt la relation de réplication et met l'application en ligne sur le cluster de destination. Trident Protect n'arrête pas l'application sur le cluster source si elle était opérationnelle.

Étapes

1. Sur le cluster de destination, modifiez le fichier CR AppMirrorRelationship (par exemple, `trident-protect-relationship.yaml`) et modifiez la valeur de **spec.desiredState** en `Promoted` .
2. Enregistrez le fichier CR.
3. Appliquer le CR :

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-namespace
```

4. (*Facultatif*) Créez les plans de protection nécessaires sur l'application basculée.
5. (*Facultatif*) Vérifiez l'état et le statut de la relation de réplication :

```
kubectl get amr -n my-app-namespace <relationship name> -o=jsonpath
='{.status}' | jq
```

Resynchroniser une relation de réplication ayant échoué

L'opération de resynchronisation rétablit la relation de réplication. Après une opération de resynchronisation, l'application source d'origine devient l'application en cours d'exécution, et toutes les modifications apportées à l'application en cours d'exécution sur le cluster de destination sont annulées.

Le processus interrompt l'application sur le cluster de destination avant de rétablir la réplication.

Toutes les données écrites dans l'application de destination pendant le basculement seront perdues.

Étapes

1. Facultatif : sur le cluster source, créez un instantané de l'application source. Cela permet de garantir que les dernières modifications provenant du cluster source sont prises en compte.
2. Sur le cluster de destination, modifiez le fichier CR AppMirrorRelationship (par exemple, `trident-protect-relationship.yaml`) et modifiez la valeur de spec.desiredState en `Established` .
3. Enregistrez le fichier CR.
4. Appliquer le CR :

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-namespace
```

5. Si vous avez créé des plans de protection sur le cluster de destination pour protéger l'application basculée, supprimez-les. Toute planification restante entraîne des échecs de snapshots de volume.

Resynchronisation inverse d'une relation de réplication ayant échoué

Lors d'une resynchronisation inverse d'une relation de réplication ayant basculé, l'application de destination devient l'application source et la source devient la destination. Les modifications apportées à l'application de destination pendant le basculement sont conservées.

Étapes

1. Sur le cluster de destination d'origine, supprimez la ressource personnalisée AppMirrorRelationship. Cela a pour conséquence que la destination devienne la source. S'il reste des plans de protection sur le nouveau cluster de destination, supprimez-les.
2. Établissez une relation de réplication en appliquant les fichiers CR que vous avez initialement utilisés pour établir la relation aux clusters opposés.
3. Assurez-vous que la nouvelle destination (cluster source d'origine) est configurée avec les deux CR AppVault.
4. Configurez une relation de réplication sur le cluster opposé, en configurant les valeurs pour la direction inverse.

sens de réplication de l'application inverse

Lorsque vous inversez le sens de la réplication, Trident Protect déplace l'application vers le système de stockage de destination tout en continuant à répliquer vers le système de stockage source d'origine. Trident Protect arrête l'application source et réplique les données vers la destination avant de basculer vers l'application de destination.

Dans ce cas, vous inversez la source et la destination.

Étapes

1. Sur le cluster source, créez un instantané d'arrêt :

Créez un instantané d'arrêt à l'aide d'une CR

a. Désactivez les calendriers de stratégie de protection pour l'application source.

b. Créer un fichier CR ShutdownSnapshot :

i. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-shutdownsnapshot.yaml`).

ii. Configurez les attributs suivants :

- **metadata.name**: (*Obligatoire*) Le nom de la ressource personnalisée.
- **spec.AppVaultRef** : (*Obligatoire*) Cette valeur doit correspondre au champ metadata.name de l'AppVault pour l'application source.
- **spec.ApplicationRef**: (*Obligatoire*) Cette valeur doit correspondre au champ metadata.name du fichier CR de l'application source.

Exemple de YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: ShutdownSnapshot
metadata:
  name: replication-shutdown-snapshot-afc4c564-e700-4b72-86c3-
c08a5dbe844e
  namespace: my-app-namespace
spec:
  appVaultRef: generic-s3-trident-protect-src-bucket-04b6b4ec-
46a3-420a-b351-45795e1b5e34
  applicationRef: my-app-name
```

c. Après avoir rempli le `trident-protect-shutdownsnapshot.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-shutdownsnapshot.yaml -n my-app-
namespace
```

Créez un instantané d'arrêt à l'aide de l'interface de ligne de commande (CLI).

a. Créez un instantané d'arrêt en remplaçant les valeurs entre crochets par les informations de votre environnement. Par exemple:

```
tridentctl-protect create shutdownsnapshot <my_shutdown_snapshot>
--appvault <my_vault> --app <app_to_snapshot> -n
<application_namespace>
```

2. Sur le cluster source, une fois la capture instantanée de l'arrêt terminée, obtenez l'état de cette capture :

```
kubectl get shutdownsnapshot -n my-app-namespace
<shutdown_snapshot_name> -o yaml
```

3. Sur le cluster source, recherchez la valeur de **shutdownsnapshot.status.appArchivePath** à l'aide de la commande suivante et notez la dernière partie du chemin d'accès au fichier (également appelée nom de base ; il s'agit de tout ce qui suit la dernière barre oblique) :

```
k get shutdownsnapshot -n my-app-namespace <shutdown_snapshot_name> -o
jsonpath='{.status.appArchivePath}'
```

4. Effectuez un basculement du nouveau cluster de destination vers le nouveau cluster source, avec la modification suivante :

> ⓘ À l'étape 2 de la procédure de basculement, incluez le `spec.promotedSnapshot` champ dans le fichier CR AppMirrorRelationship, et définissez sa valeur sur le nom de base que vous avez enregistré à l'étape 3 ci-dessus.

5. Effectuez les étapes de resynchronisation inverses dansResynchronisation inverse d'une relation de réplication ayant échoué .
6. Activez les plans de protection sur le nouveau cluster source.

Résultat

Les actions suivantes se produisent en raison de la réplication inverse :

- Une capture instantanée des ressources Kubernetes de l'application source d'origine est effectuée.
- Les pods de l'application source d'origine sont arrêtés en douceur en supprimant les ressources Kubernetes de l'application (en laissant les PVC et les PV en place).
- Une fois les pods arrêtés, des instantanés des volumes de l'application sont pris et répliqués.
- Les relations SnapMirror sont rompues, ce qui rend les volumes de destination prêts pour la lecture/écriture.
- Les ressources Kubernetes de l'application sont restaurées à partir de l'instantané antérieur à l'arrêt, en utilisant les données de volume répliquées après l'arrêt de l'application source d'origine.
- La réplication est rétablie dans le sens inverse.

Rétablir les applications sur le cluster source d'origine

Avec Trident Protect, vous pouvez effectuer un « retour en arrière » après une opération de basculement en utilisant la séquence d'opérations suivante. Dans ce flux de travail visant à rétablir le sens de réplication d'origine, Trident Protect réplique (resynchronise) toutes les modifications apportées à l'application vers l'application source d'origine avant d'inverser le sens de réplication.

Ce processus débute à partir d'une relation ayant effectué un basculement vers une destination et comprend les étapes suivantes :

- Commencez par un état de basculement.
- Inverser la resynchronisation de la relation de réplication.

> N'effectuez pas d'opération de resynchronisation normale, car cela supprimerait les données écrites sur le cluster de destination pendant la procédure de basculement.

- Inverser le sens de la réplication.

Étapes

1. Effectuez leResynchronisation inverse d'une relation de réplication ayant échoué mesures.
2. Effectuez lesens de réplication de l'application inverse mesures.

Supprimer une relation de réplication

Vous pouvez supprimer une relation de réplication à tout moment. Lorsque vous supprimez la relation de réplication d'applications, cela crée deux applications distinctes sans aucune relation entre elles.

Étapes

1. Sur le cluster de destination actuel, supprimez la ressource personnalisée AppMirrorRelationship :

```
kubectl delete -f trident-protect-relationship.yaml -n my-app-namespace
```

Migrer les applications à l'aide de Trident Protect

Vous pouvez migrer vos applications entre clusters ou vers différentes classes de stockage en restaurant les données de sauvegarde.

> Lors de la migration d'une application, tous les points d'exécution configurés pour celle-ci sont migrés avec elle. Si un point d'entrée d'exécution post-restauration est présent, il s'exécute automatiquement dans le cadre de l'opération de restauration.

opérations de sauvegarde et de restauration

Pour effectuer des opérations de sauvegarde et de restauration dans les scénarios suivants, vous pouvez automatiser des tâches spécifiques de sauvegarde et de restauration.

Cloner sur le même cluster

Pour cloner une application sur le même cluster, créez un instantané ou une sauvegarde et restaurez les données sur le même cluster.

Étapes

1. Effectuez l'une des opérations suivantes :
   a. "Créer un instantané".
   b. "Créer une sauvegarde".
2. Sur le même cluster, effectuez l'une des opérations suivantes, selon que vous ayez créé un instantané ou une sauvegarde :

a. "Restaurez vos données à partir de l'instantané.".

b. "Restaurez vos données à partir de la sauvegarde".

Cloner sur un cluster différent

Pour cloner une application sur un cluster différent (effectuer un clonage inter-clusters), créez une sauvegarde sur le cluster source, puis restaurez la sauvegarde sur un cluster différent. Assurez-vous que Trident Protect est installé sur le cluster de destination.

> Vous pouvez répliquer une application entre différents clusters en utilisant"Réplication SnapMirror" .

Étapes

1. "Créer une sauvegarde".
2. Assurez-vous que la ressource personnalisée AppVault pour le compartiment de stockage d'objets contenant la sauvegarde a été configurée sur le cluster de destination.
3. Sur le cluster de destination,"restaurez vos données à partir de la sauvegarde" .

Migrer des applications d'une classe de stockage à une autre classe de stockage

Vous pouvez migrer des applications d'une classe de stockage vers une autre classe de stockage en restaurant une sauvegarde vers la classe de stockage de destination.

Par exemple (en excluant les secrets de la restauration CR) :

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: "${snapshotRestoreCRName}"
spec:
  appArchivePath: "${snapshotArchivePath}"
  appVaultRef: "${appVaultCRName}"
  namespaceMapping:
    - destination: "${destinationNamespace}"
      source: "${sourceNamespace}"
  storageClassMapping:
    - destination: "${destinationStorageClass}"
      source: "${sourceStorageClass}"
  resourceFilter:
    resourceMatchers:
      kind: Secret
      version: v1
    resourceSelectionCriteria: exclude
```

Restaurez l'instantané à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-snapshot-restore-cr.yaml` .
2. Dans le fichier que vous avez créé, configurez les attributs suivants :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.appArchivePath** : Le chemin d'accès dans AppVault où le contenu des instantanés est stocké. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get snapshots <my-snapshot-name> -n trident-protect -o jsonpath='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où le contenu de l'instantané est stocké.
   - **spec.namespaceMapping** : Le mappage de l'espace de noms source de l'opération de restauration vers l'espace de noms de destination. Remplacer `my-source-namespace` et `my-destination-namespace` avec des informations provenant de votre environnement.

     ```
     ---
     apiVersion: protect.trident.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: my-cr-name
       namespace: trident-protect
     spec:
       appArchivePath: my-snapshot-path
       appVaultRef: appvault-name
       namespaceMapping: [{"source": "my-source-namespace",
     "destination": "my-destination-namespace"}]
     ```

3. Si vous souhaitez sélectionner uniquement certaines ressources de l'application à restaurer, vous pouvez ajouter un filtrage qui inclut ou exclut les ressources marquées d'étiquettes particulières :
   - **resourceFilter.resourceSelectionCriteria** : (Requis pour le filtrage) Utiliser `include or exclude` inclure ou exclure une ressource définie dans resourceMatchers. Ajoutez les paramètres resourceMatchers suivants pour définir les ressources à inclure ou à exclure :
     - **resourceFilter.resourceMatchers** : Un tableau d'objets resourceMatcher. Si vous définissez plusieurs éléments dans ce tableau, ils correspondent selon une opération OU, et les champs à l'intérieur de chaque élément (groupe, type, version) correspondent selon une opération ET.
       - **resourceMatchers[].group**: (*Optionnel*) Groupe de la ressource à filtrer.
       - **resourceMatchers[].kind**: (*Optionnel*) Type de ressource à filtrer.
       - **resourceMatchers[].version**: (*Optionnel*) Version de la ressource à filtrer.
       - **resourceMatchers[].names**: (*Optionnel*) Noms dans le champ metadata.name de

Kubernetes de la ressource à filtrer.

- **resourceMatchers[].namespaces**: (*Optionnel*) Espaces de noms dans le champ metadata.name de Kubernetes de la ressource à filtrer.
- **resourceMatchers[].labelSelectors** : (*Facultatif*) Chaîne de sélection d'étiquette dans le champ metadata.name de la ressource Kubernetes, telle que définie dans le "Documentation Kubernetes" . Par exemple: `"trident.netapp.io/os=linux"` .

  Par exemple:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Après avoir rempli le `trident-protect-snapshot-restore-cr.yaml` fichier contenant les valeurs correctes, appliquer le CR :

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Restaurez l'instantané à l'aide de l'interface de ligne de commande (CLI).

Étapes

1. Restaurez l'instantané dans un espace de noms différent, en remplaçant les valeurs entre crochets par les informations de votre environnement.

   - Le `snapshot` L'argument utilise un espace de noms et un nom d'instantané au format `<namespace>/<name>` .
   - Le `namespace-mapping` L'argument utilise des espaces de noms séparés par deux-points pour associer les espaces de noms source aux espaces de noms de destination corrects au format `source1:dest1,source2:dest2` .

     Par exemple:

```
tridentctl-protect create snapshotrestore <my_restore_name>
--snapshot <namespace/snapshot_to_restore> --namespace-mapping
<source_to_destination_namespace_mapping>
```

Gérer les hooks d'exécution de Trident Protect

Un hook d'exécution est une action personnalisée que vous pouvez configurer pour qu'elle s'exécute conjointement avec une opération de protection des données d'une application gérée. Par exemple, si vous disposez d'une application de base de données, vous pouvez utiliser un hook d'exécution pour suspendre toutes les transactions de base de données avant un instantané et reprendre les transactions une fois l'instantané terminé. Cela garantit des instantanés cohérents avec les applications.

Types de hooks d'exécution

Trident Protect prend en charge les types de hooks d'exécution suivants, en fonction du moment où ils peuvent être exécutés :

- Pré-instantané
- Post-instantané
- Pré-sauvegarde
- Post-sauvegarde
- Post-restauration
- Après le basculement

Ordre d'exécution

Lorsqu'une opération de protection des données est exécutée, les événements de hook d'exécution se produisent dans l'ordre suivant :

1. Tous les hooks d'exécution de pré-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de hooks de pré-opération personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces hooks avant l'opération n'est ni garanti ni configurable.
2. Des blocages du système de fichiers se produisent, le cas échéant. "Apprenez-en davantage sur la configuration du gel du système de fichiers avec Trident Protect.".
3. L'opération de protection des données est effectuée.
4. Les systèmes de fichiers gelés sont dégelés, le cas échéant.
5. Tous les hooks d'exécution post-opération personnalisés applicables sont exécutés sur les conteneurs appropriés. Vous pouvez créer et exécuter autant de hooks post-opération personnalisés que vous le souhaitez, mais l'ordre d'exécution de ces hooks après l'opération n'est ni garanti ni configurable.

Si vous créez plusieurs hooks d'exécution du même type (par exemple, pré-snapshot), l'ordre d'exécution de ces hooks n'est pas garanti. Cependant, l'ordre d'exécution des hooks de différents types est garanti. Par exemple, voici l'ordre d'exécution d'une configuration qui possède tous les différents types de hooks :

1. Hooks pré-instantanés exécutés
2. Hooks post-instantanés exécutés
3. Hooks de pré-sauvegarde exécutés
4. Hooks post-sauvegarde exécutés

L'exemple de commande précédent ne s'applique que lorsque vous exécutez une sauvegarde qui n'utilise pas d'instantané existant.

Vous devez toujours tester vos scripts d'exécution avant de les activer dans un environnement de production. Vous pouvez utiliser la commande « kubectl exec » pour tester facilement les scripts. Après avoir activé les hooks d'exécution dans un environnement de production, testez les snapshots et les sauvegardes résultants pour vous assurer qu'ils sont cohérents. Vous pouvez le faire en clonant l'application dans un espace de noms temporaire, en restaurant l'instantané ou la sauvegarde, puis en testant l'application.

Si un hook d'exécution pré-snapshot ajoute, modifie ou supprime des ressources Kubernetes, ces modifications sont incluses dans le snapshot ou la sauvegarde et dans toute opération de restauration ultérieure.

Remarques importantes sur les hooks d'exécution personnalisés

Tenez compte des éléments suivants lors de la planification des hooks d'exécution pour vos applications.

- Un hook d'exécution doit utiliser un script pour effectuer des actions. De nombreux hooks d'exécution peuvent référencer le même script.
- Trident Protect exige que les scripts utilisés par les hooks d'exécution soient écrits au format de scripts shell exécutables.
- La taille du script est limitée à 96 Ko.
- Trident Protect utilise les paramètres d'exécution et tous les critères correspondants pour déterminer quels hooks sont applicables à une opération de snapshot, de sauvegarde ou de restauration.

Étant donné que les hooks d'exécution réduisent ou désactivent souvent complètement les fonctionnalités de l'application sur laquelle ils s'exécutent, vous devez toujours essayer de minimiser le temps d'exécution de vos hooks d'exécution personnalisés. Si vous démarrez une opération de sauvegarde ou de snapshot avec des hooks d'exécution associés, mais que vous l'annulez ensuite, les hooks sont toujours autorisés à s'exécuter si l'opération de sauvegarde ou de snapshot a déjà commencé. Cela signifie que la logique utilisée dans un hook d'exécution post-sauvegarde ne peut pas supposer que la sauvegarde a été terminée.

Filtres de crochet d'exécution

Lorsque vous ajoutez ou modifiez un hook d'exécution pour une application, vous pouvez ajouter des filtres au hook d'exécution pour gérer les conteneurs auxquels le hook correspondra. Les filtres sont utiles pour les applications qui utilisent la même image de conteneur sur tous les conteneurs, mais peuvent utiliser chaque image à des fins différentes (comme Elasticsearch). Les filtres vous permettent de créer des scénarios dans lesquels les hooks d'exécution s'exécutent sur certains conteneurs identiques, mais pas nécessairement sur tous. Si vous créez plusieurs filtres pour un seul hook d'exécution, ils sont combinés avec un opérateur AND logique. Vous pouvez avoir jusqu'à 10 filtres actifs par hook d'exécution.

Chaque filtre que vous ajoutez à un hook d'exécution utilise une expression régulière pour faire correspondre les conteneurs de votre cluster. Lorsqu'un hook correspond à un conteneur, le hook exécutera son script associé sur ce conteneur. Les expressions régulières pour les filtres utilisent la syntaxe d'expression régulière 2 (RE2), qui ne prend pas en charge la création d'un filtre excluant les conteneurs de la liste des correspondances. Pour plus d'informations sur la syntaxe prise en charge par Trident Protect pour les expressions régulières dans les filtres de hook d'exécution, consultez "Prise en charge de la syntaxe des expressions régulières 2 (RE2)" .

Si vous ajoutez un filtre d'espace de noms à un hook d'exécution qui s'exécute après une opération de restauration ou de clonage et que la source et la destination de restauration ou de clonage se trouvent dans des espaces de noms différents, le filtre d'espace de noms est appliqué uniquement à l'espace de noms de destination.

Exemples de crochets d'exécution

Visitez le "Projet GitHub NetApp Verda" pour télécharger de véritables hooks d'exécution pour des applications populaires telles qu'Apache Cassandra et Elasticsearch. Vous pouvez également voir des exemples et obtenir des idées pour structurer vos propres hooks d'exécution personnalisés.

Créer un point d'accroche d'exécution

Vous pouvez créer un hook d'exécution personnalisé pour une application en utilisant . Vous devez disposer des autorisations de propriétaire, d'administrateur ou de membre pour créer des points d'exécution.

Utilisez un CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-hook.yaml` .
2. Configurez les attributs suivants pour qu'ils correspondent à votre environnement Trident Protect et à la configuration de votre cluster :

   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.applicationRef**: (*Obligatoire*) Le nom Kubernetes de l'application pour laquelle exécuter le hook d'exécution.
   - **spec.stage**: (*Obligatoire*) Une chaîne de caractères indiquant à quelle étape de l'action le hook d'exécution doit s'exécuter. Valeurs possibles :
     - Pré
     - Poste
   - **spec.action**: (*Obligatoire*) Une chaîne indiquant l'action que le hook d'exécution entreprendra, en supposant que tous les filtres de hook d'exécution spécifiés correspondent. Valeurs possibles :
     - Instantané
     - Sauvegarde
     - Restaurer
     - Basculement
   - **spec.enabled**: (*Optionnel*) Indique si ce point d'accroche d'exécution est activé ou désactivé. Si aucune valeur n'est spécifiée, la valeur par défaut est « vrai ».
   - **spec.hookSource**: (*Obligatoire*) Une chaîne contenant le script de hook encodé en base64.
   - **spec.timeout**: (*Optionnel*) Un nombre définissant la durée en minutes pendant laquelle le hook d'exécution est autorisé à s'exécuter. La valeur minimale est de 1 minute, et la valeur par défaut est de 25 minutes si elle n'est pas spécifiée.
   - **spec.arguments**: (*Optionnel*) Une liste YAML d'arguments que vous pouvez spécifier pour le hook d'exécution.
   - **spec.matchingCriteria**: (*Optionnel*) Une liste facultative de paires clé-valeur de critères, chaque paire constituant un filtre de crochet d'exécution. Vous pouvez ajouter jusqu'à 10 filtres par point d'exécution.
   - **spec.matchingCriteria.type**: (*Optionnel*) Une chaîne identifiant le type de filtre de crochet d'exécution. Valeurs possibles :
     - Image conteneur
     - Nom du conteneur
     - Nom du pod
     - Étiquette de podcast
     - Nom de l'espace de noms
   - **spec.matchingCriteria.value**: (*Optionnel*) Une chaîne de caractères ou une expression régulière identifiant la valeur du filtre du point d'exécution.

     Exemple de YAML :

```
apiVersion: protect.trident.netapp.io/v1
kind: ExecHook
metadata:
  name: example-hook-cr
  namespace: my-app-namespace
  annotations:
    astra.netapp.io/astra-control-hook-source-id:
/account/test/hookSource/id
spec:
  applicationRef: my-app-name
  stage: Pre
  action: Snapshot
  enabled: true
  hookSource: IyEvYmluL2Jhc2gKZWNobyAiZXhhbXBsZSBzY3JpcHQiCg==
  timeout: 10
  arguments:
    - FirstExampleArg
    - SecondExampleArg
  matchingCriteria:
    - type: containerName
      value: mysql
    - type: containerImage
      value: bitnami/mysql
    - type: podName
      value: mysql
    - type: namespaceName
      value: mysql-a
    - type: podLabel
      value: app.kubernetes.io/component=primary
    - type: podLabel
      value: helm.sh/chart=mysql-10.1.0
    - type: podLabel
      value: deployment-type=production
```

3. Après avoir rempli le fichier CR avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-hook.yaml
```

Utiliser la CLI

Étapes

1. Créez le point d'exécution en remplaçant les valeurs entre crochets par les informations provenant de votre environnement. Par exemple:

```
tridentctl-protect create exechook <my_exec_hook_name> --action
<action_type> --app <app_to_use_hook> --stage <pre_or_post_stage>
--source-file <script-file> -n <application_namespace>
```

Exécuter manuellement un hook d'exécution

Vous pouvez exécuter manuellement un hook d'exécution à des fins de test ou si vous devez le réexécuter manuellement après un échec. Vous devez disposer des autorisations de propriétaire, d'administrateur ou de membre pour exécuter manuellement les hooks d'exécution.

L'exécution manuelle d'un hook se compose de deux étapes de base :

1. Créez une sauvegarde des ressources, qui collecte les ressources et en crée une copie, déterminant ainsi où le hook s'exécutera.
2. Exécutez le script d'exécution sur la sauvegarde

Étape 1 : Créer une sauvegarde des ressources

Utilisez un CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-resource-backup.yaml` .
2. Configurez les attributs suivants pour qu'ils correspondent à votre environnement Trident Protect et à la configuration de votre cluster :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.applicationRef**: (*Obligatoire*) Le nom Kubernetes de l'application pour laquelle créer la sauvegarde de ressource.
   - **spec.appVaultRef**: (*Obligatoire*) Le nom de l'AppVault où sont stockés les contenus de sauvegarde.
   - **spec.appArchivePath** : Chemin d'accès dans AppVault où sont stockés les contenus de sauvegarde. Vous pouvez utiliser la commande suivante pour trouver ce chemin :

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath='{.status.appArchivePath}'
     ```

     Exemple de YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: ResourceBackup
metadata:
  name: example-resource-backup
spec:
  applicationRef: my-app-name
  appVaultRef: my-appvault-name
  appArchivePath: example-resource-backup
```

3. Après avoir rempli le fichier CR avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-resource-backup.yaml
```

Utiliser la CLI

Étapes

1. Créez la sauvegarde en remplaçant les valeurs entre crochets par les informations provenant de votre environnement. Par exemple:

```
tridentctl protect create resourcebackup <my_backup_name> --app
<my_app_name> --appvault <my_appvault_name> -n
<my_app_namespace> --app-archive-path <app_archive_path>
```

2. Consultez l'état de la sauvegarde. Vous pouvez utiliser cette commande d'exemple à plusieurs reprises jusqu'à ce que l'opération soit terminée :

```
tridentctl protect get resourcebackup -n <my_app_namespace>
<my_backup_name>
```

3. Vérifiez que la sauvegarde a réussi :

```
kubectl describe resourcebackup <my_backup_name>
```

Étape 2 : Exécuter le hook d’exécution

Utilisez un CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le. `trident-protect-hook-run.yaml` .
2. Configurez les attributs suivants pour qu'ils correspondent à votre environnement Trident Protect et à la configuration de votre cluster :
   - **metadata.name** : (*Obligatoire*) Le nom de cette ressource personnalisée ; choisissez un nom unique et pertinent pour votre environnement.
   - **spec.applicationRef** : (*Obligatoire*) Assurez-vous que cette valeur corresponde au nom de l'application de la ressource de sauvegarde que vous avez créée à l'étape 1.
   - **spec.appVaultRef** : (*Obligatoire*) Assurez-vous que cette valeur correspond à l'appVaultRef de la ressource CR ResourceBackup que vous avez créée à l'étape 1.
   - **spec.appArchivePath** : Assurez-vous que cette valeur correspond à appArchivePath de la ressource personnalisée ResourceBackup que vous avez créée à l'étape 1.

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o
     jsonpath='{.status.appArchivePath}'
     ```

   - **spec.action**: (*Obligatoire*) Une chaîne indiquant l'action que le hook d'exécution entreprendra, en supposant que tous les filtres de hook d'exécution spécifiés correspondent. Valeurs possibles :
     - Instantané
     - Sauvegarde
     - Restaurer
     - Basculement
   - **spec.stage**: (*Obligatoire*) Une chaîne de caractères indiquant à quelle étape de l'action le hook d'exécution doit s'exécuter. Cette opération d'accrochage ne permettra pas d'accrocher les hameçons à aucune autre étape. Valeurs possibles :
     - Pré
     - Poste

     Exemple de YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: ExecHooksRun
metadata:
  name: example-hook-run
spec:
  applicationRef: my-app-name
  appVaultRef: my-appvault-name
  appArchivePath: example-resource-backup
  stage: Post
  action: Failover
```

3. Après avoir rempli le fichier CR avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-hook-run.yaml
```

Utiliser la CLI

Étapes

1. Créer la requête d'exécution manuelle du hook :

```
tridentctl protect create exechooksrun <my_exec_hook_run_name>
-n <my_app_namespace> --action snapshot --stage <pre_or_post>
--app <my_app_name> --appvault <my_appvault_name> --path
<my_backup_name>
```

2. Vérifiez l'état d'exécution du hook. Vous pouvez exécuter cette commande à plusieurs reprises jusqu'à ce que l'opération soit terminée :

```
tridentctl protect get exechooksrun -n <my_app_namespace>
<my_exec_hook_run_name>
```

3. Décrivez l'objet exechooksrun pour voir les détails et l'état finaux :

```
kubectl -n <my_app_namespace> describe exechooksrun
<my_exec_hook_run_name>
```

Désinstallez Trident Protect

Vous devrez peut-être supprimer des composants de Trident Protect si vous passez d'une version d'essai à une version complète du produit.

Pour retirer Trident Protect, procédez comme suit.

Étapes

1. Supprimez les fichiers CR de Trident Protect :

   Cette étape n'est pas requise pour la version 25.06 et les versions ultérieures.

   ```
   helm uninstall -n trident-protect trident-protect-crds
   ```

2. Supprimer Trident Protect :

   ```
   helm uninstall -n trident-protect trident-protect
   ```

3. Supprimez l'espace de noms Trident Protect :

   ```
   kubectl delete ns trident-protect
   ```