Reprise après sinistre

NetApp virtualization solutions

NetApp
July 21, 2026

Sommaire

Reprise après sinistre

Prérequis de Trident Protect/AppMirror pour la reprise après sinistre de virtualisation OpenShift

Cette section fournit des informations sur les prérequis pour utiliser NetApp Trident Protect et AppMirror pour la reprise après sinistre des charges de travail OpenShift Virtualization. Cela inclut les configurations de cluster nécessaires, les exigences de stockage et les étapes d'installation pour configurer Trident Protect et AppMirror en vue d'une reprise après sinistre efficace des machines virtuelles exécutées sur OpenShift Virtualization.

Prérequis

1. Un cluster OpenShift Red Hat avec OpenShift Virtualization installé et configuré. Pour les instructions d'installation, consultez le "documentation ici".
2. Deux systèmes de stockage NetApp ONTAP avec une SVM configurée sur chacun, pour fournir du stockage aux clusters OpenShift actifs et de reprise après sinistre. Chaque SVM doit avoir au moins une LIF de gestion et une LIF de données configurées et accessibles depuis le cluster OpenShift correspondant.
3. L'appairage de clusters et l'appairage SVM sont configurés entre les deux systèmes ONTAP pour permettre la réplication des données du SVM du cluster source vers le SVM du cluster de destination. Pour obtenir des instructions sur la configuration de l'appairage de clusters et de l'appairage SVM, consultez la "Documentation sur le peering de clusters ONTAP ici".
4. NetApp Trident est installé et configuré sur le cluster OpenShift pour fournir un stockage persistant à partir du SVM ONTAP. Pour les instructions d'installation, consultez le "Documentation Trident ici".
5. Une configuration de backend Trident a été créée pour la SVM ONTAP et une StorageClass configurée sur le cluster OpenShift pour utiliser ce backend Trident comme provisionneur. Pour obtenir des instructions sur la création d'une configuration de backend Trident et d'une StorageClass, consultez la "Documentation de configuration du backend Trident disponible ici".
6. Accès d'administrateur de cluster au cluster OpenShift et accès d'administrateur au système de stockage ONTAP pour effectuer les configurations nécessaires.
7. Un poste de travail d'administrateur avec `tridentctl` et `oc` des outils installés et ajoutés à la variable d'environnement $PATH pour interagir avec le cluster OpenShift et Trident.
8. Des ressources matérielles adéquates sur le cluster OpenShift pour prendre en charge l'opérateur OpenShift Virtualization et les machines virtuelles qui seront provisionnées. Pour plus de détails sur les exigences en ressources, consultez le "documentation ici".
9. Vous pouvez, si vous le souhaitez, configurer des règles de placement des nœuds pour OpenShift Virtualization afin de spécifier un sous-ensemble de nœuds du cluster pour héberger les opérateurs, les contrôleurs et les machines virtuelles OpenShift Virtualization. Pour obtenir des instructions sur la configuration des règles de placement des nœuds, consultez le "documentation ici".
10. Pour le stockage sous-jacent à OpenShift Virtualization, il est recommandé d'avoir une StorageClass dédiée qui sollicite le stockage auprès d'un backend Trident particulier, lequel est lui-même soutenu par une SVM dédiée. Cela permet de maintenir un niveau de multitenance concernant les données servies pour les charges de travail basées sur des machines virtuelles dans le cluster OpenShift.
11. Une machine virtuelle doit être disponible dans OpenShift Virtualization. Pour plus de détails sur le

déploiement d'une nouvelle machine virtuelle ou la migration d'une machine virtuelle existante vers OpenShift Virtualization, consultez la section appropriée dans la documentation.

Installez NetApp Trident Protect pour la virtualisation OpenShift

Pour activer les fonctionnalités de reprise après sinistre pour les charges de travail de virtualisation OpenShift utilisant NetApp Trident Protect, vous devez avoir Trident Protect installé et configuré sur le cluster OpenShift. Trident Protect peut être installé à l'aide d'un chart Helm.

L'installation de Trident Protect doit être effectuée après l'installation de Trident.

Pour obtenir les instructions d'installation complètes, consultez le "Documentation Trident Protect ici".

Afficher un exemple


```
[root@localhost SnapMirror]#
[root@localhost SnapMirror]# oc get pods -n trident-protect
NAME                                                READY   STATUS    RESTARTS   AGE
autosupportbundle-e9252a48-34a9-4b40-99c2-c00876d962ee-bk2vx   1/1     Running   0          16h
trident-protect-controller-manager-7b76c8b59f-2rmh2            2/2     Running   0          22h
[root@localhost SnapMirror]#
```

Configuration du cluster source pour la reprise après sinistre de Red Hat OpenShift Virtualization

Cette section fournit des informations sur la configuration du cluster source pour la reprise après sinistre des charges de travail de virtualisation OpenShift à l'aide de NetApp Trident Protect et AppMirror. Cela inclut la création d'un AppVault à l'aide d'ONTAP S3, la création d'une application Trident Protect pour la machine virtuelle source, ainsi que la création d'instantanés à la demande et planifiés de la machine virtuelle avec Trident Protect. Ces étapes sont essentielles pour garantir que le cluster source est correctement configuré afin de répliquer les données vers le cluster de destination pour la reprise après sinistre et de permettre la restauration des machines virtuelles en cas de sinistre.

Configurer le cluster source de reprise après sinistre pour la virtualisation OpenShift

Toutes les étapes suivantes sont effectuées sur le cluster source, c'est-à-dire le cluster sur lequel la machine virtuelle protégée est actuellement en cours d'exécution.

Créer AppVault à l’aide de ONTAP S3

Cette section explique comment configurer un objet AppVault dans Trident Protect à l’aide du stockage d’objets ONTAP S3. L’objet AppVault créé à cette étape sera utilisé pour stocker les données répliquées du cluster source, et ces données seront utilisées pour la restauration dans le cluster de destination de reprise après sinistre.

Utilisez les commandes oc et les fichiers yaml ci-dessous pour créer un secret et la ressource personnalisée AppVault pour ONTAP s3. Assurez-vous de les créer dans l’espace de noms trident-protect.

Afficher un exemple

```
apiVersion: v1
# You can provide the keys either as stringData or base 64 encoded data
stringData:
  accessKeyID: "<access key id as obtained from ONTAP>"
  secretAccessKey: "<secret access key as obtained from ONTAP>"
#data:
  #accessKeyID: <base 64 encoded value of access key>
  #secretAccessKey: <base 64 encoded value of secret access key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque
```

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    s3:
      bucketName: oc-dr
      endpoint: <data lif to use to access S3>
      secure: "false" # Setting this to "false" will disable TLS, which
is not recommended for production environments.
      skipCertValidation: "true" # When TLS is enabled, setting
skipCertValidation to "true" will skip TLS certificate validation,
which is not recommended for production environments.
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3
```

Assurez-vous que le coffre-fort ONTAP S3 est créé et qu'il est dans l'état Disponible

```
oc create -f app-vault-secret.yaml -n trident-protect
oc create -f app-vault.yaml -n trident-protect
```

```
[root@00-50-56-b5-2b-9b dr]# oc get appvault -n trident-protect
NAME                STATE       ERROR   MESSAGE   AGE
ontap-s3-appvault   Available                     2d23h
```

Créez une application Trident Protect pour la machine virtuelle source.

Créez une ressource personnalisée Application dans l'espace de noms où se trouve la machine virtuelle source.

Afficher un exemple

```
# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: test-source-app
  namespace: test-dr-ns
spec:
  includedNamespaces:
  - namespace: test-dr-ns
```

```
tridentctl-protect create app <source-vm> -n <source-ns> --namespaces
<source-ns>
```

```
[root@00-50-56-b5-2b-9b dr]# oc get applications.protect.trident.netapp.io -n test-dr-ns
NAME              PROTECTION STATE   AGE
test-source-app   Partial            25h
```

La machine virtuelle et son PVC dans l'espace de noms inclus dans la ressource personnalisée de l'App sont présentés ci-dessous.

```
[root@00-50-56-b5-2b-9b dr]# oc get vm,pods,pvc -n test-dr-ns
NAME                                        AGE   STATUS    READY
virtualmachine.kubevirt.io/test-dr-vm1      25h   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-test-dr-vm1-ns9qq  1/1     Running   0          25h

NAME                                  STATUS   VOLUME                                     CAPACITY     ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/test-dr-vm1     Bound    pvc-43b51d12-ce76-4063-bd59-6e74588ee266   34144990004  RWX            sc-nas         <unset>                 25h
```

Créez un instantané de la machine virtuelle à l'aide de Trident Protect

Vous pouvez créer un instantané à la demande de la machine virtuelle à l'aide de l'interface de ligne de commande (CLI) ou de l'API de Trident Protect. Cet instantané sera stocké dans le AppVault créé à l'étape précédente et pourra être utilisé pour la restauration dans le cluster de destination en cas de reprise après sinistre.

Afficher un exemple

```
# snapshot.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  name: test-source-dr-init-snapshot
  namespace: test-dr-ns
spec:
  applicationRef: test-source-app
  appVaultRef: ontap-s3-appvault
  reclaimPolicy: Delete
```

```
[root@00-50-56-b5-2b-9b dr]# oc get snapshot -n test-dr-ns
NAME                          APP              RECLAIM POLICY   STATE       ERROR   AGE
test-source-dr-init-snapshot  test-source-app   Delete           Completed           25h
```

Créez un instantané planifié de la machine virtuelle à l'aide de Trident Protect

Vous pouvez également créer un instantané planifié en créant une ressource personnalisée Schedule dans le même espace de noms que la ressource personnalisée Application. La planification créera automatiquement des instantanés de la machine virtuelle selon la planification spécifiée et les stockera dans le AppVault.

Afficher un exemple

```
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  name: appmirror-sched1
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: test-source-app
  backupRetention: "0"
  enabled: true
  granularity: Custom
  recurrenceRule: |-
    DTSTART:20240901T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  snapshotRetention: "2"
```

Configuration du cluster de destination pour la reprise après sinistre de Red Hat OpenShift Virtualization

Cette section fournit des informations sur la configuration du cluster de destination pour la reprise après sinistre des charges de travail OpenShift Virtualization à l'aide de NetApp Trident Protect et AppMirror. Cela inclut la création d'un AppVault à l'aide d'ONTAP S3 et la création d'un nouvel espace de noms pour la machine virtuelle de destination. Ces étapes sont essentielles pour garantir que le cluster de destination est correctement configuré pour recevoir les données répliquées du cluster source et permettre la récupération des machines virtuelles en cas de sinistre.

1. Créez un objet AppVault dans le cluster de destination. Cet objet doit pointer vers le même S3 que la source afin qu'il puisse récupérer l'instantané depuis le S3 où le cluster source l'a placé.

Afficher un exemple

```
apiVersion: v1
# You can provide the keys either as stringData or base 64 encoded
data
stringData:
  accessKeyID: "<access key id as obtained from ONTAP>"
  secretAccessKey: "<secret access key as obtained from ONTAP>"
#data:
  #accessKeyID: <base 64 encoded value of access key>
  #secretAccessKey: <base 64 encoded value of secret access key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque
```

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    s3:
      bucketName: oc-dr
      endpoint: <data lif to use to access S3>
      secure: "false" # Setting this to "false" will disable TLS,
which is not recommended for production
      skipCertValidation: "true" # When TLS is enabled, setting
skipCertValidation to "true" will skip TLS certificate validation,
which is not recommended for production environments.
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3
```

```
oc create -f app-vault-secret.yaml -n trident-protect
oc create -f app-vault.yaml -n trident-protect
```

```
[root@00-50-56-b5-01-5b dr]# oc get appvault -A
NAMESPACE          NAME                                STATE       ERROR   MESSAGE   AGE
trident-protect    ontap-s3-appvault                   Available                     29h
```

2. Créez un nouvel espace de noms sur le cluster de destination pour héberger la machine virtuelle basculée. Créez une application sur le cluster de destination qui référence le AppVault créé à l'étape 1 et le nouvel espace de noms. Cette application sera utilisée pour établir la relation AppMirror entre le cluster source et le cluster de destination, et pour gérer la réplication des données du cluster source vers le cluster de destination.

Afficher un exemple

```
# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: test-dest-app
  namespace: test-dr-ns-dest
spec:
  includedNamespaces:
  - namespace: test-dr-ns-dest
```

```
tridentctl-protect create app <dest-app-name> -n <dest-ns>
--namespaces <dest-ns>
```

Basculement d'une machine virtuelle dans OpenShift Virtualization Disaster Recovery

Cette section décrit comment effectuer un basculement d'une machine virtuelle d'un cluster source vers un cluster de destination de reprise après sinistre à l'aide de NetApp Trident Protect et AppMirror. Cette procédure est utile pour tester le processus de basculement et pour effectuer des opérations de maintenance planifiées sur le cluster source. En suivant ces étapes, vous pouvez vous assurer que votre machine virtuelle fonctionne sur le cluster de destination de reprise après sinistre avec toutes les modifications intactes après un événement de reprise après sinistre.

Basculement sans interruption de service pour la OpenShift Virtualization

Cette section décrit comment effectuer un basculement d'une machine virtuelle à partir d'un cluster source sans interruption de service. Ceci est utile pour tester le processus de basculement et pour effectuer une maintenance planifiée sur le cluster source. +

Pour effectuer un basculement sans interruption de service, assurez-vous d'abord que les clusters source et cible sont configurés pour la reprise après sinistre, comme décrit dans les sections précédentes. Ensuite, procédez comme suit :

1. Établissez la relation AppMirror entre le cluster source et le cluster de destination. Lorsque la relation AppMirror est établie, le snapshot le plus récent est transféré vers l'espace de noms de destination. Le PVC est créé pour la machine virtuelle dans l'espace de noms de destination, cependant, le pod de la machine virtuelle n'est pas encore créé dans l'espace de noms de destination.

Afficher un exemple

```
# application-mirror-relationship.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppMirrorRelationship
metadata:
  name: amr1
spec:
  desiredState: Established
  destinationAppVaultRef: ontap-s3-appvault
  destinationApplicationRef: test-dest-app
  namespaceMapping:
  - destination: test-dr-ns-dest
    source: test-dr-ns
  recurrenceRule: |-
    DTSTART:20240901T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  sourceAppVaultRef: ontap-s3-appvault
  sourceApplicationName: test-source-app
  sourceApplicationUID: "<application-uid-of-the-source-app>"
  storageClassName: "sc-nas"
```

```
[root@00-50-56-b5-2b-9b dr]# oc get amr -n test-dr-ns
NAME   DESIRED STATE   STATE          ERROR   AGE
amr1   Established     Establishing           115s
```

```
[root@00-50-56-b5-2b-9b dr]# oc get amr -A
NAMESPACE    NAME   DESIRED STATE   STATE         ERROR   AGE
test-dr-ns   amr1   Established     Established           94s
```

La relation AppMirror doit être créée depuis l'interface de ligne de commande du cluster de destination. Elle doit être créée avec l'état souhaité défini sur Établie. Cela garantira que les données du dernier instantané sont répliquées vers le cluster de destination.

2. Promouvez la relation AppMirror. Modifiez l'état souhaité de la relation à « Promue » pour créer la machine virtuelle dans l'espace de noms de destination. La machine virtuelle continue de s'exécuter dans l'espace de noms source. Les données du dernier instantané sont répliquées vers le cluster de destination et la machine virtuelle est démarrée sur le cluster de destination. Cette méthode vous permet de tester le basculement et de maintenir la disponibilité de la machine virtuelle sans avoir à arrêter l'ensemble du cluster source.

Afficher un exemple

```
oc patch amr amr1 -n test-dr-ns-dest --type=merge -p
'{"spec":{"desiredState":"Promoted"}}'
```

```
[root@00-50-56-b5-01-5b dr]# oc get amr -n test-dr-ns-dest
NAME   DESIRED STATE   STATE      ERROR   AGE
amr2   Promoted        Promoted           25h
```

```
oc get pod, pvc,vm -n test-dr-ns-dest
oc get pod, pvc,vm -n test-dr-ns
```

Restauration d'une machine virtuelle dans la reprise après sinistre de virtualisation OpenShift

Cette section fournit des informations sur le processus de restauration (failback) d'une machine virtuelle (VM) dans le cadre de la reprise après sinistre de OpenShift Virtualization à l'aide de NetApp Trident Protect et AppMirror. Après qu'une opération de basculement a été effectuée vers un cluster de destination de reprise après sinistre, vous pouvez utiliser le processus de restauration pour inverser la direction de la réplication et rétablir le cluster source d'origine en tant que cluster principal pour la VM. Cela implique de resynchroniser toutes les modifications apportées à la VM pendant la période de basculement vers le cluster source d'origine, puis de promouvoir la relation de réplication dans le sens inverse. En suivant ces étapes, vous pouvez vous assurer que votre VM s'exécute sur le cluster source d'origine avec toutes les modifications intactes après un événement de reprise après sinistre.

Retour arrière pour la reprise après sinistre de virtualisation OpenShift

Avec Trident Protect, vous pouvez effectuer un « retour arrière » après une opération de basculement en utilisant la séquence d'opérations suivante. Dans ce workflow pour restaurer la direction de réplication d'origine, Trident Protect réplique (resynchronise) toutes les modifications de l'application vers l'application source d'origine avant d'inverser la direction de la réplication.

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

1. Commencez par un état de basculement échoué.
2. Resynchronisez à l'inverse la relation de réplication

   Lorsque vous effectuez 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.

a. Sur le cluster de destination d'origine, supprimez le CR AppMirrorRelationship. Cela fait en sorte que la destination devienne la source. S'il reste des planifications de protection sur le nouveau cluster de destination, supprimez-les.

Afficher un exemple

```
[root@00-50-56-b5-01-5b dr]# oc delete -f app-mirror-relationship.yaml -n test-dr-ns-dest
appmirrorrelationship.protect.trident.netapp.io "amr2" deleted from test-dr-ns-dest namespace
```

b. Créez un instantané sur le nouveau cluster source (destination d'origine) afin de capturer les modifications apportées pendant la période de basculement. Cela garantit que toutes les modifications sont répliquées sur le cluster source d'origine lors de la resynchronisation.

Afficher un exemple

```
# snapshot.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  name: test-source-dr-init-snapshot-failback
  namespace: test-dr-ns
spec:
  applicationRef: test-dest-app
  appVaultRef: ontap-s3-appvault
  reclaimPolicy: Delete
```

```
[root@00-50-56-b5-01-5b dr]# cat failback-snapshot.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  name: test-source-dr-init-snapshot-failback
  namespace: test-dr-ns-dest
spec:
  applicationRef: test-dest-app
  appVaultRef: ontap-s3-appvault
  reclaimPolicy: Delete
```

```
[root@00-50-56-b5-01-5b dr]# oc get snapshot -n test-dr-ns-dest
NAME                                    APP            RECLAIM POLICY   STATE     ERROR   AGE
test-source-dr-init-snapshot-failback   test-dest-app  Delete           Running           10s
```

```
[root@00-50-56-b5-01-5b dr]# oc get snapshot -n test-dr-ns-dest
NAME                                    APP            RECLAIM POLICY   STATE       ERROR   AGE
test-source-dr-init-snapshot-failback   test-dest-app  Delete           Completed           8m50s
test-source-dr-init-snapshot-failback-2 test-dest-app  Delete           Completed           32s
```

c. Configurez une relation de réplication du nouveau cluster source (destination d'origine) vers le cluster source d'origine, en configurant les valeurs pour la direction inverse.

Afficher un exemple

application-mirror-relationship.yaml

```
apiVersion: protect.trident.netapp.io/v1
kind: AppMirrorRelationship
metadata:
  name: amr1
spec:
  desiredState: Established
  destinationAppVaultRef: ontap-s3-appvault
  destinationApplicationRef: dr-source-vm-failback
  namespaceMapping:
  - destination: test-dr-ns
    source: test-dr-ns-dest
  recurrenceRule: |-
    DTSTART:20240901T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  sourceAppVaultRef: ontap-s3-appvault
  sourceApplicationName: test-dest-app
  sourceApplicationUID: "uid of the app in the original source
cluster"
  storageClassName: "sc-nas"
```

```
[root@00-50-56-b5-2b-9b dr]# oc get amr -n test-dr-ns
NAME   DESIRED STATE   STATE          ERROR   AGE
amr1   Established     Establishing           115s
[root@00-50-56-b5-2b-9b dr]# oc get amr -A
NAMESPACE    NAME   DESIRED STATE   STATE         ERROR   AGE
test-dr-ns   amr1   Established     Established           94s
```

d. Promouvez la relation de réplication du nouveau cluster source (destination d'origine) vers le cluster source d'origine en mettant à jour le champ desiredState dans le CR AppMirrorRelationship sur « Promoted ».

Afficher un exemple

```
[root@00-50-56-b5-2b-9b dr]# oc get vm -n test-dr-ns
No resources found in test-dr-ns namespace.
[root@00-50-56-b5-2b-9b dr]# oc patch amr amr1 -n test-dr-ns --type=merge -p '{"spec":{"desiredState":"Promoted"}}'
appmirrorrelationship.protect.trident.netapp.io/amr1 patched
```

Vous voyez maintenant la machine virtuelle s'exécuter dans le cluster source d'origine. Le processus de restauration est maintenant terminé. Vous pouvez maintenant nettoyer les ressources dans le cluster de destination d'origine. Vous pouvez également configurer une nouvelle relation de réplication si vous souhaitez maintenir les capacités de reprise après sinistre après le processus de restauration.

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

Informations sur le copyright

Informations sur les marques commerciales