Verwenden Sie Astra Control Provisioner

Astra Control Service

NetApp
April 24, 2024

Inhalt

Verwenden Sie Astra Control Provisioner

Konfiguration der Storage-Back-End-Verschlüsselung

Mit Astra Control Provisioner können Sie die Datensicherheit verbessern, indem Sie die Verschlüsselung für den Datenverkehr zwischen dem gemanagten Cluster und dem Storage-Back-End aktivieren.

Astra Control Provisioner unterstützt Kerberos-Verschlüsselung für zwei Arten von Storage-Back-Ends:

- **On-Premises-ONTAP** – Astra Control Provisioner unterstützt Kerberos-Verschlüsselung über NFSv3- und NFSv4-Verbindungen von Red hat OpenShift und Upstream-Kubernetes-Clustern zu On-Premises-ONTAP-Volumes.
- **Azure NetApp Files** – Astra Control Provisioner unterstützt Kerberos-Verschlüsselung über NFSv4.1-Verbindungen von Upstream-Kubernetes-Clustern zu Azure NetApp Files Volumes.

Sie können Snapshots, Klone, schreibgeschütztes Klonen und Importieren von Volumes mit NFS-Verschlüsselung.

Konfiguration der Verschlüsselung von Kerberos während der Übertragung mit lokalen ONTAP Volumes

Sie können die Kerberos-Verschlüsselung für den Storage-Datenverkehr zwischen dem verwalteten Cluster und einem lokalen ONTAP Storage-Back-End aktivieren.

> Kerberos-Verschlüsselung für NFS-Datenverkehr mit On-Premises ONTAP Storage-Back-Ends wird nur mithilfe des unterstützt `ontap-nas` Storage-Treiber:

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie es haben "Astra Control Provisioner wurde aktiviert" Auf dem verwalteten Cluster.
- Stellen Sie sicher, dass Sie Zugriff auf haben `tridentctl` Utility:
- Stellen Sie sicher, dass Sie Administratorzugriff auf das ONTAP Storage Back-End haben.
- Stellen Sie sicher, dass Sie den Namen des Volumes oder der Volumes kennen, die Sie über das ONTAP-Speicher-Back-End freigeben werden.
- Stellen Sie sicher, dass Sie die ONTAP-Storage-VM auf die Unterstützung der Kerberos-Verschlüsselung für NFS-Volumes vorbereitet haben. Siehe "Aktivieren Sie Kerberos auf einer Daten-LIF" Weitere Anweisungen.
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Weitere Informationen finden Sie im Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) des "NetApp Leitfaden zu NFSv4-Verbesserungen und Best Practices".

ONTAP-Exportrichtlinien hinzufügen oder ändern

Sie müssen bestehenden ONTAP-Exportrichtlinien Regeln hinzufügen oder neue Exportrichtlinien erstellen, die Kerberos-Verschlüsselung für das ONTAP Storage-VM-Root-Volume sowie alle mit dem Upstream-Kubernetes-Cluster gemeinsam genutzten ONTAP-Volumes unterstützen. Die von Ihnen hinzugefügten Regeln für die Exportrichtlinie oder neu erstellte Richtlinien für den Export müssen die folgenden Zugriffsprotokolle und

Zugriffsberechtigungen unterstützen:

Zugriffsprotokolle

Konfigurieren Sie die Exportrichtlinie mit NFS-, NFSv3- und NFSv4-Zugriffsprotokollen.

Zugriffsdetails

Sie können eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung konfigurieren, je nach Ihren Anforderungen für das Volume:

- **Kerberos 5** - (Authentifizierung und Verschlüsselung)
- **Kerberos 5i** - (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- **Kerberos 5p** - (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Konfigurieren Sie die ONTAP-Exportrichtlinie mit den entsprechenden Zugriffsberechtigungen. Wenn beispielsweise Cluster die NFS-Volumes mit einer Mischung aus Kerberos 5i- und Kerberos 5p-Verschlüsselung mounten, verwenden Sie die folgenden Zugriffseinstellungen:

Typ	Schreibgeschützter Zugriff	Lese-/Schreibzugriff	Superuser-Zugriff
UNIX	Aktiviert	Aktiviert	Aktiviert
Kerberos 5i	Aktiviert	Aktiviert	Aktiviert
Kerberos 5p	Aktiviert	Aktiviert	Aktiviert

Informationen zum Erstellen von ONTAP Exportrichtlinien und Exportrichtlinienregeln finden Sie in der folgenden Dokumentation:

- "Erstellen Sie eine Exportrichtlinie"
- "Fügen Sie eine Regel zu einer Exportrichtlinie hinzu"

Erstellen eines Storage-Backends

Sie können eine Astra Control Provisioner-Storage-Back-End-Konfiguration erstellen, die Kerberos Verschlüsselungsfunktionen umfasst.

Über diese Aufgabe

Wenn Sie eine Speicher-Back-End-Konfigurationsdatei erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung mithilfe des angeben `spec.nfsMountOptions` Parameter:

- `spec.nfsMountOptions: sec=krb5` (Authentifizierung und Verschlüsselung)
- `spec.nfsMountOptions: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `spec.nfsMountOptions: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Geben Sie nur eine Kerberos-Ebene an. Wenn Sie in der Parameterliste mehr als eine Kerberos-Verschlüsselungsebene angeben, wird nur die erste Option verwendet.

Schritte

1. Erstellen Sie auf dem verwalteten Cluster mithilfe des folgenden Beispiels eine Speicher-Back-End-

Konfigurationsdatei. Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

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

2. Verwenden Sie die Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben, um das Backend zu erstellen:

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

Wenn die Backend-Erstellung fehlschlägt, ist mit der Back-End-Konfiguration ein Fehler aufgetreten. Sie können die Protokolle zur Bestimmung der Ursache anzeigen, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und korrigiert haben, können Sie den Befehl „Erstellen“ erneut ausführen.

Erstellen Sie eine Speicherklasse

Sie können eine Storage-Klasse für die Bereitstellung von Volumes mit Kerberos-Verschlüsselung erstellen.

Über diese Aufgabe

Wenn Sie ein Storage-Klasse-Objekt erstellen, können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung mithilfe des angeben `mountOptions` Parameter:

- `mountOptions: sec=krb5` (Authentifizierung und Verschlüsselung)
- `mountOptions: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `mountOptions: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Geben Sie nur eine Kerberos-Ebene an. Wenn Sie in der Parameterliste mehr als eine Kerberos-Verschlüsselungsebene angeben, wird nur die erste Option verwendet. Wenn die in der Storage-Backend-Konfiguration angegebene Verschlüsselungsebene von der Ebene abweicht, die Sie im Storage-Klasse-Objekt angeben, hat das Storage-Klasse-Objekt Vorrang.

Schritte

1. Erstellen Sie mithilfe des folgenden Beispiels ein StorageClass-Kubernetes-Objekt:

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

2. Speicherklasse erstellen:

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

3. Stellen Sie sicher, dass die Storage-Klasse erstellt wurde:

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

   Sie sollten eine Ausgabe wie die folgende sehen:

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

Bereitstellen von Volumes

Nachdem Sie ein Storage-Back-End und eine Storage-Klasse erstellt haben, können Sie nun ein Volume bereitstellen. Beachten Sie diese Anweisungen für "Bereitstellen eines Volumes".

Konfiguration der Verschlüsselung von Kerberos während der Übertragung mit Azure NetApp Files Volumes

Sie können die Kerberos-Verschlüsselung für den Storage-Datenverkehr zwischen dem gemanagten Cluster und einem einzelnen Azure NetApp Files Storage-Back-End oder einem virtuellen Pool von Azure NetApp Files Storage-Back-Ends aktivieren.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Astra Control Provisioner auf dem verwalteten Red hat OpenShift-Cluster aktiviert haben. Siehe "Astra Control Provisioner Aktivieren" Weitere Anweisungen.
- Stellen Sie sicher, dass Sie Zugriff auf haben `tridentctl` Utility:
- Stellen Sie sicher, dass Sie das Azure NetApp Files-Speicher-Back-End für die Kerberos-Verschlüsselung vorbereitet haben, indem Sie die Anforderungen beachten und die Anweisungen in befolgen "Azure NetApp Files-Dokumentation".
- Stellen Sie sicher, dass alle NFSv4-Volumes, die Sie mit Kerberos-Verschlüsselung verwenden, korrekt konfiguriert sind. Weitere Informationen finden Sie im Abschnitt NetApp NFSv4-Domänenkonfiguration (Seite 13) des "NetApp Leitfaden zu NFSv4-Verbesserungen und Best Practices".

Erstellen eines Storage-Backends

Sie können eine Azure NetApp Files-Storage-Back-End-Konfiguration mit Kerberos Verschlüsselungsfunktionen erstellen.

Über diese Aufgabe

Wenn Sie eine Speicher-Backend-Konfigurationsdatei erstellen, die die Kerberos-Verschlüsselung konfiguriert, können Sie sie so definieren, dass sie auf einer der zwei möglichen Ebenen angewendet werden sollte:

- Die **Speicher-Backend-Ebene** unter Verwendung der `spec.kerberos` Feld
- Die **virtuelle Pool-Ebene** mit dem `spec.storage.kerberos` Feld

Wenn Sie die Konfiguration auf der Ebene des virtuellen Pools definieren, wird der Pool mithilfe der Beschriftung in der Speicherklasse ausgewählt.

Auf beiden Ebenen können Sie eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben:

- `kerberos: sec=krb5` (Authentifizierung und Verschlüsselung)
- `kerberos: sec=krb5i` (Authentifizierung und Verschlüsselung mit Identitätsschutz)
- `kerberos: sec=krb5p` (Authentifizierung und Verschlüsselung mit Identitäts- und Datenschutz)

Schritte

1. Erstellen Sie auf dem verwalteten Cluster eine Speicher-Backend-Konfigurationsdatei mit einem der folgenden Beispiele, je nachdem, wo Sie das Speicher-Back-End definieren müssen (Speicher-Back-End-Ebene oder virtuelle Pool-Ebene). Ersetzen Sie Werte in Klammern <> durch Informationen aus Ihrer Umgebung:

Beispiel auf Storage-Back-End-Ebene

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

Beispiel auf Ebene des virtuellen Pools

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

2. Verwenden Sie die Konfigurationsdatei, die Sie im vorherigen Schritt erstellt haben, um das Backend zu erstellen:

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

Wenn die Backend-Erstellung fehlschlägt, ist mit der Back-End-Konfiguration ein Fehler aufgetreten. Sie können die Protokolle zur Bestimmung der Ursache anzeigen, indem Sie den folgenden Befehl ausführen:

```
tridentctl logs
```

Nachdem Sie das Problem mit der Konfigurationsdatei identifiziert und korrigiert haben, können Sie den Befehl „Erstellen“ erneut ausführen.

Erstellen Sie eine Speicherklasse

Sie können eine Storage-Klasse für die Bereitstellung von Volumes mit Kerberos-Verschlüsselung erstellen.

Schritte

1. Erstellen Sie mithilfe des folgenden Beispiels ein StorageClass-Kubernetes-Objekt:

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

2. Speicherklasse erstellen:

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

3. Stellen Sie sicher, dass die Storage-Klasse erstellt wurde:

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

Sie sollten eine Ausgabe wie die folgende sehen:

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

Bereitstellen von Volumes

Nachdem Sie ein Storage-Back-End und eine Storage-Klasse erstellt haben, können Sie nun ein Volume bereitstellen. Beachten Sie diese Anweisungen für "Bereitstellen eines Volumes".

Wiederherstellen von Volume-Daten mithilfe eines Snapshots

Astra Control Provisioner ermöglicht die schnelle Wiederherstellung von Volumes aus einem Snapshot mithilfe von `TridentActionSnapshotRestore` (TASR) CR. Dieser CR fungiert als eine zwingend notwendige Kubernetes-Aktion und bleibt nach Abschluss des Vorgangs nicht erhalten.

Astra Control Provisioner unterstützt die Wiederherstellung von Snapshots auf dem `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, und `solidfire-san` Treiber.

Bevor Sie beginnen

Sie müssen über einen gebundenen PVC-Snapshot und einen verfügbaren Volume-Snapshot verfügen.

- Vergewissern Sie sich, dass der PVC-Status gebunden ist.

```
kubectl get pvc
```

- Überprüfen Sie, ob der Volume-Snapshot einsatzbereit ist.

```
kubectl get vs
```

Schritte

1. Erstellen Sie den TASR CR. In diesem Beispiel wird ein CR für PVC erstellt `pvc1` Und Volume-Snapshot `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Wenden Sie den CR an, um ihn aus dem Snapshot wiederherzustellen. Dieses Beispiel wird aus einem Snapshot wiederhergestellt `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Ergebnisse

Mit Astra Control Provisioner werden die Daten aus dem Snapshot wiederhergestellt. Sie können den Status der Snapshot-Wiederherstellung überprüfen.

```
kubectl get tasr -o yaml

apiVersion: v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```

- In den meisten Fällen versucht die Astra Control Provisioner bei einem Ausfall nicht automatisch einen weiteren Vorgang auszuführen. Sie müssen den Vorgang erneut ausführen.
- Kubernetes-Benutzer ohne Administratorzugriff müssen möglicherweise vom Administrator zum Erstellen eines TASR CR in ihrem Applikations-Namespace erhalten.

Replizieren Sie Volumes mit SnapMirror

Mit Astra Control Provisioner können Sie Spiegelungsbeziehungen zwischen einem Quell-Volume auf einem Cluster und dem Ziel-Volume auf dem Peering-Cluster erstellen,

um Daten für die Disaster Recovery zu replizieren. Sie können eine benutzerdefinierte Ressourcendefinition (CRD, Namested Custom Resource Definition) verwenden, um die folgenden Vorgänge auszuführen:

- Erstellen von Spiegelbeziehungen zwischen Volumes (VES)
- Entfernen Sie Spiegelungsbeziehungen zwischen Volumes
- Brechen Sie die Spiegelbeziehungen auf
- Bewerben des sekundären Volumes bei Ausfällen (Failover)
- Verlustfreie Transition von Applikationen von Cluster zu Cluster (während geplanter Failover oder Migrationen)

Replikationsvoraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie beginnen:

ONTAP Cluster

- **Astra Control Provisioner**: Astra Control Provisioner Version 23.10 oder höher muss sowohl auf den Quell- als auch auf den Ziel-Kubernetes-Clustern vorhanden sein, die ONTAP als Backend verwenden.
- **Lizenzen**: Asynchrone Lizenzen von ONTAP SnapMirror, die das Datensicherungspaket verwenden, müssen sowohl auf den Quell- als auch auf den Ziel-ONTAP-Clustern aktiviert sein. Siehe "Übersicht über die SnapMirror Lizenzierung in ONTAP" Finden Sie weitere Informationen.

Peering

- **Cluster und SVM**: Die ONTAP Speicher-Back-Ends müssen aktiviert werden. Siehe "Übersicht über Cluster- und SVM-Peering" Finden Sie weitere Informationen.

> Vergewissern Sie sich, dass die in der Replizierungsbeziehung zwischen zwei ONTAP-Clustern verwendeten SVM-Namen eindeutig sind.

- **Astra Control Provisioner und SVM**: Die Peering von Remote-SVMs müssen für die Astra Control Bereitstellung im Ziel-Cluster verfügbar sein.

Unterstützte Treiber

- Die Volume-Replizierung wird von ontap-nas und ontap-san Treibern unterstützt.

Erstellen Sie eine gespiegelte PVC

Führen Sie die folgenden Schritte aus, und verwenden Sie die CRD-Beispiele, um eine Spiegelungsbeziehung zwischen primären und sekundären Volumes zu erstellen.

Schritte

1. Führen Sie auf dem primären Kubernetes-Cluster die folgenden Schritte aus:
   a. Erstellen Sie ein StorageClass-Objekt mit dem `trident.netapp.io/replication: true` Parameter.

Beispiel

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  fsType: "nfs"
  trident.netapp.io/replication: "true"
```

b. PVC mit zuvor erstellter StorageClass erstellen.

Beispiel

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Erstellen Sie eine MirrorRelation CR mit lokalen Informationen.

Beispiel

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

Astra Control Provisioner ruft die internen Informationen für das Volume und den aktuellen DP-Status des Volumes ab und füllt dann das Statusfeld der MirrorRelationship aus.

d. Holen Sie sich den TridentMirrorRelationship CR, um den internen Namen und die SVM der PVC zu erhalten.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Führen Sie auf dem sekundären Kubernetes-Cluster die folgenden Schritte aus:
   a. Erstellen Sie eine StorageClass mit dem Parameter trident.netapp.io/replication: true.

      Beispiel

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        trident.netapp.io/replication: true
      ```

   b. Erstellen Sie eine MirrorRelationship-CR mit Ziel- und Quellinformationen.

Beispiel

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: established
  volumeMappings:
  - localPVCName: csi-nas
    remoteVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
```

Astra Control Provisioner erstellt eine SnapMirror Beziehung zum Namen der konfigurierten Beziehungsrichtlinie (oder dem Standard für ONTAP) und initialisiert sie.

c. PVC mit zuvor erstellter StorageClass erstellen, um als sekundäres Ziel zu fungieren (SnapMirror Ziel).

Beispiel

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
  - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

Astra Control Provisioner überprüft die CRD für die TridentMirrorRelationship und erstellt das Volume nicht, wenn die Beziehung nicht vorhanden ist. Falls die Beziehung besteht, stellt Astra Control Provisioner sicher, dass das neue FlexVol Volume auf eine SVM platziert wird, die mit der in MirrorRelation definierten Remote SVM verbunden ist.

Volume-Replikationsstatus

Eine Trident Mirror-Beziehung (TMR) ist eine CRD, die ein Ende einer Replizierungsbeziehung zwischen PVCs darstellt. Das Ziel-TMR verfügt über einen Status, der Astra Control Provisioner über den gewünschten Status informiert. Das Ziel-TMR hat die folgenden Zustände:

- **Etabliert**: Die lokale PVC ist das Zielvolumen einer Spiegelbeziehung, und das ist eine neue Beziehung.
- **Befördert**: Die lokale PVC ist ReadWrite und montierbar, ohne dass aktuell eine Spiegelbeziehung besteht.

- **Wiederhergestellt**: Die lokale PVC ist das Zielvolumen einer Spiegelbeziehung und war zuvor auch in dieser Spiegelbeziehung.
  - Der neu eingerichtete Status muss verwendet werden, wenn das Ziel-Volume jemals in einer Beziehung zum Quell-Volume stand, da es den Inhalt des Ziel-Volume überschreibt.
  - Der neu eingerichtete Status schlägt fehl, wenn das Volume zuvor nicht in einer Beziehung zur Quelle stand.

Fördern Sie die sekundäre PVC während eines ungeplanten Failover

Führen Sie den folgenden Schritt auf dem sekundären Kubernetes-Cluster aus:

- Aktualisieren Sie das Feld *spec.State* von TridentMirrorRelationship auf `promoted`.

Fördern Sie die sekundäre PVC während eines geplanten Failover

Führen Sie während eines geplanten Failover (Migration) die folgenden Schritte durch, um die sekundäre PVC hochzustufen:

Schritte

1. Erstellen Sie auf dem primären Kubernetes-Cluster einen Snapshot der PVC und warten Sie, bis der Snapshot erstellt wurde.
2. Erstellen Sie auf dem primären Kubernetes-Cluster SnapshotInfo CR, um interne Details zu erhalten.

   Beispiel

   ```
   kind: SnapshotInfo
   apiVersion: trident.netapp.io/v1
   metadata:
     name: csi-nas
   spec:
     snapshot-name: csi-nas-snapshot
   ```

3. Aktualisieren Sie im sekundären Kubernetes-Cluster das Feld *spec.State* des *tridentMirrorRelationship* CR auf *promoted* und *spec.promotedSnapshotHandle* als InternalName des Snapshots.
4. Bestätigen Sie auf sekundärem Kubernetes-Cluster den Status (Feld Status.State) von TridentMirrorRelationship auf hochgestuft.

Stellen Sie nach einem Failover eine gespiegelte Beziehung wieder her

Wählen Sie vor dem Wiederherstellen einer Spiegelbeziehung die Seite aus, die Sie als neuen primären festlegen möchten.

Schritte

1. Stellen Sie auf dem sekundären Kubernetes-Cluster sicher, dass die Werte für das Feld *spec.remoteVolumeHandle* auf dem TridentMirrorRelationship aktualisiert werden.
2. Aktualisieren Sie im sekundären Kubernetes-Cluster das Feld *spec.mirror* von TridentMirrorRelationship auf `reestablished`.

Zusätzliche Vorgänge

Astra Control Provisioner unterstützt die folgenden Vorgänge für primäre und sekundäre Volumes:

Replizieren der primären PVC auf eine neue sekundäre PVC

Stellen Sie sicher, dass Sie bereits über eine primäre PVC und eine sekundäre PVC verfügen.

Schritte

1. Löschen Sie die CRDs PersistentVolumeClaim und TridentMirrorRelationship aus dem eingerichteten sekundären Cluster (Ziel).
2. Löschen Sie die CRD für TridentMirrorRelationship aus dem primären (Quell-) Cluster.
3. Erstellen Sie eine neue TRIdentMirrorRelationship CRD auf dem primären (Quell-) Cluster für die neue sekundäre (Ziel-) PVC, die Sie einrichten möchten.

Ändern der Größe einer gespiegelten, primären oder sekundären PVC

Die PVC-Größe kann wie gewohnt geändert werden. ONTAP erweitert automatisch alle Zielflvxole, wenn die Datenmenge die aktuelle Größe überschreitet.

Entfernen Sie die Replikation aus einer PVC

Um die Replikation zu entfernen, führen Sie einen der folgenden Vorgänge auf dem aktuellen sekundären Volume aus:

- Löschen Sie MirrorRelation auf der sekundären PVC. Dadurch wird die Replikationsbeziehung unterbrochen.
- Oder aktualisieren Sie das Feld spec.State auf *promoted*.

Löschen einer PVC (die zuvor gespiegelt wurde)

Astra Control Provisioner überprüft nach replizierten PVCs und gibt die Replizierungsbeziehung frei, bevor versucht wird, das Volume zu löschen.

Löschen eines TMR

Das Löschen eines TMR auf einer Seite einer gespiegelten Beziehung führt dazu, dass der verbleibende TMR in den Status *promoted* übergeht, bevor Astra Control Provisioner den Löschvorgang abgeschlossen hat. Wenn der für den Löschvorgang ausgewählte TMR bereits den Status *promoted* hat, gibt es keine bestehende Spiegelbeziehung und der TMR wird entfernt und Astra Control Provisioner wird die lokale PVC auf *ReadWrite* hochstufen. Durch dieses Löschen werden SnapMirror Metadaten für das lokale Volume in ONTAP freigegeben. Wenn dieses Volume in Zukunft in einer Spiegelbeziehung verwendet wird, muss es beim Erstellen der neuen Spiegelbeziehung ein neues TMR mit einem *established* Volume-Replikationsstatus verwenden.

Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP online ist

Spiegelbeziehungen können jederzeit nach ihrer Einrichtung aktualisiert werden. Sie können das verwenden `state: promoted` Oder `state: reestablished` Felder zum Aktualisieren der Beziehungen.
Wenn Sie ein Zielvolume auf ein reguläres ReadWrite-Volume heraufstufen, können Sie *promotedSnapshotHandle* verwenden, um einen bestimmten Snapshot anzugeben, auf dem das aktuelle Volume wiederhergestellt werden soll.

Aktualisieren Sie Spiegelbeziehungen, wenn ONTAP offline ist

Sie können ein CRD verwenden, um ein SnapMirror Update durchzuführen, ohne dass Astra Control direkt mit dem ONTAP Cluster verbunden ist. Im folgenden Beispielformat finden Sie das TridentActionMirrorUpdate:

Beispiel

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Gibt den Status von TridentActionMirrorUpdate CRD wieder. Es kann einen Wert von *suileded*, *in progress* oder *failed* annehmen.