Sicherheit

Astra Trident

NetApp
January 14, 2026

Inhalt

Sicherheit

Sicherheit

Stellen Sie mit den hier aufgeführten Empfehlungen sicher, dass Ihre Astra Trident Installation sicher ist.

Führen Sie Astra Trident in einem eigenen Namespace aus

Es ist wichtig, dass Applikationen, Applikationsadministratoren, Benutzer und Managementapplikationen auf die Objektdefinitionen von Astra Trident oder die Pods zugreifen können, um zuverlässigen Storage sicherzustellen und potenzielle schädliche Aktivitäten zu blockieren.

Zur Trennung der anderen Applikationen und Benutzer von Astra Trident muss immer Astra Trident in einem eigenen Kubernetes Namespace installiert werden (`trident`). Wenn Astra Trident in einem eigenen Namespace bereitgestellt wird, wird sichergestellt, dass nur die Administratoren von Kubernetes auf den Astra Trident Pod und die Artefakte (z. B. Backend und CHAP-Schlüssel, falls zutreffend) zugreifen können, die in den namenweisen CRD-Objekten gespeichert sind.
Sie sollten sicherstellen, dass nur Administratoren Zugriff auf den Astra Trident Namespace und damit auf das haben `tridentctl` Applikation.

Verwenden Sie CHAP-Authentifizierung mit ONTAP SAN Back-Ends

Astra Trident unterstützt die CHAP-basierte Authentifizierung für ONTAP-SAN-Workloads (mithilfe von `ontap-san` Und `ontap-san-economy` Treiber). NetApp empfiehlt die Verwendung von bidirektionalem CHAP mit Astra Trident zur Authentifizierung zwischen einem Host und dem Storage-Backend.

Bei ONTAP-Back-Ends, die die SAN-Storage-Treiber verwenden, kann Astra Trident bidirektionales CHAP einrichten und CHAP-Benutzernamen und -Schlüssel über managen `tridentctl`.
Siehe "" Um zu erfahren, wie Astra Trident CHAP auf ONTAP Back-Ends konfiguriert.

Verwenden Sie CHAP-Authentifizierung mit NetApp HCI und SolidFire Back-Ends

NetApp empfiehlt die Implementierung von bidirektionalem CHAP, um die Authentifizierung zwischen einem Host und den NetApp HCI und SolidFire Back-Ends zu gewährleisten. Astra Trident verwendet ein geheimes Objekt mit zwei CHAP-Passwörtern pro Mandant. Wenn Astra Trident installiert ist, managt es die CHAP-Schlüssel und speichert sie in einem `tridentvolume` CR-Objekt für das jeweilige PV. Bei der Erstellung eines PV verwendet Astra Trident die CHAP-Schlüssel, um eine iSCSI-Sitzung zu initiieren und mit dem NetApp HCI- und dem SolidFire-System über CHAP zu kommunizieren.

Die von Astra Trident erstellten Volumes sind keiner Volume Access Group zugeordnet.

Nutzen Sie Astra Trident mit NVE und NAE

NetApp ONTAP bietet Verschlüsselung ruhender Daten zum Schutz sensibler Daten, wenn eine Festplatte gestohlen, zurückgegeben oder einer neuen Verwendung zugewiesen wird. Weitere Informationen finden Sie unter "NetApp Volume Encryption Übersicht konfigurieren".

- Wenn NAE auf dem Backend aktiviert ist, wird jedes im Astra Trident bereitgestellte Volume NAE-aktiviert.
- Wenn NAE im Backend nicht aktiviert ist, wird jedes in Astra Trident bereitgestellte Volume mit NVE

aktiviert, es sei denn, Sie setzen das NVE-Verschlüsselungsflag auf `false` Bei der Back-End-Konfiguration:

> Volumes, die in Astra Trident auf einem NAE-fähigen Back-End erstellt werden, müssen NVE oder NAE-verschlüsselt sein.
>
> - Sie können das NVE-Verschlüsselungsflag auf einstellen `true` In der Trident-Back-End-Konfiguration können Sie die NAE-Verschlüsselung außer Kraft setzen und für jedes Volume einen bestimmten Verschlüsselungsschlüssel verwenden.
> - Setzen des NVE-Verschlüsselungsfahne auf `false` Auf einem NAE-fähigen Back-End wird ein NAE-fähiges Volume erstellt. Sie können die NAE-Verschlüsselung nicht deaktivieren, indem Sie das NVE-Verschlüsselungsfahne auf setzen `false`.

- Sie können in Astra Trident manuell ein NVE-Volume erstellen, indem Sie explizit das NVE-Verschlüsselungsflag auf festlegen `true`.

Weitere Informationen zu Back-End-Konfigurationsoptionen finden Sie unter:

- "ONTAP SAN-Konfigurationsoptionen"
- "NAS-Konfigurationsoptionen von ONTAP"

Linux Unified Key Setup (LUKS)

Sie können Linux Unified Key Setup (LUKS) aktivieren, um ONTAP SAN und ONTAP SAN ECONOMY Volumes auf Astra Trident zu verschlüsseln. Astra Trident unterstützt die Rotation von Passphrase und die Volume-Erweiterung für LUKS-verschlüsselte Volumes.

In Astra Trident verwenden LUKS-verschlüsselte Volumen den aes-xts-plain64 Zypher und den Modus, wie von empfohlen "NIST".

Bevor Sie beginnen

- Worker Nodes müssen cryptsetup 2.1 oder höher (aber unter 3.0) installiert sein. Weitere Informationen finden Sie unter "Gitlab: Cryptsetup".
- Aus Performance-Gründen wird empfohlen, dass Arbeiterknoten Advanced Encryption Standard New Instructions (AES-NI) unterstützen. Führen Sie den folgenden Befehl aus, um die Unterstützung von AES-NI zu überprüfen:

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

Wenn nichts zurückgegeben wird, unterstützt Ihr Prozessor nicht AES-NI. Weitere Informationen zu AES-NI finden Sie unter: "Intel: Advanced Encryption Standard Instructions (AES-NI)".

Aktivieren Sie die LUKS-Verschlüsselung

Sie können die Verschlüsselung auf Host-Seite pro Volume mithilfe von Linux Unified Key Setup (LUKS) für ONTAP SAN und ONTAP SAN ECONOMY Volumes aktivieren.

Schritte

1. Definieren Sie LUKS-Verschlüsselungsattribute in der Backend-Konfiguration. Weitere Informationen zu den Back-End-Konfigurationsoptionen für ONTAP SAN finden Sie unter "ONTAP SAN-Konfigurationsoptionen".

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

2. Nutzung `parameters.selector` So definieren Sie die Speicherpools mit LUKS-Verschlüsselung. Beispiel:

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

3. Erstellen Sie ein Geheimnis, das die LUKS-Passphrase enthält. Beispiel:

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

Einschränkungen

LUKS-verschlüsselte Volumes können die ONTAP Deduplizierung und Komprimierung nicht nutzen.

Back-End-Konfiguration zum Importieren von LUKS-Volumes

Um ein LUKS-Volume zu importieren, müssen Sie festlegen `luksEncryption` Bis(`true` Am Backend. Der `luksEncryption` Die Option teilt Astra Trident mit, ob das Volume LUKS-konform ist (`true`) Oder nicht LUKS-konform (`false`) Wie im folgenden Beispiel gezeigt.

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

Eine LUKS-Passphrase drehen

Sie können die LUKS-Passphrase drehen und die Drehung bestätigen.

> Vergessen Sie keine Passphrase, bis Sie überprüft haben, dass sie nicht mehr von einem Volume, einem Snapshot oder einem geheimen Schlüssel referenziert wird. Wenn eine referenzierte Passphrase verloren geht, können Sie das Volume möglicherweise nicht mounten und die Daten bleiben verschlüsselt und unzugänglich.

Über diese Aufgabe

DIE Drehung der LUKS-Passphrase erfolgt, wenn ein Pod, das das Volume bindet, nach der Angabe einer neuen LUKS-Passphrase erstellt wird. Bei der Erstellung eines neuen Pods vergleicht Astra Trident die LUKS-Passphrase auf dem Volume mit der aktiven Passphrase im Geheimnis.

- Wenn die Passphrase auf dem Volume nicht mit der aktiven Passphrase im Geheimnis übereinstimmt, erfolgt die Drehung.
- Wenn die Passphrase auf dem Volume mit der aktiven Passphrase im Geheimnis übereinstimmt, wird das angezeigt `previous-luks-passphrase` Parameter wird ignoriert.

Schritte

1. Fügen Sie die hinzu `node-publish-secret-name` Und `node-publish-secret-namespace` StorageClass-Parameter. Beispiel:

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

2. Identifizieren Sie vorhandene Passphrases auf dem Volume oder Snapshot.

Datenmenge

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

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

Snapshot

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

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

3. Aktualisieren Sie das LUKS-Geheimnis für das Volume, um die neuen und vorherigen Passphrases anzugeben. Unbedingt `previous-luke-passphrase-name` Und `previous-luks-passphrase` Übereinstimmung mit der vorherigen Passphrase.

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

4. Erstellen Sie einen neuen Pod, der das Volume montiert. Dies ist erforderlich, um die Rotation zu initiieren.
5. Überprüfen Sie, ob die Passphrase gedreht wurde.

Datenmenge

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

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

Snapshot

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

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

Ergebnisse

Die Passphrase wurde gedreht, wenn nur die neue Passphrase auf dem Volume und dem Snapshot zurückgegeben wird.

> Werden beispielsweise zwei Passphrases zurückgegeben `luksPassphraseNames: ["B", "A"]`, Die Rotation ist unvollständig. Sie können einen neuen Pod auslösen, um zu versuchen, die Rotation abzuschließen.

Aktivieren Sie die Volume-Erweiterung

Sie können Volume-Erweiterung auf einem LUKS-verschlüsselten Volume aktivieren.

Schritte

1. Aktivieren Sie die `CSINodeExpandSecret` Funktionstor (Beta 1.25+). Siehe "Kubernetes 1.25: Verwenden Sie Secrets zur Node-gesteuerten Erweiterung von CSI Volumes" Entsprechende Details.
2. Fügen Sie die hinzu `node-expand-secret-name` Und `node-expand-secret-namespace` StorageClass-Parameter. Beispiel:

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

Ergebnisse

Wenn Sie die Online-Speichererweiterung initiieren, gibt das Kubelet die entsprechenden Zugangsdaten an den Treiber weiter.

Konfiguration der Verschlüsselung von Kerberos während der Übertragung

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 über NFSv3- und NFSv4-Verbindungen von Red hat OpenShift und Upstream-Kubernetes-Clustern zu lokalen ONTAP 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 Storage-Treibers unterstützt `ontap-nas` .

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie sich "Astra Control Provisioner wurde aktiviert" auf dem verwalteten Cluster befinden.
- Stellen Sie sicher, dass Sie Zugriff auf das Dienstprogramm haben `tridentctl` .
- 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. Anweisungen hierzu finden Sie unter "Aktivieren Sie Kerberos auf einer Daten-LIF" .
- 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) der "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 Parameters angeben `spec.nfsMountOptions`:

- `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 mit dem Parameter eine von drei verschiedenen Versionen der Kerberos-Verschlüsselung angeben `mountOptions` :

- `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. Anweisungen hierzu finden Sie unter "Astra Control Provisioner Aktivieren" .
- Stellen Sie sicher, dass Sie Zugriff auf das Dienstprogramm haben `tridentctl` .
- 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) der "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** mit dem `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

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

Beispiel auf Ebene des virtuellen Pools

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

2. 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: 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-sc-nfs.yaml
```

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

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

Sie sollten eine Ausgabe wie die folgende sehen:

```
NAME          PROVISIONER             AGE
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".