Sécurité

Trident

NetApp
July 01, 2026

Sommaire

Sécurité

Sécurité

Utilisez les recommandations listées ici pour garantir que votre installation Trident est sécurisée.

Exécutez Trident dans son propre espace de noms

Il est important d'empêcher les applications, les administrateurs d'applications, les utilisateurs et les applications de gestion d'accéder aux définitions d'objets Trident ou aux pods afin de garantir un stockage fiable et de bloquer toute activité malveillante potentielle.

Pour séparer les autres applications et utilisateurs de Trident, installez toujours Trident dans son propre espace de noms Kubernetes (`trident`). Mettre Trident dans son propre espace de noms garantit que seul le personnel administratif de Kubernetes a accès au pod Trident et aux artefacts (tels que les secrets backend et CHAP, le cas échéant) stockés dans les objets CRD de l'espace de noms. Vous devez vous assurer que seuls les administrateurs ont accès à l'espace de noms Trident et donc à l'application `tridentctl`.

Utilisez l'authentification CHAP avec les backends SAN ONTAP

Trident prend en charge l'authentification CHAP pour les charges de travail ONTAP SAN (à l'aide des pilotes `ontap-san` et `ontap-san-economy`). NetApp recommande d'utiliser l'authentification CHAP bidirectionnelle avec Trident pour l'authentification entre un hôte et le système de stockage.

Pour les backends ONTAP qui utilisent les pilotes de stockage SAN, Trident peut configurer le CHAP bidirectionnel et gérer les noms d'utilisateur et les secrets CHAP via `tridentctl`. Reportez-vous à "Préparez-vous à configurer le backend avec les pilotes SAN ONTAP" pour comprendre comment Trident configure CHAP sur les backends ONTAP.

Utilisez l'authentification CHAP avec NetApp HCI et SolidFire backends

NetApp recommande de déployer CHAP bidirectionnel pour garantir l'authentification entre un hôte et les backends NetApp HCI et SolidFire. Trident utilise un objet secret qui inclut deux mots de passe CHAP par locataire. Lorsque Trident est installé, il gère les secrets CHAP et les stocke dans un objet CR `tridentvolume` pour le PV respectif. Lorsque vous créez un PV, Trident utilise les secrets CHAP pour initier une session iSCSI et communiquer avec le système NetApp HCI et SolidFire via CHAP.

Les volumes créés par Trident ne sont associés à aucun Volume Access Group.

Utilisez Trident avec NVE et NAE

NetApp ONTAP assure le chiffrement des données au repos afin de protéger les données sensibles en cas de vol, de retour ou de réutilisation d'un disque. Pour plus de détails, consultez "Configurer l'aperçu du chiffrement des volumes NetApp".

- Si NAE est activé sur le backend, tout volume provisionné dans Trident sera activé NAE.
  - Vous pouvez définir le indicateur de chiffrement NVE sur `""` pour créer des volumes compatibles NAE.
- Si NAE n'est pas activé sur le backend, tout volume provisionné dans Trident sera activé NVE à moins que l'indicateur de chiffrement NVE ne soit défini sur `false` (la valeur par défaut) dans la configuration du

backend.

> Les volumes créés dans Trident sur un backend activé NAE doivent être chiffrés NVE ou NAE.
>
> - Vous pouvez définir le indicateur de chiffrement NVE sur `true` dans la configuration du backend Trident pour remplacer le chiffrement NAE et utiliser une clé de chiffrement spécifique pour chaque volume.
> - Définir le drapeau de chiffrement NVE sur `false` sur un backend activé NAE crée un volume activé NAE. Vous ne pouvez pas désactiver le chiffrement NAE en définissant le drapeau de chiffrement NVE sur `false`.

- Vous pouvez créer manuellement un volume NVE dans Trident en définissant explicitement le indicateur de chiffrement NVE sur `true`.

Pour plus d'informations sur les options de configuration du backend, consultez :

- "Options de configuration SAN ONTAP"
- "Options de configuration NAS ONTAP"

Linux Unified Key Setup (LUKS)

Vous pouvez activer Linux Unified Key Setup (LUKS) pour chiffrer les volumes ONTAP SAN et ONTAP SAN ECONOMY sur Trident. Trident prend en charge la rotation des phrases de passe et l'extension de volume pour les volumes chiffrés avec LUKS.

Dans Trident, les volumes chiffrés LUKS utilisent le cypher et le mode aes-xts-plain64, comme recommandé par "NIST".

> Le chiffrement LUKS n'est pas pris en charge pour les systèmes ASA r2. Pour des informations sur les systèmes ASA r2, voir "En savoir plus sur les systèmes de stockage ASA r2".

Avant de commencer

- Les nœuds de travail doivent avoir cryptsetup 2.1 ou une version supérieure (mais inférieure à 3.0) installée. Pour plus d'informations, consultez "Gitlab : cryptsetup".
- Pour des raisons de performance, NetApp recommande que les nœuds de travail prennent en charge Advanced Encryption Standard New Instructions (AES-NI). Pour vérifier la prise en charge d'AES-NI, exécutez la commande suivante :

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

Si aucune réponse n'est renvoyée, votre processeur ne prend pas en charge AES-NI. Pour plus d'informations sur AES-NI, visitez : "Intel: Instructions Advanced Encryption Standard (AES-NI)".

Activer le chiffrement LUKS

Vous pouvez activer le chiffrement par volume, côté hôte, à l'aide de Linux Unified Key Setup (LUKS) pour les volumes ONTAP SAN et ONTAP SAN ECONOMY.

Étapes

1. Définissez les attributs de chiffrement LUKS dans la configuration du backend. Pour plus d'informations sur les options de configuration du backend pour ONTAP SAN, consultez "Options de configuration SAN ONTAP".

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

2. Utilisez `parameters.selector` pour définir les pools de stockage utilisant le chiffrement LUKS. Par exemple :

```
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. Créez un secret qui contient la phrase de passe LUKS. Par exemple :

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

Limitations

Les volumes chiffrés LUKS ne peuvent pas bénéficier de la déduplication et de la compression ONTAP.

Configuration du backend pour l'importation des volumes LUKS

Pour importer un volume LUKS, vous devez définir `luksEncryption` sur (`true` dans le backend. L' `luksEncryption`option indique à Trident si le volume est conforme LUKS (`true`) ou non conforme LUKS (`false`), comme illustré dans l'exemple suivant.

```
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'
```

Configuration PVC pour l'importation de volumes LUKS

Pour importer dynamiquement des volumes LUKS, définissez l'annotation `trident.netapp.io/luksEncryption` sur `true` et incluez une classe de stockage compatible LUKS dans le PVC comme indiqué dans cet exemple.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: luks-pvc
  namespace: trident
  annotations:
    trident.netapp.io/luksEncryption: "true"
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: luks-sc
```

Faire pivoter une phrase de passe LUKS

Vous pouvez faire pivoter la phrase de passe LUKS et confirmer la rotation.

> N'oubliez pas votre phrase de passe tant que vous n'avez pas vérifié qu'elle n'est plus utilisée par aucun volume, instantané ou secret. Si une phrase de passe référencée est perdue, vous pourriez être dans l'incapacité de monter le volume et les données resteront chiffrées et inaccessibles.

À propos de cette tâche

La rotation de la phrase de passe LUKS a lieu lorsqu'un pod qui monte le volume est créé après la spécification d'une nouvelle phrase de passe LUKS. Lorsqu'un nouveau pod est créé, Trident compare la phrase de passe LUKS du volume à la phrase de passe active dans le secret.

- Si la phrase de passe sur le volume ne correspond pas à la phrase de passe active dans le secret, une rotation a lieu.
- Si la phrase de passe du volume correspond à la phrase de passe active du secret, le `previous-luks-passphrase` paramètre est ignoré.

Étapes

1. Ajoutez les `node-publish-secret-name` et `node-publish-secret-namespace` paramètres StorageClass. Par exemple :

```
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. Identifiez les phrases de passe existantes sur le volume ou le snapshot.

Volume

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

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

Instantané

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

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

3. Mettez à jour le secret LUKS du volume en spécifiant la nouvelle et l'ancienne phrase de passe. Assurez-vous que `previous-luke-passphrase-name` et `previous-luks-passphrase` correspondent à la phrase de passe précédente.

```
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. Créez un nouveau pod en montant le volume. Ceci est nécessaire pour initier la rotation.
5. Vérifiez que la phrase de passe a été modifiée.

Volume

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

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

Instantané

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

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

Résultats

La phrase de passe a été renouvelée lorsque seule la nouvelle phrase de passe est renvoyée sur le volume et l'instantané.

> Si deux phrases de passe sont renvoyées, par exemple `luksPassphraseNames: ["B", "A"]`, la rotation est incomplète. Vous pouvez déclencher un nouveau pod pour tenter de terminer la rotation.

Activer l'expansion du volume

Vous pouvez activer l'extension de volume sur un volume chiffré LUKS.

Étapes

1. Activez la `CSINodeExpandSecret` feature gate (bêta 1.25+). Consultez "Kubernetes 1.25 : Utilisez des secrets pour l'extension des volumes CSI pilotée par les nœuds" pour plus de détails.
2. Ajoutez les `node-expand-secret-name` et `node-expand-secret-namespace` paramètres StorageClass. Par exemple :

```
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
```

Résultats

Lorsque vous lancez une extension de stockage en ligne, le kubelet transmet les informations d'identification appropriées au driver.

Chiffrement Kerberos en vol

En utilisant le chiffrement Kerberos in-flight, vous pouvez améliorer la sécurité d'accès aux données en activant le chiffrement pour le trafic entre votre cluster géré et le stockage backend.

Trident prend en charge le chiffrement Kerberos pour ONTAP en tant que backend de stockage :

- **On-premise ONTAP** - Trident prend en charge le chiffrement Kerberos sur les connexions NFSv3 et NFSv4 depuis Red Hat OpenShift et les clusters Kubernetes en amont vers les volumes ONTAP sur site.

Vous pouvez créer, supprimer, redimensionner, prendre un instantané, cloner, cloner en lecture seule et importer des volumes qui utilisent le chiffrement NFS.

Configurer le chiffrement Kerberos en transit avec les volumes ONTAP sur site

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un système de stockage ONTAP sur site.

Le chiffrement Kerberos pour le trafic NFS avec des backends de stockage ONTAP sur site n'est pris en charge qu'à l'aide du `ontap-nas` storage driver.

Avant de commencer

- Assurez-vous d'avoir accès à l' `tridentctl`utilitaire.
- Assurez-vous de disposer d'un accès administrateur au système de stockage ONTAP.
- Assurez-vous de connaître le nom du ou des volumes que vous partagerez depuis le stockage backend ONTAP.
- Assurez-vous d'avoir préparé la machine virtuelle de stockage ONTAP pour prendre en charge le chiffrement Kerberos pour les volumes NFS. Consultez "Activer Kerberos sur une dataLIF" pour obtenir des instructions.
- Assurez-vous que tous les volumes NFSv4 que vous utilisez avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section « Configuration du domaine NFSv4 » (page 13) de NetApp "NetApp NFSv4 : améliorations et guide des bonnes pratiques".

Ajouter ou modifier les règles d'export ONTAP

Vous devez ajouter des règles aux règles d'export ONTAP existantes ou créer de nouvelles règles d'export prenant en charge le chiffrement Kerberos pour le volume racine de la machine virtuelle de stockage ONTAP, ainsi que pour tous les volumes ONTAP partagés avec le cluster Kubernetes en amont. Les règles d'export que vous ajoutez, ou les nouvelles règles d'export que vous créez, doivent prendre en charge les protocoles d'accès et les autorisations d'accès suivants :

Protocoles d'accès

Configurez la règle d'export avec les protocoles d'accès NFS, NFSv3 et NFSv4.

Détails d'accès

Vous pouvez configurer l'une des trois versions différentes du chiffrement Kerberos, en fonction de vos besoins pour le volume :

- **Kerberos 5** - (authentification et chiffrement)
- **Kerberos 5i** - (authentification et chiffrement avec protection de l'identité)
- **Kerberos 5p** - (authentification et chiffrement avec protection de l'identité et de la vie privée)

Configurez la règle d'export ONTAP avec les autorisations d'accès appropriées. Par exemple, si les clusters doivent monter les volumes NFS avec un mélange de chiffrement Kerberos 5i et Kerberos 5p, utilisez les paramètres d'accès suivants :

Type	Accès en lecture seule	Accès en lecture/écriture	accès superutilisateur
UNIX	Activé	Activé	Activé
Kerberos 5i	Activé	Activé	Activé
Kerberos 5p	Activé	Activé	Activé

Consultez la documentation suivante pour savoir comment créer des règles d'export ONTAP et des règles de règles d'export :

- "Créer une règles d'export"
- "Ajouter une règle à une règle d'export"

Créer un backend de stockage

Vous pouvez créer une configuration de stockage Trident qui inclut la capacité de chiffrement Kerberos.

À propos de cette tâche

Lorsque vous créez un fichier de configuration du stockage qui configure le chiffrement Kerberos, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du `spec.nfsMountOptions` paramètre :

- `spec.nfsMountOptions: sec=krb5` (authentification et chiffrement)
- `spec.nfsMountOptions: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `spec.nfsMountOptions: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la vie privée)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de chiffrement Kerberos dans la liste des paramètres, seule la première option est utilisée.

Étapes

1. Sur le cluster géré, créez un fichier de configuration du backend de stockage en utilisant l'exemple suivant. Remplacez les valeurs entre crochets <> avec les informations de votre environnement :

```
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. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

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

Si la création du backend échoue, cela signifie qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour en déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

Après avoir identifié et corrigé le problème avec le fichier de configuration, vous pouvez exécuter à nouveau la commande create.

Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec chiffrement Kerberos.

À propos de cette tâche

Lorsque vous créez un objet de classe de stockage, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos à l'aide du `mountOptions` paramètre :

- `mountOptions: sec=krb5` (authentification et chiffrement)
- `mountOptions: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `mountOptions: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la vie privée)

Spécifiez un seul niveau Kerberos. Si vous spécifiez plusieurs niveaux de chiffrement Kerberos dans la liste des paramètres, seule la première option est utilisée. Si le niveau de chiffrement que vous avez spécifié dans la configuration du backend de stockage est différent de celui que vous spécifiez dans l'objet de classe de stockage, l'objet de classe de stockage prévaut.

Étapes

1. Créez un objet Kubernetes StorageClass en utilisant l'exemple suivant :

```
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. Créez la classe de stockage :

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

3. Assurez-vous que la classe de stockage a été créée :

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

Vous devriez voir une sortie similaire à la suivante :

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

Approvisionner des volumes

Après avoir créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour obtenir des instructions, consultez "Provisionner un volume".

Configurer le chiffrement Kerberos en transit avec les volumes Azure NetApp Files

Vous pouvez activer le chiffrement Kerberos sur le trafic de stockage entre votre cluster géré et un seul backend de stockage Azure NetApp Files ou un pool virtuel de backends de stockage Azure NetApp Files.

Avant de commencer

- Assurez-vous d'avoir activé Trident sur le cluster Red Hat OpenShift géré.
- Assurez-vous d'avoir accès à l' `tridentctl`utilitaire.
- Assurez-vous d'avoir préparé le stockage Azure NetApp Files pour le chiffrement Kerberos en prenant note des exigences et en suivant les instructions dans "Documentation Azure NetApp Files".
- Assurez-vous que tous les volumes NFSv4 que vous utilisez avec le chiffrement Kerberos sont correctement configurés. Reportez-vous à la section « Configuration du domaine NFSv4 » (page 13) de NetApp "NetApp NFSv4 : améliorations et guide des bonnes pratiques".

Créer un backend de stockage

Vous pouvez créer une configuration de stockage backend Azure NetApp Files qui inclut la capacité de chiffrement Kerberos.

À propos de cette tâche

Lorsque vous créez un fichier de configuration de stockage qui configure le chiffrement Kerberos, vous pouvez le définir de sorte qu'il soit appliqué à l'un des deux niveaux possibles :

- Le **niveau du backend de stockage** utilisant le `spec.kerberos` champ
- Le **niveau de pool virtuel** utilisant le champ `spec.storage.kerberos`

Lorsque vous définissez la configuration au niveau du pool virtuel, le pool est sélectionné à l'aide de l'étiquette dans la classe de stockage.

À chaque niveau, vous pouvez spécifier l'une des trois versions différentes du chiffrement Kerberos :

- `kerberos: sec=krb5` (authentification et chiffrement)
- `kerberos: sec=krb5i` (authentification et chiffrement avec protection de l'identité)
- `kerberos: sec=krb5p` (authentification et chiffrement avec protection de l'identité et de la vie privée)

Étapes

1. Sur le cluster géré, créez un fichier de configuration du backend de stockage en utilisant l'un des exemples suivants, selon l'endroit où vous devez définir le backend de stockage (au niveau du backend de stockage ou au niveau du pool virtuel). Remplacez les valeurs entre crochets <> avec les informations de votre environnement :

Exemple de niveau de backend de stockage

```
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
```

Exemple de niveau de pool virtuel

```
---
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. Utilisez le fichier de configuration que vous avez créé à l'étape précédente pour créer le backend :

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

Si la création du backend échoue, cela signifie qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour en déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

Après avoir identifié et corrigé le problème avec le fichier de configuration, vous pouvez exécuter à nouveau la commande create.

Créer une classe de stockage

Vous pouvez créer une classe de stockage pour provisionner des volumes avec chiffrement Kerberos.

Étapes

1. Créez un objet Kubernetes StorageClass en utilisant l'exemple suivant :

```
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. Créez la classe de stockage :

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

3. Assurez-vous que la classe de stockage a été créée :

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

Vous devriez voir une sortie similaire à la suivante :

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

Approvisionner des volumes

Après avoir créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour obtenir des instructions, consultez "Provisionner un volume".

Informations sur le copyright

Informations sur les marques commerciales