



Sécurité

Trident

NetApp
January 15, 2026

Sommaire

- Sécurité 1
 - Sécurité 1
 - Exécutez Trident dans son propre espace de noms 1
 - Utilisez l'authentification CHAP avec les backends SAN ONTAP..... 1
 - Utilisez l'authentification CHAP avec les backends NetApp HCI et SolidFire.. 1
 - Utilisez Trident avec NVE et NAE 1
 - Configuration unifiée des clés Linux (LUKS) 2
 - Activer le chiffrement LUKS 2
 - Configuration du backend pour l'importation des volumes LUKS 4
 - Configuration PVC pour l'importation de volumes LUKS..... 4
 - Rotation d'une phrase de passe LUKS 5
 - Activer l'expansion du volume 7
 - Chiffrement Kerberos en transit 8
 - Configurer le chiffrement Kerberos en transit avec les volumes ONTAP sur site 8
 - Configurer le chiffrement Kerberos en transit avec les volumes Azure NetApp Files 12

Sécurité

Sécurité

Suivez les recommandations ci-dessous pour garantir la sécurité de votre installation Trident .

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`). Placer 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'accès à `tridentctl` application.

Utilisez l'authentification CHAP avec les backends SAN ONTAP.

Trident prend en charge l'authentification basée sur CHAP pour les charges de travail ONTAP SAN (en utilisant le `ontap-san` et `ontap-san-economy` conducteurs). NetApp recommande l'utilisation du protocole CHAP bidirectionnel avec Trident pour l'authentification entre un hôte et le système de stockage dorsal.

Pour les backends ONTAP utilisant les pilotes de stockage SAN, Trident peut configurer un protocole CHAP bidirectionnel et gérer les noms d'utilisateur et les secrets CHAP via `tridentctl` . Se référer 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 les backends NetApp HCI et SolidFire.

NetApp recommande le déploiement du protocole CHAP bidirectionnel pour garantir l'authentification entre un hôte et les serveurs dorsaux NetApp HCI et SolidFire . Trident utilise un objet secret qui inclut deux mots de passe CHAP par locataire. Lors de son installation, Trident gère les secrets CHAP et les stocke dans un `tridentvolume` Objet CR 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 groupe d'accès aux volumes.

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, reportez-vous à ["Présentation de la configuration du chiffrement de volume NetApp"](#) .

- Si NAE est activé sur le système dorsal, tout volume provisionné dans Trident sera compatible NAE.
 - Vous pouvez définir l'indicateur de chiffrement NVE sur `""` pour créer des volumes compatibles NAE.
- Si NAE n'est pas activé sur le système dorsal, tout volume provisionné dans Trident sera compatible NVE, sauf si l'indicateur de chiffrement NVE est défini sur `false` (la valeur par défaut) dans la configuration du

backend.

Les volumes créés dans Trident sur un backend compatible NAE doivent être chiffrés NVE ou NAE.



- Vous pouvez définir l'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 l'indicateur de chiffrement NVE sur `false` sur un backend compatible NAE crée un volume compatible NAE. Vous ne pouvez pas désactiver le chiffrement NAE en définissant l'indicateur de chiffrement NVE sur `false`.

- Vous pouvez créer manuellement un volume NVE dans Trident en définissant explicitement l'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 ONTAP NAS"](#)

Configuration unifiée des clés Linux (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 LUKS.

Dans Trident, les volumes chiffrés LUKS utilisent le chiffrement 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 plus d'informations sur les systèmes ASA r2, consultez ["En savoir plus sur les systèmes de stockage ASA r2"](#).

Avant de commencer

- Les nœuds de travail doivent avoir `cryptsetup 2.1` ou supérieur (mais inférieur à 3.0) installé. Pour plus d'informations, consultez ["Gitlab : cryptsetup"](#).
- Pour des raisons de performance, NetApp recommande que les nœuds de travail prennent en charge les nouvelles instructions de la norme de chiffrement avancé (AES-NI). Pour vérifier la prise en charge d'AES-NI, exécutez la commande suivante :

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

Si aucune réponse n'est reçue, votre processeur ne prend pas en charge AES-NI. Pour plus d'informations sur AES-NI, consultez : ["Intel : Instructions de la norme de chiffrement avancée \(AES-NI\)"](#).

Activer le chiffrement LUKS

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

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, veuillez consulter la documentation "[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. Utiliser `parameters.selector` définir les pools de stockage à l'aide du 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 contenant 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
```

Limites

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 configurer `luksEncryption` à `true` en arrière-plan. Le `luksEncryption` Cette option indique à Trident si le volume est conforme à la norme LUKS. (`true`) ou non conforme à LUKS (`false`) comme le montre 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` à `true` et inclure 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

```

Rotation d'une phrase de passe LUKS

Vous pouvez modifier la phrase de passe LUKS et confirmer la modification.



N'oubliez pas une phrase de passe tant que vous n'avez pas vérifié qu'elle n'est plus référencée par aucun volume, instantané ou secret. Si la phrase de passe de référence est perdue, vous risquez de ne pas pouvoir monter le volume et les données resteront chiffrées et inaccessibles.

À propos de cette tâche

La rotation de la phrase de passe LUKS se produit lorsqu'un pod qui monte le volume est créé après la spécification d'une nouvelle phrase de passe LUKS. Lors de la création d'un nouveau pod, Trident compare la phrase de passe LUKS du volume à la phrase de passe active du secret.

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

Étapes

1. Ajoutez le `node-publish-secret-name` et `node-publish-secret-namespace` Paramètres de `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. Identifier les phrases de passe existantes sur le volume ou l'instantané.

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 pour spécifier les nouvelles et anciennes phrases de passe. Assurer `previous-luks-passphrase-name` et `previous-luks-passphrase` correspondre 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 lancer 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 a été 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 une nouvelle capsule 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. Activer `CSINodeExpandSecret` fonctionnalité gate (bêta 1.25+). Se référer à ["Kubernetes 1.25 : Utilisation des secrets pour l'extension des volumes CSI pilotée par les nœuds"](#) pour plus de détails.
2. Ajoutez le `node-expand-secret-name` et `node-expand-secret-namespace` Paramètres de `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 l'extension du stockage en ligne, le kubelet transmet les informations d'identification appropriées au pilote.

Chiffrement Kerberos en transit

En utilisant le chiffrement Kerberos en transit, vous pouvez améliorer la sécurité d'accès aux données en activant le chiffrement du trafic entre votre cluster géré et le système de stockage dorsal.

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

- * ONTAP sur site* - 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 utilisant 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 systèmes de stockage ONTAP sur site n'est pris en charge qu'avec l'interface suivante : `ontap-nas` pilote de stockage.

Avant de commencer

- Assurez-vous d'avoir accès à `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 système de stockage ONTAP .
- Assurez-vous d'avoir préparé la machine virtuelle de stockage ONTAP pour prendre en charge le chiffrement Kerberos pour les volumes NFS. Se référer à "[Activer Kerberos sur une LIF de données](#)" pour les 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 NetApp NFSv4 (page 13) du manuel. "[Guide des améliorations et des bonnes pratiques NetApp NFSv4](#)" .

Ajouter ou modifier les politiques d'exportation ONTAP

Vous devez ajouter des règles aux politiques d'exportation ONTAP existantes ou créer de nouvelles politiques d'exportation 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 de politique d'exportation que vous ajoutez, ou les nouvelles politiques d'exportation que vous créez, doivent prendre en charge les protocoles d'accès et les autorisations d'accès suivants :

Protocoles d'accès

Configurez la politique d'exportation 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 des besoins de votre 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 de stratégie d'exportation 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 politiques d'exportation ONTAP et des règles de politique d'exportation :

- ["Créer une politique d'exportation"](#)
- ["Ajouter une règle à une politique d'exportation"](#)

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 de stockage dorsal qui configure le chiffrement Kerberos, vous pouvez spécifier l'une des trois versions différentes de chiffrement Kerberos à l'aide de `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 sera utilisée.

Étapes

1. Sur le cluster géré, créez un fichier de configuration de stockage en utilisant l'exemple suivant. Remplacez les valeurs entre crochets <> par les informations provenant 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, c'est qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour déterminer la cause en exécutant la commande suivante :

```
tridentctl logs
```

Une fois le problème du fichier de configuration identifié et corrigé, vous pouvez exécuter à nouveau la commande de création.

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 de `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 sera utilisée. Si le niveau de chiffrement que vous avez spécifié dans la configuration du backend de stockage est différent de celui que vous avez spécifié dans l'objet de classe de stockage, c'est l'objet de classe de stockage qui prévaut.

Étapes

1. Créez un objet `StorageClass` Kubernetes 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 obtenir un résultat similaire à celui-ci :

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

Volumes de provision

Une fois que vous avez créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour les instructions, reportez-vous à ["Provisionnez 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 `tridentctl` utilitaire.
- Assurez-vous d'avoir préparé le système de stockage Azure NetApp Files pour le chiffrement Kerberos en prenant en compte les exigences et en suivant les instructions. ["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 NetApp NFSv4 (page 13) du manuel. ["Guide des améliorations et des bonnes pratiques NetApp NFSv4"](#) .

Créer un backend de stockage

Vous pouvez créer une configuration de stockage backend Azure NetApp Files incluant la fonctionnalité 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 suivants :

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

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 de backend de stockage en utilisant l'un des exemples suivants, selon l'endroit où vous devez définir le backend de stockage (niveau du backend de stockage ou niveau du pool virtuel). Remplacez les valeurs entre crochets `<>` par les informations provenant de votre environnement :

Exemple de niveau 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 piscine virtuelle

```

---
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, c'est qu'il y a un problème avec la configuration du backend. Vous pouvez consulter les journaux pour déterminer la cause en exécutant la commande suivante :


```
tridentctl logs
```

Une fois le problème du fichier de configuration identifié et corrigé, vous pouvez exécuter à nouveau la commande de création.

Créer une classe de stockage

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

Étapes

1. Créez un objet StorageClass Kubernetes 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 obtenir un résultat similaire à celui-ci :

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

Volumes de provision

Une fois que vous avez créé un système de stockage et une classe de stockage, vous pouvez maintenant provisionner un volume. Pour les instructions, reportez-vous à ["Provisionnez un volume"](#) .

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.