



Configuration des systèmes back-end

Astra Trident

NetApp
April 16, 2024

Sommaire

- Configuration des systèmes back-end 1
 - Configurer un back-end Azure NetApp Files 1
 - Configurer CVS pour le back-end GCP 9
 - Configurer un système NetApp HCI ou SolidFire backend 20
 - Configurer un système back-end avec des pilotes ONTAP ou Cloud Volumes ONTAP SAN 26
 - Configurer un système back-end avec les pilotes NAS ONTAP 45
 - Utilisez Astra Trident avec Amazon FSX pour NetApp ONTAP 66

Configuration des systèmes back-end

Un système back-end définit la relation entre Astra Trident et un système de stockage. Il explique à Astra Trident comment communiquer avec ce système de stockage et comment Astra Trident doit provisionner des volumes à partir de celui-ci. Astra Trident proposera automatiquement des pools de stockage provenant des systèmes back-end qui correspondent aux exigences définies par une classe de stockage. En savoir plus sur la configuration du système back-end en fonction du type de système de stockage dont vous disposez.

- ["Configurer un back-end Azure NetApp Files"](#)
- ["Configurer un système back-end Cloud Volumes Service pour Google Cloud Platform"](#)
- ["Configurer un système NetApp HCI ou SolidFire backend"](#)
- ["Configurer un système back-end avec des pilotes NAS ONTAP ou Cloud Volumes ONTAP"](#)
- ["Configurer un système back-end avec des pilotes ONTAP ou Cloud Volumes ONTAP SAN"](#)
- ["Utilisez Astra Trident avec Amazon FSX pour NetApp ONTAP"](#)

Configurer un back-end Azure NetApp Files

Découvrez comment configurer Azure NetApp Files (ANF) en tant que backend pour votre installation d'Astra Trident à l'aide des exemples de configuration fournis.



Le service Azure NetApp Files ne prend pas en charge des volumes inférieurs à 100 Go. Astra Trident crée automatiquement des volumes de 100 Go en cas de demande d'un volume plus petit.

Ce dont vous avez besoin

Pour configurer et utiliser un ["Azure NetApp Files"](#) back-end, vous avez besoin des éléments suivants :

- `subscriptionID` Depuis un abonnement Azure avec Azure NetApp Files activé.
- `tenantID`, `clientID`, et `clientSecret` à partir d'un ["Enregistrement d'applications"](#) Dans Azure Active Directory avec les autorisations suffisantes pour le service Azure NetApp Files. L'enregistrement de l'application doit utiliser le `Owner` ou `Contributor` Rôle prédéfini par Azure.



Pour en savoir plus sur les rôles intégrés dans Azure, consultez la ["Documentation Azure"](#).

- `Azure location` qui contient au moins un ["sous-réseau délégué"](#). À partir de Trident 22.01, le `location` le paramètre est un champ obligatoire au niveau supérieur du fichier de configuration back-end. Les valeurs d'emplacement spécifiées dans les pools virtuels sont ignorées.
- Si vous utilisez Azure NetApp Files pour la première fois ou à un nouvel emplacement, une certaine configuration initiale est requise. Voir la ["guide de démarrage rapide"](#).

Description de la tâche

En fonction de la configuration back-end (sous-réseau, réseau virtuel, niveau de service et emplacement), Trident crée des volumes ANF dans des pools de capacité disponibles à l'emplacement demandé et qui correspondent au niveau de service et au sous-réseau requis.



REMARQUE : Astra Trident ne prend pas en charge les pools de capacité manuels de QoS.

Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	« azure-netapp-files »
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + caractères aléatoires
subscriptionID	L'ID d'abonnement de votre abonnement Azure	
tenantID	ID locataire d'un enregistrement d'application	
clientID	L'ID client d'un enregistrement d'application	
clientSecret	Secret client d'un enregistrement d'application	
serviceLevel	Un de Standard, Premium, ou Ultra	« » (aléatoire)
location	Nom de l'emplacement Azure dans lequel les nouveaux volumes seront créés	
serviceLevel	Un de Standard, Premium, ou Ultra	« » (aléatoire)
resourceGroups	Liste des groupes de ressources pour le filtrage des ressources découvertes	« [] » (sans filtre)
netappAccounts	Liste des comptes NetApp permettant de filtrer les ressources découvertes	« [] » (sans filtre)
capacityPools	Liste des pools de capacité pour le filtrage des ressources découvertes	« [] » (sans filtre, aléatoire)
virtualNetwork	Nom d'un réseau virtuel avec un sous-réseau délégué	« »
subnet	Nom d'un sous-réseau délégué à Microsoft.Netapp/volumes	« »
nfsMountOptions	Contrôle précis des options de montage NFS.	« nfsvers=3 »
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur	« » (non appliqué par défaut)

Paramètre	Description	Valeur par défaut
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple <pre>\{"api": false, "method": true, "discovery": true\}.</pre> Ne l'utilisez pas à moins que vous ne soyez en mesure de résoudre les problèmes et que vous ayez besoin d'un vidage détaillé des journaux.	nul



Si vous rencontrez une erreur "aucun pool de capacité détecté" lors de la tentative de création d'une demande de volume persistant, il est probable que votre enregistrement d'application ne dispose pas des autorisations et ressources requises (sous-réseau, réseau virtuel, pool de capacité) associées. Astra Trident consigne les ressources Azure qu'il a découvertes lors de la création du système back-end lorsque le débogage est activé. Assurez-vous de vérifier si un rôle approprié est utilisé.



Si vous souhaitez monter des volumes à l'aide de la version 4.1 de NFS, vous pouvez inclure `nfsvers=4` Dans la liste des options de montage délimitées par des virgules, choisissez NFS v4.1. Toutes les options de montage définies dans une classe de stockage remplacent les options de montage définies dans un fichier de configuration backend.

Les valeurs de `resourceGroups`, `netappAccounts`, `capacityPools`, `virtualNetwork`, et `subnet` peut être spécifié à l'aide de noms courts ou complets. Les noms abrégés peuvent correspondre à plusieurs ressources avec le même nom, donc l'utilisation de noms complets est recommandée dans la plupart des cas. Le `resourceGroups`, `netappAccounts`, et `capacityPools` les valeurs sont des filtres qui limitent l'ensemble des ressources découvertes aux ressources disponibles pour ce stockage back-end et peuvent être spécifiés dans n'importe quelle combinaison. Les noms complets sont au format suivant :

Type	Format
Groupe de ressources	<groupe de ressources>
Compte NetApp	<groupe de ressources>/<compte netapp>
Pool de capacité	<groupe de ressources>/<compte netapp>/<pool de capacité>
Réseau virtuel	<groupe de ressources>/<réseau virtuel>
Sous-réseau	<groupe de ressources>/<réseau virtuel>/<sous-réseau>

Vous pouvez contrôler la manière dont chaque volume est provisionné par défaut en spécifiant les options suivantes dans une section spéciale du fichier de configuration. Voir les exemples de configuration ci-dessous.

Paramètre	Description	Valeur par défaut
exportRule	Règle(s) d'exportation pour les nouveaux volumes	« 0.0.0.0/0 »
snapshotDir	Contrôle la visibilité du répertoire <code>.snapshot</code>	« faux »

Paramètre	Description	Valeur par défaut
size	Taille par défaut des nouveaux volumes	« 100 G »
unixPermissions	Les autorisations unix des nouveaux volumes (4 chiffres octaux)	« » (fonction d'aperçu, liste blanche requise dans l'abonnement)

Le `exportRule` La valeur doit être une liste séparée par des virgules d'une combinaison d'adresses IPv4 ou de sous-réseaux IPv4 en notation CIDR.



Pour tous les volumes créés sur un back-end ANF, Astra Trident copie tous les libellés présents sur un pool de stockage vers le volume de stockage au moment du provisionnement. Les administrateurs de stockage peuvent définir des étiquettes par pool de stockage et regrouper tous les volumes créés dans un pool de stockage. Cela permet de différencier facilement les volumes en fonction d'un ensemble d'étiquettes personnalisables fournies dans la configuration back-end.

Exemple 1 : configuration minimale

Il s'agit de la configuration back-end minimale absolue. Avec cette configuration, Astra Trident détecte tous vos comptes, pools de capacité et sous-réseaux NetApp délégués à ANF à l'emplacement configuré et place les nouveaux volumes sur l'un de ces pools et sous-réseaux de manière aléatoire.

Cette configuration est idéale pour commencer avec ANF et essayer certaines choses. Toutefois, dans la pratique, vous voulez fournir des fonctionnalités supplémentaires pour déterminer les volumes que vous provisionnez.

```
{
  "version": 1,
  "storageDriverName": "azure-netapp-files",
  "subscriptionID": "9f87c765-4774-fake-ae98-a721add45451",
  "tenantID": "68e4f836-edc1-fake-bff9-b2d865ee56cf",
  "clientID": "dd043f63-bf8e-fake-8076-8de91e5713aa",
  "clientSecret": "SECRET",
  "location": "eastus"
}
```

Exemple 2 : configuration de niveau de service spécifique avec des filtres de pool de capacité

Cette configuration back-end place les volumes dans des Azure `eastus` emplacement dans un `Ultra` pool de capacité. Astra Trident détecte automatiquement tous les sous-réseaux délégués à ANF dans cet emplacement et place un nouveau volume de façon aléatoire sur l'un d'entre eux.

```
{
  "version": 1,
  "storageDriverName": "azure-netapp-files",
  "subscriptionID": "9f87c765-4774-fake-ae98-a721add45451",
  "tenantID": "68e4f836-edc1-fake-bff9-b2d865ee56cf",
  "clientID": "dd043f63-bf8e-fake-8076-8de91e5713aa",
  "clientSecret": "SECRET",
  "location": "eastus",
  "serviceLevel": "Ultra",
  "capacityPools": [
    "application-group-1/account-1/ultra-1",
    "application-group-1/account-1/ultra-2"
  ],
}
```

Exemple 3 : configuration avancée

Cette configuration back-end réduit davantage l'étendue du placement des volumes sur un seul sous-réseau et modifie également certains paramètres par défaut du provisionnement des volumes.

```

{
  "version": 1,
  "storageDriverName": "azure-netapp-files",
  "subscriptionID": "9f87c765-4774-fake-ae98-a721add45451",
  "tenantID": "68e4f836-edc1-fake-bff9-b2d865ee56cf",
  "clientID": "dd043f63-bf8e-fake-8076-8de91e5713aa",
  "clientSecret": "SECRET",
  "location": "eastus",
  "serviceLevel": "Ultra",
  "capacityPools": [
    "application-group-1/account-1/ultra-1",
    "application-group-1/account-1/ultra-2"
  ],
  "virtualNetwork": "my-virtual-network",
  "subnet": "my-subnet",
  "nfsMountOptions": "vers=3,proto=tcp,timeo=600",
  "limitVolumeSize": "500Gi",
  "defaults": {
    "exportRule": "10.0.0.0/24,10.0.1.0/24,10.0.2.100",
    "snapshotDir": "true",
    "size": "200Gi",
    "unixPermissions": "0777"
  }
}
=====

```

Exemple 4 : configuration de pool de stockage virtuel

Cette configuration back-end définit plusieurs pools de stockage dans un seul fichier. Cette fonction est utile lorsque plusieurs pools de capacité prennent en charge différents niveaux de service, et que vous souhaitez créer des classes de stockage dans Kubernetes qui les représentent.


```

{
  "version": 1,
  "storageDriverName": "azure-netapp-files",
  "subscriptionID": "9f87c765-4774-fake-ae98-a721add45451",
  "tenantID": "68e4f836-edc1-fake-bff9-b2d865ee56cf",
  "clientID": "dd043f63-bf8e-fake-8076-8de91e5713aa",
  "clientSecret": "SECRET",
  "location": "eastus",
  "resourceGroups": ["application-group-1"],
  "nfsMountOptions": "vers=3,proto=tcp,timeo=600",
  "labels": {
    "cloud": "azure"
  },
  "location": "eastus",

  "storage": [
    {
      "labels": {
        "performance": "gold"
      },
      "serviceLevel": "Ultra",
      "capacityPools": ["ultra-1", "ultra-2"]
    },
    {
      "labels": {
        "performance": "silver"
      },
      "serviceLevel": "Premium",
      "capacityPools": ["premium-1"]
    },
    {
      "labels": {
        "performance": "bronze"
      },
      "serviceLevel": "Standard",
      "capacityPools": ["standard-1", "standard-2"]
    }
  ]
}

```

Les éléments suivants StorageClass les définitions font référence aux pools de stockage ci-dessus. À l'aide du `parameters.selector` vous pouvez spécifier pour chaque champ StorageClass pool virtuel utilisé pour héberger un volume. Les aspects définis dans le pool sélectionné seront définis pour le volume.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gold
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: bronze
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze"
allowVolumeExpansion: true

```

Et la suite ?

Après avoir créé le fichier de configuration backend, exécutez la commande suivante :

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

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour 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 de nouveau la commande create.

Configurer CVS pour le back-end GCP

Découvrez comment configurer NetApp Cloud Volumes Service (CVS) pour Google Cloud Platform (GCP) en tant que backend avec votre installation d'Astra Trident, à l'aide des exemples de configurations fournis.



NetApp Cloud Volumes Service pour Google Cloud ne prend pas en charge les volumes CVS-Performance de moins de 100 Gio, ou les volumes CVS de moins de 300 Gio. Astra Trident crée automatiquement des volumes de taille minimale si le volume demandé est inférieur à la taille minimale.

Ce dont vous avez besoin

Pour configurer et utiliser le ["Cloud Volumes Service pour Google Cloud"](#) back-end, vous avez besoin des éléments suivants :

- Un compte Google Cloud configuré avec NetApp CVS
- Numéro de projet de votre compte Google Cloud
- Compte de service Google Cloud avec le `netappcloudvolumes.admin` rôle
- Fichier de clé API pour votre compte de service CVS

Astra Trident inclut désormais la prise en charge par défaut des volumes plus petits ["Type de service CVS sur GCP"](#). Pour les systèmes back-end créés avec `storageClass=software`, Les volumes auront une taille de provisionnement minimale de 300 Gio. CVS offre actuellement cette fonctionnalité sous disponibilité contrôlée et ne fournit pas de support technique. Les utilisateurs doivent s'inscrire pour accéder aux volumes de sous-Tio ["ici"](#). NetApp recommande aux clients d'utiliser des volumes de sous-Tio pour **charges de travail non-production**.



Lors du déploiement des systèmes back-end avec le type de service CVS par défaut (`storageClass=software`), les utilisateurs doivent obtenir l'accès à la fonctionnalité de volumes de sous-Tio dans GCP pour le(s) numéro(s) de projet et l'ID de projet en question. Il est nécessaire qu'Astra Trident provisionne des volumes de sous-Tio. Si ce n'est pas le cas, les créations de volume échoueront pour les demandes de volume dont la taille est inférieure à 600 Gio. Obtenir l'accès aux volumes de sous-Tio à l'aide de ["ce formulaire"](#).

Les volumes créés par Astra Trident pour le niveau de service CVS par défaut seront provisionnés comme suit :

- Si la quantité de PVC est inférieure à 300 Gio, l'Astra Trident crée un volume CVS de 300 Gio.
- Avec des demandes de volume persistant comprises entre 300 Gio et 600 Gio, l'Astra Trident crée un volume CVS de la taille demandée.
- Si les demandes de volume persistant sont comprises entre 600 Gio et 1 Tio, l'Astra Trident crée un volume CVS Tio.
- Avec des demandes de volume supérieur à 1 Tio, Astra Trident crée un volume CVS de la taille demandée.

Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	« gcp-cvs »
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + partie de la clé API
storageClass	Type de stockage. Choisissez parmi <code>hardware</code> (performances optimisées) ou <code>software</code> (Type de service CVS)	
projectNumber	Numéro de projet de compte Google Cloud. La valeur ajoutée est disponible sur la page d'accueil du portail Google Cloud.	
apiRegion	Région de compte CVS. Il s'agit de la région où le back-end provisionne les volumes.	
apiKey	Clé API pour le compte de service Google Cloud avec le <code>netappcloudvolumes.admin</code> rôle. Il inclut le contenu au format JSON du fichier de clé privée d'un compte de service Google Cloud (copié en compte dans le fichier de configuration back-end).	
proxyURL	URL proxy si le serveur proxy doit se connecter au compte CVS. Le serveur proxy peut être un proxy HTTP ou HTTPS. Pour un proxy HTTPS, la validation du certificat est ignorée pour permettre l'utilisation de certificats auto-signés dans le serveur proxy. Les serveurs proxy avec authentification activée ne sont pas pris en charge.	
nfsMountOptions	Contrôle précis des options de montage NFS.	« nfsvers=3 »
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur	« » (non appliqué par défaut)
serviceLevel	Niveau de service CVS pour les nouveaux volumes. Les valeurs sont « standard », « Premium » et « extrême ».	« standard »
network	Réseau GCP utilisé pour les volumes CVS	« par défaut »

Paramètre	Description	Valeur par défaut
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple <code>\{"api":false,"method":true\}</code> . Ne l'utilisez pas à moins que vous ne soyez en mesure de résoudre les problèmes et que vous ayez besoin d'un vidage détaillé des journaux.	nul

Si vous utilisez un réseau VPC partagé, les deux `projectNumber` et `hostProjectNumber` doit être spécifié. Dans ce cas, `projectNumber` est le projet de service, et `hostProjectNumber` est le projet hôte.

Le `apiRegion` Il représente la région GCP dans laquelle Astra Trident crée des volumes CVS. Lors de la création de clusters Kubernetes multi-région, des volumes CVS sont créés dans un `apiRegion` Peut être utilisé pour des charges de travail planifiées sur des nœuds dans plusieurs régions GCP. Sachez que le trafic entre les régions coûte plus cher.



- Pour activer l'accès inter-région, votre définition de classe de stockage pour `allowedTopologies` doit inclure toutes les régions. Par exemple :

```
- key: topology.kubernetes.io/region
  values:
  - us-east1
  - europe-west1
```

- `storageClass` est un paramètre facultatif que vous pouvez utiliser pour sélectionner le paramètre souhaité "Type de service CVS". Vous pouvez choisir parmi le type de service CVS de base (`storageClass=software`) Ou le type de service CVS-Performance (`storageClass=hardware`), que Trident utilise par défaut. Assurez-vous de spécifier un `apiRegion` Qui fournit le CVS respectif `storageClass` dans votre définition de back-end.



L'intégration d'Astra Trident avec le type de service CVS de base sur Google Cloud est une fonctionnalité **bêta**, non destinée aux workloads de production. Trident est **entièrement pris en charge** avec le type de service CVS-Performance et l'utilise par défaut.

Chaque back-end provisionne les volumes dans une seule région Google Cloud. Pour créer des volumes dans d'autres régions, vous pouvez définir des systèmes back-end supplémentaires.

Vous pouvez contrôler la manière dont chaque volume est provisionné par défaut en spécifiant les options suivantes dans une section spéciale du fichier de configuration. Voir les exemples de configuration ci-dessous.

Paramètre	Description	Valeur par défaut
exportRule	Règle(s) d'exportation pour les nouveaux volumes	« 0.0.0.0/0 »
snapshotDir	Accès au <code>.snapshot</code> répertoire	« faux »


```

sIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOgu
SaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyA
ZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz
1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3
bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4
Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5o
jY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nzn
HczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrt
HisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbO
guSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKe
yAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRA
Gz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4j
K3bl/qp8B4Kws8zX5ojY9m\nXsYg6gyxy4zq7OlwWgLwGa==\n-----END PRIVATE
KEY-----\n",
    "client_email": "cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com",
    "client_id": "123456789012345678901",
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url":
"https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url":
"https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com"
  }
}

```

Exemple 3 : configuration de niveau de service unique

Cet exemple montre un fichier back-end qui applique les mêmes aspects à tous les systèmes de stockage créés par Astra Trident dans la région Google Cloud US-west2. Cet exemple montre également l'utilisation de proxyURL dans le fichier de configuration back-end.

```

{
  "version": 1,
  "storageDriverName": "gcp-cvs",
  "projectNumber": "012345678901",
  "apiRegion": "us-west2",
  "apiKey": {
    "type": "service_account",
    "project_id": "my-gcp-project",
    "private_key_id": "1234567890123456789012345678901234567890",
    "private_key": "-----BEGIN PRIVATE KEY-----
\nznHczZsrrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZ
srrtHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisI
sAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrrtHisIsAbOguSa

```



```

PIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZN
chRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1z
ZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl
/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4K
ws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5oj
Y9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznH
czZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtr
HisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbO
guSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPI
KeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyA
ZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAG
z1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK
3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B
4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX
5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nzn
HczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtr
HisIsAbOguSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbO
guSaPIKeyAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKe
yAZNchRAGz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRA
Gz1zZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz1zZE4j
K3bl/qp8B4Kws8zX5ojY9m\nXsYg6gyxy4zq70lwWgLwGa==\n-----END PRIVATE
KEY-----\n",
    "client_email": "cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com",
    "client_id": "123456789012345678901",
    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url":
"https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url":
"https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com"
  },
  "proxyURL": "http://proxy-server-hostname/",
  "nfsMountOptions": "vers=3,proto=tcp,timeo=600",
  "limitVolumeSize": "10Ti",
  "serviceLevel": "premium",
  "defaults": {
    "snapshotDir": "true",
    "snapshotReserve": "5",
    "exportRule": "10.0.0.0/24,10.0.1.0/24,10.0.2.100",
    "size": "5Ti"
  }
}

```

Exemple 4 : configuration de pool de stockage virtuel

Cet exemple représente le fichier de définition back-end configuré avec des pools de stockage virtuel et avec StorageClasses cela leur renvoie.

Dans l'exemple de fichier de définition de back-end illustré ci-dessous, des valeurs par défaut spécifiques sont définies pour tous les pools de stockage, qui définissent le snapshotReserve à 5 % et le exportRule à 0.0.0.0/0. Les pools de stockage virtuels sont définis dans le storage section. Dans cet exemple, chaque pool de stockage est défini lui-même serviceLevel, et certains pools remplacent les valeurs par défaut.

```
{
  "version": 1,
  "storageDriverName": "gcp-cvs",
  "projectNumber": "012345678901",
  "apiRegion": "us-west2",
  "apiKey": {
    "type": "service_account",
    "project_id": "my-gcp-project",
    "private_key_id": "1234567890123456789012345678901234567890",
    "private_key": "-----BEGIN PRIVATE KEY-----
\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZ
srtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisI
sAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSa
PIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZN
chRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzll
ZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl
/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kw
s8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY
9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHc
zZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHi
sIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOgu
SaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyA
ZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGz
llZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3
bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4
Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5o
jY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nzn
HczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtr
HisIsAbOguSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbO
guSaPIKeyAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKe
yAZNchRAGzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRA
GzllZE4jK3bl/qp8B4Kws8zX5ojY9m\nznHczZsrtrHisIsAbOguSaPIKeyAZNchRAGzllZE4j
K3bl/qp8B4Kws8zX5ojY9m\nXsYg6gyxy4zq7OlwWgLwGa==\n-----END PRIVATE
KEY-----\n",
    "client_email": "cloudvolumes-admin-sa@my-gcp-
project.iam.gserviceaccount.com",
    "client_id": "123456789012345678901",
```

```

    "auth_uri": "https://accounts.google.com/o/oauth2/auth",
    "token_uri": "https://oauth2.googleapis.com/token",
    "auth_provider_x509_cert_url":
"https://www.googleapis.com/oauth2/v1/certs",
    "client_x509_cert_url":
"https://www.googleapis.com/robot/v1/metadata/x509/cloudvolumes-admin-
sa%40my-gcp-project.iam.gserviceaccount.com"
  },
  "nfsMountOptions": "vers=3,proto=tcp,timeo=600",

  "defaults": {
    "snapshotReserve": "5",
    "exportRule": "0.0.0.0/0"
  },

  "labels": {
    "cloud": "gcp"
  },
  "region": "us-west2",

  "storage": [
    {
      "labels": {
        "performance": "extreme",
        "protection": "extra"
      },
      "serviceLevel": "extreme",
      "defaults": {
        "snapshotDir": "true",
        "snapshotReserve": "10",
        "exportRule": "10.0.0.0/24"
      }
    },
    {
      "labels": {
        "performance": "extreme",
        "protection": "standard"
      },
      "serviceLevel": "extreme"
    },
    {
      "labels": {
        "performance": "premium",
        "protection": "extra"
      },
      "serviceLevel": "premium",

```

```

        "defaults": {
            "snapshotDir": "true",
            "snapshotReserve": "10"
        },
        {
            "labels": {
                "performance": "premium",
                "protection": "standard"
            },
            "serviceLevel": "premium"
        },
        {
            "labels": {
                "performance": "standard"
            },
            "serviceLevel": "standard"
        }
    ]
}

```

Les définitions de classe de stockage suivantes font référence aux pools de stockage ci-dessus. À l'aide du `parameters.selector` Vous pouvez spécifier pour chaque classe de stockage le pool virtuel utilisé pour héberger un volume. Les aspects définis dans le pool sélectionné seront définis pour le volume.

La première classe de stockage (`cvs-extreme-extra-protection`) correspond au premier pool de stockage virtuel. Il s'agit du seul pool offrant des performances extrêmes avec une réserve Snapshot de 10 %. La dernière classe de stockage (`cvs-extra-protection`) appelle tout pool de stockage qui fournit une réserve d'instantanés de 10%. Astra Trident décide du pool de stockage virtuel sélectionné et s'assure que les exigences de la réserve Snapshot sont respectées.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=extreme; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extreme-standard-protection
provisioner: netapp.io/trident

```

```

parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=extra"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-premium
provisioner: netapp.io/trident
parameters:
  selector: "performance=premium; protection=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-standard
provisioner: netapp.io/trident
parameters:
  selector: "performance=standard"
allowVolumeExpansion: true
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: cvs-extra-protection
provisioner: netapp.io/trident
parameters:
  selector: "protection=extra"
allowVolumeExpansion: true

```

Et la suite ?

Après avoir créé le fichier de configuration backend, exécutez la commande suivante :

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

Si la création du back-end échoue, la configuration du back-end est erronée. Vous pouvez afficher les journaux pour 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 de nouveau la commande `create`.

Configurer un système NetApp HCI ou SolidFire backend

Découvrez comment créer et utiliser un système Element backend avec votre installation d'Astra Trident.

Ce dont vous avez besoin

- Système de stockage pris en charge exécutant le logiciel Element.
- Identifiants de locataire ou administrateur de cluster NetApp HCI/SolidFire pouvant gérer les volumes
- Tous vos nœuds workers Kubernetes doivent avoir installé les outils iSCSI appropriés. Voir ["informations de préparation du nœud de travail"](#).

Ce que vous devez savoir

Le `solidfire-san` le pilote de stockage prend en charge les deux modes de volume : fichier et bloc. Pour le `Filesystem` En mode volume, Astra Trident crée un volume et crée un système de fichiers. Le type de système de fichiers est spécifié par la classe de stockage.

Conducteur	Protocole	Mode Volume	Modes d'accès pris en charge	Systèmes de fichiers pris en charge
<code>solidfire-san</code>	ISCSI	Bloc	RWO,ROX,RWX	Aucun système de fichiers. Périphérique de bloc brut.
<code>solidfire-san</code>	ISCSI	Bloc	RWO,ROX,RWX	Aucun système de fichiers. Périphérique de bloc brut.
<code>solidfire-san</code>	ISCSI	Système de fichiers	RWO,ROX	<code>xfs</code> , <code>ext3</code> , <code>ext4</code>
<code>solidfire-san</code>	ISCSI	Système de fichiers	RWO,ROX	<code>xfs</code> , <code>ext3</code> , <code>ext4</code>



Astra Trident utilise le protocole CHAP lorsqu'il fonctionne comme un mécanisme de provisionnement CSI amélioré. Si vous utilisez CHAP (qui est la valeur par défaut pour CSI), aucune autre préparation n'est requise. Il est recommandé de définir explicitement le `UseCHAP` Possibilité d'utiliser CHAP avec Trident non CSI. Sinon, voir ["ici"](#).



Les groupes d'accès aux volumes sont uniquement pris en charge par le framework classique non CSI pour Astra Trident. Lorsqu'il est configuré pour fonctionner en mode CSI, Astra Trident utilise le protocole CHAP.

Si aucun de ces deux cas `AccessGroups` ou `UseCHAP` sont définies, l'une des règles suivantes s'applique :

- Si la valeur par défaut `trident` groupe d'accès détecté, groupes d'accès utilisés.
- Si aucun groupe d'accès n'est détecté et que la version de Kubernetes est 1.7 ou ultérieure, CHAP est utilisé.

Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
<code>version</code>		Toujours 1
<code>storageDriverName</code>	Nom du pilote de stockage	Toujours « <code>solidfire-san</code> ».
<code>backendName</code>	Nom personnalisé ou système back-end de stockage	"SolidFire_" + adresse IP de stockage (iSCSI)
<code>Endpoint</code>	MVIP pour le cluster SolidFire avec les identifiants de locataire	
<code>SVIP</code>	Port et adresse IP de stockage (iSCSI)	
<code>labels</code>	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes.	« »
<code>TenantName</code>	Nom du locataire à utiliser (créé si introuvable)	
<code>InitiatorIFace</code>	Limitez le trafic iSCSI à une interface hôte spécifique	« par défaut »
<code>UseCHAP</code>	Utilisez CHAP pour authentifier iSCSI	vrai
<code>AccessGroups</code>	Liste des ID de groupes d'accès à utiliser	Recherche l'ID d'un groupe d'accès nommé « <code>trident</code> »
<code>Types</code>	Spécifications de QoS	
<code>limitVolumeSize</code>	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur	« » (non appliqué par défaut)
<code>debugTraceFlags</code>	Indicateurs de débogage à utiliser lors du dépannage. Exemple, <code>{"api":false, "méthode":true}</code>	nul



Ne pas utiliser `debugTraceFlags` à moins que vous ne soyez en mesure de dépanner et que vous ayez besoin d'un vidage détaillé des journaux.



Pour tous les volumes créés, Astra Trident copie tous les libellés présents dans un pool de stockage vers le LUN de stockage back-end au moment du provisionnement. Les administrateurs de stockage peuvent définir des étiquettes par pool de stockage et regrouper tous les volumes créés dans un pool de stockage. Cela permet de différencier facilement les volumes en fonction d'un ensemble d'étiquettes personnalisables fournies dans la configuration back-end.

Exemple 1 : configuration back-end pour `solidfire-san` avec trois types de volume

Cet exemple montre un fichier back-end utilisant l'authentification CHAP et la modélisation de trois types de volumes avec des garanties de QoS spécifiques. Il est fort probable que vous définiriez ensuite des classes de stockage pour consommer chacune de ces catégories à l'aide de l' `IOPS` paramètre de classe de stockage.

```
{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://<user>:<password>@<mvip>/json-rpc/8.0",
  "SVIP": "<svip>:3260",
  "TenantName": "<tenant>",
  "labels": {"k8scluster": "dev1", "backend": "dev1-element-cluster"},
  "UseCHAP": true,
  "Types": [{"Type": "Bronze", "Qos": {"minIOPS": 1000, "maxIOPS": 2000,
    "burstIOPS": 4000}},
    {"Type": "Silver", "Qos": {"minIOPS": 4000, "maxIOPS": 6000,
    "burstIOPS": 8000}},
    {"Type": "Gold", "Qos": {"minIOPS": 6000, "maxIOPS": 8000,
    "burstIOPS": 10000}}]
}
```

Exemple 2 : configuration du back-end et de la classe de stockage pour `solidfire-san` pilote avec pools de stockage virtuel

Cet exemple représente le fichier de définition back-end configuré avec des pools de stockage virtuel et des classes de stockage qui les renvoient.

Dans l'exemple de fichier de définition de back-end illustré ci-dessous, des valeurs par défaut spécifiques sont définies pour tous les pools de stockage, qui définissent le `type` Du niveau Silver. Les pools de stockage virtuels sont définis dans le `storage` section. Dans cet exemple, certains pools de stockage définissent leur propre type et certains pools remplacent les valeurs par défaut définies ci-dessus.


```

{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://<user>:<password>@<mvip>/json-rpc/8.0",
  "SVIP": "<svip>:3260",
  "TenantName": "<tenant>",
  "UseCHAP": true,
  "Types": [{"Type": "Bronze", "Qos": {"minIOPS": 1000, "maxIOPS": 2000,
"burstIOPS": 4000}},
            {"Type": "Silver", "Qos": {"minIOPS": 4000, "maxIOPS": 6000,
"burstIOPS": 8000}},
            {"Type": "Gold", "Qos": {"minIOPS": 6000, "maxIOPS": 8000,
"burstIOPS": 10000}}],

  "type": "Silver",
  "labels":{"store":"solidfire", "k8scluster": "dev-1-cluster"},
  "region": "us-east-1",

  "storage": [
    {
      "labels":{"performance":"gold", "cost":"4"},
      "zone":"us-east-1a",
      "type":"Gold"
    },
    {
      "labels":{"performance":"silver", "cost":"3"},
      "zone":"us-east-1b",
      "type":"Silver"
    },
    {
      "labels":{"performance":"bronze", "cost":"2"},
      "zone":"us-east-1c",
      "type":"Bronze"
    },
    {
      "labels":{"performance":"silver", "cost":"1"},
      "zone":"us-east-1d"
    }
  ]
}

```

Les définitions de classe de stockage suivantes font référence aux pools de stockage virtuels ci-dessus. À l'aide du `parameters.selector` Chaque classe de stockage indique quel(s) pool(s) virtuel(s) peut(s) être utilisé(s) pour héberger un volume. Les aspects définis dans le pool virtuel sélectionné seront définis pour le volume.

La première classe de stockage (`solidfire-gold-four`) sera mappé sur le premier pool de stockage virtuel. Il s'agit du seul pool offrant des performances Gold avec un `Volume Type QoS` De l'or. La dernière classe de stockage (`solidfire-silver`) appelle n'importe quel pool de stockage qui offre une performance silver. Astra Trident va décider du pool de stockage virtuel sélectionné et s'assurer que les besoins en stockage sont satisfaits.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-gold-four
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=gold; cost=4"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-three
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=3"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-bronze-two
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=bronze; cost=2"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver-one
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver; cost=1"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: solidfire-silver
provisioner: csi.trident.netapp.io
parameters:
  selector: "performance=silver"
  fsType: "ext4"

```

Trouvez plus d'informations

- ["Groupes d'accès de volume"](#)

Configurer un système back-end avec des pilotes ONTAP ou Cloud Volumes ONTAP SAN

Découvrez comment configurer un back-end ONTAP avec les pilotes ONTAP et Cloud Volumes ONTAP SAN.

- ["Préparation"](#)
- ["Configuration et exemples"](#)

Autorisations utilisateur

Astra Trident devrait être exécuté en tant qu'administrateur de ONTAP ou du SVM, généralement à l'aide du `admin` utilisateur du cluster ou un `vsadmin` Utilisateur d'un SVM ou un utilisateur avec un autre nom qui a le même rôle. Pour les déploiements Amazon FSX pour NetApp ONTAP, Astra Trident devrait être exécuté en tant qu'administrateur ONTAP ou SVM, à l'aide du cluster `fsxadmin` utilisateur ou un `vsadmin` Utilisateur d'un SVM ou un utilisateur avec un autre nom qui a le même rôle. Le `fsxadmin` l'utilisateur remplace limitée l'utilisateur administrateur du cluster.



Si vous utilisez le `limitAggregateUsage` paramètre, des autorisations d'administration du cluster sont requises. Avec Amazon FSX pour NetApp ONTAP avec Astra Trident, le `limitAggregateUsage` le paramètre ne fonctionne pas avec le `vsadmin` et `fsxadmin` comptes d'utilisateur. L'opération de configuration échoue si vous spécifiez ce paramètre.

S'il est possible de créer un rôle plus restrictif au sein de ONTAP qu'un pilote Trident peut utiliser, nous ne le recommandons pas. La plupart des nouvelles versions de Trident appellent des API supplémentaires qui devront être prises en compte, ce qui complique les mises à niveau et risque d'erreurs.

Préparation

Découvrez comment vous préparer à configurer un système ONTAP backend avec les pilotes SAN ONTAP. Pour tous les systèmes back-end ONTAP, Astra Trident requiert au moins un agrégat affecté à la SVM.

N'oubliez pas que vous pouvez également exécuter plusieurs pilotes et créer des classes de stockage qui pointent vers l'un ou l'autre. Par exemple, vous pouvez configurer un `san-dev` classe qui utilise le `ontap-san` conducteur et a `san-default` classe qui utilise le `ontap-san-economy` une seule.

Tous vos nœuds workers Kubernetes doivent avoir installé les outils iSCSI appropriés. Voir ["ici"](#) pour en savoir plus.

Authentification

Astra Trident propose deux modes d'authentification d'un système back-end ONTAP.

- Basé sur les informations d'identification : nom d'utilisateur et mot de passe pour un utilisateur ONTAP disposant des autorisations requises. Il est recommandé d'utiliser un rôle de connexion de sécurité prédéfini, par exemple `admin` ou `vsadmin` Pour garantir une compatibilité maximale avec les versions ONTAP.
- Basé sur des certificats : Astra Trident peut également communiquer avec un cluster ONTAP à l'aide d'un

certificat installé sur le système back-end. Dans ce cas, la définition backend doit contenir des valeurs encodées Base64 du certificat client, de la clé et du certificat d'autorité de certification de confiance, le cas échéant (recommandé).

Les utilisateurs ont également la possibilité de mettre à jour les systèmes back-end existants, en choisissant de passer d'un système basé sur les identifiants à un système basé sur les certificats, et inversement. Si **les deux identifiants et certificats sont fournis**, Astra Trident utilisera par défaut les certificats tout en émettant un avertissement pour supprimer les identifiants de la définition du back-end.

Activer l'authentification basée sur les informations d'identification

Astra Trident nécessite les identifiants d'un administrateur SVM-scoped/cluster-scoped pour communiquer avec le ONTAP backend. Il est recommandé d'utiliser des rôles standard prédéfinis tels que `admin` ou `vsadmin`. Il est ainsi possible d'assurer une compatibilité avec les futures versions d'ONTAP et d'exposer les API de fonctionnalités à utiliser avec les futures versions d'Astra Trident. Un rôle de connexion de sécurité personnalisé peut être créé et utilisé avec Astra Trident, mais il n'est pas recommandé.

Voici un exemple de définition du back-end :

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret",
}
```

Gardez à l'esprit que la définition du back-end est le seul endroit où les informations d'identification sont stockées en texte brut. Une fois le système backend créé, les noms d'utilisateur/mots de passe sont codés avec Base64 et stockés sous forme de secrets Kubernetes. La création/la conversion d'un back-end est la seule étape qui nécessite la connaissance des informations d'identification. Il s'agit donc d'une opération uniquement administrative, qui doit être effectuée par l'administrateur Kubernetes/du stockage.

Activez l'authentification basée sur les certificats

Les systèmes back-end, nouveaux et existants, peuvent utiliser un certificat et communiquer avec le système back-end ONTAP. Trois paramètres sont requis dans la définition du back-end.

- `ClientCertificate` : valeur encodée en Base64 du certificat client.
- `ClientPrivateKey` : valeur encodée en Base64 de la clé privée associée.
- `TrustedCACertificate` : valeur encodée Base64 du certificat CA de confiance. Si vous utilisez une autorité de certification approuvée, ce paramètre doit être fourni. Ceci peut être ignoré si aucune autorité de certification approuvée n'est utilisée.

Un flux de travail type comprend les étapes suivantes.

Étapes

1. Générez un certificat client et une clé. Lors de la génération, définissez le nom commun (CN) sur l'utilisateur ONTAP pour qu'il s'authentifie.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=admin"
```

2. Ajoutez un certificat d'autorité de certification de confiance au cluster ONTAP. Il se peut déjà que l'administrateur de stockage gère cet espace. Ignorer si aucune autorité de certification approuvée n'est utilisée.

```
security certificate install -type server -cert-name <trusted-ca-cert-  
name> -vserver <vserver-name>  
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled  
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca  
<cert-authority>
```

3. Installez le certificat client et la clé (à partir de l'étape 1) sur le cluster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-  
name> -vserver <vserver-name>  
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. Vérifiez que le rôle de connexion de sécurité ONTAP est pris en charge cert methode d'authentification.

```
security login create -user-or-group-name admin -application ontapi  
-authentication-method cert  
security login create -user-or-group-name admin -application http  
-authentication-method cert
```

5. Testez l'authentification à l'aide d'un certificat généré. Remplacer <ONTAP Management LIF> et <vserver name> par Management LIF IP et SVM name.

```
curl -X POST -Lk https://<ONTAP-Management-  
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key  
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp  
xmlns="http://www.netapp.com/filer/admin" version="1.21"  
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Encodez le certificat, la clé et le certificat CA de confiance avec Base64.

```
base64 -w 0 k8senv.pem >> cert_base64
base64 -w 0 k8senv.key >> key_base64
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Créez le back-end à l'aide des valeurs obtenues à partir de l'étape précédente.

```
$ cat cert-backend.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "trustedCACertificate": "QNFinfO...SiqOyN",
  "storagePrefix": "myPrefix_"
}

$ tridentctl create backend -f cert-backend.json -n trident
+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |         0 |
+-----+-----+-----+-----+
+-----+-----+
```

Mettre à jour les méthodes d'authentification ou faire pivoter les informations d'identification

Vous pouvez mettre à jour un back-end existant pour utiliser une méthode d'authentification différente ou pour faire pivoter leurs informations d'identification. Cela fonctionne de deux manières : les systèmes back-end qui utilisent le nom d'utilisateur/mot de passe peuvent être mis à jour pour utiliser des certificats ; les systèmes back-end qui utilisent des certificats peuvent être mis à jour en fonction du nom d'utilisateur/mot de passe. Pour cela, utilisez une mise à jour `backend.json` fichier contenant les paramètres requis à exécuter `tridentctl backend update`.

```
$ cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "SanBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "secret",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
$ tridentctl update backend SanBackend -f cert-backend-updated.json -n
trident

+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| SanBackend | ontap-san      | 586b1cd5-8cf8-428d-a76c-2872713612c1 |
online |          9 |
+-----+-----+-----+-----+
+-----+-----+
```



Lors de la rotation des mots de passe, l'administrateur du stockage doit d'abord mettre à jour le mot de passe de l'utilisateur sur ONTAP. Cette opération est suivie d'une mise à jour du back-end. Lors de la rotation de certificats, plusieurs certificats peuvent être ajoutés à l'utilisateur. Le back-end est ensuite mis à jour pour utiliser le nouveau certificat, en suivant lequel l'ancien certificat peut être supprimé du cluster ONTAP.

La mise à jour d'un back-end n'interrompt pas l'accès aux volumes qui ont déjà été créés, et n'a aucun impact sur les connexions de volume effectuées après. Une mise à jour réussie indique qu'Astra Trident peut communiquer avec le système back-end ONTAP et gérer les opérations de volumes à venir.

Spécifiez les igroups

Astra Trident utilise des igroups pour contrôler l'accès aux volumes (LUN) qu'il provisionne. Dans le cas de la spécification des igroups pour un système back-end, les administrateurs ont deux options :

- Astra Trident peut créer et gérer automatiquement un groupe initiateur par système back-end. Si `igroupName` N'est pas inclus dans la définition du système back-end, Astra Trident crée un groupe initiateur nommé `trident-<backend-UUID>` Sur le SVM. Cela permet de s'assurer que chaque système back-end dispose d'un groupe initiateur dédié et de gérer l'ajout/la suppression automatiques d'IQN de nœud Kubernetes.

- Alternativement, les groupes pré-crées peuvent être fournis dans une définition de back-end. Pour ce faire, utilisez le `igroupName` paramètre config. Astra Trident ajoute/supprime des IQN de nœud Kubernetes au groupe initiateur préexistant.

Pour les systèmes back-end dont ils ont besoin `igroupName` défini, le `igroupName` peut être supprimé avec un `tridentctl backend update`. Pour bénéficier des groupes à manipulation automatique avec Astra Trident. L'accès aux volumes déjà rattachés aux charges de travail ne sera pas perturbé. Les futures connexions seront gérées à l'aide du groupe initiateur Astra Trident.



Dédier un groupe initiateur à chaque instance unique d'Astra Trident est une bonne pratique bénéfique pour l'administrateur Kubernetes et l'administrateur du stockage. CSI Trident automatise l'ajout et la suppression des IQN du nœud du cluster au groupe initiateur, ce qui simplifie considérablement sa gestion. Lorsque vous utilisez le même SVM sur tous les environnements Kubernetes (et avec des installations Trident d'Astra), un groupe initiateur dédié permet de s'assurer que les modifications apportées à un cluster Kubernetes n'influencent pas les groupes initiateurs associés à un autre. En outre, il est important de s'assurer que chaque nœud du cluster Kubernetes dispose d'un IQN unique. Comme mentionné ci-dessus, Astra Trident s'occupe automatiquement de l'ajout et de la suppression des IQN. La réutilisation d'IQN sur des hôtes peut entraîner des scénarios indésirables où les hôtes se confondent les uns avec les autres et où l'accès aux LUN est refusé.

Si Astra Trident est configuré pour fonctionner comme un provisionnement CSI, les IQN du nœud Kubernetes sont automatiquement ajoutés ou supprimés du groupe initiateur. Lorsque des nœuds sont ajoutés à un cluster Kubernetes, `trident-csi` DemonSet déploie un pod (`trident-csi-xxxxx`) sur les nœuds récemment ajoutés et enregistre les nouveaux nœuds sur lesquels il peut attacher des volumes. Les IQN du nœud sont également ajoutés au groupe initiateur du back-end. Un ensemble d'étapes similaire gère la suppression des IQN lorsque le(s) nœud(s) est cordeleted, drainé et supprimé de Kubernetes.

Si Astra Trident ne s'exécute pas comme un provisionnement CSI, le groupe initiateur doit être mis à jour manuellement pour contenir les IQN iSCSI de chaque nœud worker du cluster Kubernetes. Les IQN des nœuds qui rejoignent le cluster Kubernetes devront être ajoutés au groupe initiateur. De même, les IQN des nœuds qui sont supprimés du cluster Kubernetes doivent être supprimés du groupe initiateur.

Authentifier les connexions avec le protocole CHAP bidirectionnel

Astra Trident peut authentifier les sessions iSCSI avec le protocole CHAP bidirectionnel pour le `ontap-san` et `ontap-san-economy` pilotes. Pour cela, il faut activer `useCHAP` dans votre définition backend. Lorsqu'il est réglé sur `true`, Astra Trident configure la sécurité de l'initiateur par défaut du SVM en CHAP bidirectionnel et définit le nom d'utilisateur et les secrets du fichier backend. NetApp recommande d'utiliser le protocole CHAP bidirectionnel pour l'authentification des connexions. Voir l'exemple de configuration suivant :

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap_san_chap",
  "managementLIF": "192.168.0.135",
  "svm": "ontap_iscsi_svm",
  "useCHAP": true,
  "username": "vsadmin",
  "password": "FaKePaSsWoRd",
  "igroupName": "trident",
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
}
```



Le `useCHAP` Paramètre est une option booléenne qui ne peut être configurée qu'une seule fois. Elle est définie sur `FALSE` par défaut. Une fois la valeur `true` définie, vous ne pouvez pas la définir sur `false`.

En plus de `useCHAP=true`, le `chapInitiatorSecret`, `chapTargetInitiatorSecret`, `chapTargetUsername`, et `chapUsername` les champs doivent être inclus dans la définition back-end. Les secrets peuvent être modifiés après la création d'un back-end en cours d'exécution `tridentctl update`.

Comment cela fonctionne

Par réglage `useCHAP` À vrai dire, l'administrateur du stockage demande à Astra Trident de configurer le protocole CHAP sur le système back-end. Ceci inclut les éléments suivants :

- Configuration du protocole CHAP sur le SVM :
 - Si le type de sécurité de l'initiateur par défaut du SVM n'est pas défini (défini par défaut) **et** il n'y a pas de LUN préexistantes dans le volume, Astra Trident définit le type de sécurité par défaut sur CHAP Et procédez à la configuration de l'initiateur CHAP et du nom d'utilisateur cible et des secrets.
 - Si le SVM contient des LUN, Astra Trident n'active pas le protocole CHAP sur le SVM. Cela permet de garantir que l'accès aux LUN déjà présentes sur le SVM n'est pas restreint.
- Configuration de l'initiateur CHAP et du nom d'utilisateur cible et des secrets ; ces options doivent être spécifiées dans la configuration backend (comme indiqué ci-dessus).
- Gestion de l'ajout d'initiateurs au `igroupName` donné en arrière-plan. Si ce n'est pas spécifié, la valeur par défaut est `trident`.

Une fois le système back-end créé, Astra Trident crée un correspondant `tridentbackend` CRD et stocke les secrets et noms d'utilisateur CHAP sous forme de secrets Kubernetes. Tous les volumes persistants créés par Astra Trident sur ce back-end seront montés et rattachés au protocole CHAP.

Rotation des identifiants et mise à jour des systèmes back-end

Vous pouvez mettre à jour les informations d'identification CHAP en mettant à jour les paramètres CHAP dans

le `backend.json` fichier. Cela nécessitera la mise à jour des secrets CHAP et l'utilisation de `tridentctl update` pour refléter ces modifications.



Lors de la mise à jour des secrets CHAP pour un back-end, vous devez utiliser `tridentctl` pour mettre à jour le backend. Ne mettez pas à jour les identifiants du cluster de stockage via l'interface de ligne de commande/ONTAP car Astra Trident ne pourra pas détecter ces modifications.

```
$ cat backend-san.json
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap_san_chap",
  "managementLIF": "192.168.0.135",
  "svm": "ontap_iscsi_svm",
  "useCHAP": true,
  "username": "vsadmin",
  "password": "FaKePaSsWoRd",
  "igroupName": "trident",
  "chapInitiatorSecret": "cl9qxUpDaTeD",
  "chapTargetInitiatorSecret": "rqxigXgkeUpDaTeD",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
}
```

```
$ ./tridentctl update backend ontap_san_chap -f backend-san.json -n
trident
+-----+-----+-----+-----+
+-----+-----+
| NAME          | STORAGE DRIVER |          UUID          |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| ontap_san_chap | ontap-san      | aa458f3b-ad2d-4378-8a33-1a472ffbeb5c |
online | 7 |
+-----+-----+-----+-----+
+-----+-----+
```

Les connexions existantes ne seront pas affectées. Elles restent actives si les identifiants sont mis à jour par Astra Trident sur le SVM. Les nouvelles connexions utiliseront les informations d'identification mises à jour et les connexions existantes continuent de rester actives. La déconnexion et la reconnexion des anciens volumes persistants se traduront par l'utilisation des identifiants mis à jour.

Exemples et options de configuration

Découvrez comment créer et utiliser des pilotes SAN ONTAP avec votre installation d'Astra Trident. Cette section présente des exemples de configuration du back-end et des détails sur le mappage des systèmes

back-end aux classes de stockage.

Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	ontap-nas, ontap-nas-économie, ontap-nas-flexgroup, ontap-san », « ontap-san », « ontap-économie san »
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + dataLIF
managementLIF	Adresse IP d'un cluster ou d'une LIF de gestion SVM	« 10.0.0.1 », « [2001:1234:abcd::fefe] »
dataLIF	Adresse IP de la LIF de protocole. Utilisez des crochets pour IPv6. Ne peut pas être mis à jour une fois que vous l'avez défini	Dérivé par la SVM sauf spécification
useCHAP	Utiliser CHAP pour authentifier iSCSI pour les pilotes SAN ONTAP [Boolean]	faux
chapInitiatorSecret	Secret de l'initiateur CHAP. Requis si useCHAP=true	« »
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	« »
chapTargetInitiatorSecret	Secret de l'initiateur cible CHAP. Requis si useCHAP=true	« »
chapUsername	Nom d'utilisateur entrant. Requis si useCHAP=true	« »
chapTargetUsername	Nom d'utilisateur cible. Requis si useCHAP=true	« »
clientCertificate	Valeur encodée en Base64 du certificat client. Utilisé pour l'authentification par certificat	« »
clientPrivateKey	Valeur encodée en Base64 de la clé privée du client. Utilisé pour l'authentification par certificat	« »
trustedCACertificate	Valeur encodée en Base64 du certificat CA de confiance. Facultatif. Utilisé pour l'authentification par certificat	« »

Paramètre	Description	Valeur par défaut
username	Nom d'utilisateur pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants	« »
password	Mot de passe pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants	« »
svm	Serveur virtuel de stockage à utiliser	Dérivé d'un SVM managementLIF est spécifié
igroupName	Nom du groupe initiateur à utiliser pour les volumes SAN	Trident-<backend-UUID>
storagePrefix	Préfixe utilisé pour le provisionnement des nouveaux volumes dans la SVM. Ne peut pas être mis à jour une fois que vous l'avez défini	trident
limitAggregateUsage	Echec du provisionnement si l'utilisation est supérieure à ce pourcentage. Ne s'applique pas à Amazon FSX pour ONTAP	« » (non appliqué par défaut)
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur.	« » (non appliqué par défaut)
lunsPerFlexvol	Nombre maximal de LUN par FlexVol, doit être compris dans la plage [50, 200]	"100"
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, {"api":false, "méthode":true}	nul
useREST	Paramètre booléen pour utiliser les API REST de ONTAP. Aperçu technique	faux



useREST est fourni sous forme d'aperçu technique ** qui est recommandé pour les environnements de test et non pour les charges de travail de production. Lorsqu'il est réglé sur true, Astra Trident va utiliser les API REST de ONTAP pour communiquer avec le système back-end. Cette fonctionnalité requiert ONTAP 9.9 et versions ultérieures. En outre, le rôle de connexion ONTAP utilisé doit avoir accès au `ontap` client supplémentaire. Ceci est satisfait par le pré-défini `vsadmin` et `cluster-admin` rôles.

Pour communiquer avec le cluster ONTAP, vous devez fournir les paramètres d'authentification. Il peut s'agir du nom d'utilisateur/mot de passe d'une connexion de sécurité ou d'un certificat installé.



Si vous utilisez un système Amazon FSX pour le système back-end NetApp ONTAP, ne spécifiez pas le système `limitAggregateUsage` paramètre. Le `fsxadmin` et `vsadmin` Les rôles fournis par Amazon FSX pour NetApp ONTAP ne contiennent pas les autorisations d'accès requises pour récupérer l'utilisation des agrégats et le limiter via Astra Trident.



Ne pas utiliser `debugTraceFlags` à moins que vous ne soyez en mesure de déboguer et que vous ayez besoin d'un vidage détaillé des journaux.

Pour le `ontap-san` Pilotes, par défaut est d'utiliser toutes les adresses IP des LIF de données du SVM et d'utiliser le chemin d'accès multivoie iSCSI. Spécification d'une adresse IP pour la LIF de données pour le `ontap-san` les pilotes les obligent à désactiver le multichemin et à utiliser uniquement l'adresse spécifiée.



Lors de la création d'un back-end, n'oubliez pas que `dataLIF` et `storagePrefix` ne peut pas être modifié après sa création. Pour mettre à jour ces paramètres, vous devez créer un nouveau back-end.

`igroupName` Peut être défini sur un groupe initiateur déjà créé sur le cluster ONTAP. Si non spécifié, Astra Trident crée automatiquement un groupe initiateur nommé `trident-<back-end-UUID>`. Si l'on fournit un nom de partenaire prédéfini, NetApp recommande d'utiliser un groupe initiateur par cluster Kubernetes si le SVM doit être partagé entre les environnements. Cela est nécessaire pour qu'Astra Trident conserve automatiquement les ajouts/suppressions d'IQN.

Les systèmes back-end peuvent également avoir mis à jour les groupes initiateurs après leur création :

- Vous pouvez mettre à jour le nom de l'outil afin de désigner un nouveau groupe initiateur créé et géré sur la SVM en dehors d'Astra Trident.
- Le nom de l'utilisateur peut être omis. Dans ce cas, Astra Trident crée et gère automatiquement un groupe initiateur `trident-<back-end-UUID>`.

Dans les deux cas, les pièces jointes de volume continueront d'être accessibles. Les pièces jointes futures utilisent le groupe initiateur mis à jour. Cette mise à jour n'interrompt pas l'accès aux volumes présents sur le back-end.

Un nom de domaine complet (FQDN) peut être spécifié pour le `managementLIF` option.

``managementLIF`` Pour tous les pilotes ONTAP peuvent également être définis sur des adresses IPv6. Veillez à installer Trident avec le ``--use-ipv6`` drapeau. Il faut veiller à définir ``managementLIF`` Adresse IPv6 entre crochets.



Lorsque vous utilisez des adresses IPv6, assurez-vous de `managementLIF` et `dataLIF` (si inclus dans votre définition de back-end) sont définis entre crochets, tels que `[28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]`. Si `dataLIF` N'est pas fourni, Astra Trident va récupérer les LIF de données IPv6 à partir du SVM.

Pour activer les pilotes `ontap-san` à l'aide du protocole CHAP, définissez la `useCHAP` paramètre à `true` dans votre définition de back-end. Astra Trident configure ensuite et utilise le protocole CHAP bidirectionnel comme authentification par défaut pour la SVM donnée en back-end. Voir "[ici](#)" pour en savoir plus sur son fonctionnement.

Pour le `ontap-san-economy` conducteur, le `limitVolumeSize` Elle limite également la taille maximale des volumes qu'elle gère pour les qtrees et les LUN.



Astra Trident définit les libellés de provisionnement dans le champ « Commentaires » de tous les volumes créés à l'aide de l' `ontap-san` conducteur. Pour chaque volume créé, le champ « Commentaires » de la FlexVol est rempli avec toutes les étiquettes présentes sur le pool de stockage dans lequel elle est placée. Les administrateurs de stockage peuvent définir des étiquettes par pool de stockage et regrouper tous les volumes créés dans un pool de stockage. Cela permet de différencier facilement les volumes en fonction d'un ensemble d'étiquettes personnalisables fournies dans la configuration back-end.

Options de configuration back-end pour les volumes de provisionnement

Vous pouvez contrôler la façon dont chaque volume est provisionné par défaut à l'aide de ces options dans une section spéciale de la configuration. Pour un exemple, voir les exemples de configuration ci-dessous.

Paramètre	Description	Valeur par défaut
<code>spaceAllocation</code>	Allocation d'espace pour les LUN	« vrai »
<code>spaceReserve</code>	Mode de réservation d'espace ; “none” (fin) ou “volume” (épais)	« aucun »
<code>snapshotPolicy</code>	Règle Snapshot à utiliser	« aucun »
<code>qosPolicy</code>	QoS policy group à affecter pour les volumes créés. Choisissez une de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> par pool de stockage/back-end	« »
<code>adaptiveQosPolicy</code>	Groupe de règles de QoS adaptative à attribuer aux volumes créés. Choisissez une de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> par pool de stockage/back-end	« »
<code>snapshotReserve</code>	Pourcentage du volume réservé pour les instantanés “0”	Si <code>snapshotPolicy</code> est « aucun », sinon « »
<code>splitOnClone</code>	Séparer un clone de son parent lors de sa création	« faux »
<code>splitOnClone</code>	Séparer un clone de son parent lors de sa création	« faux »
<code>encryption</code>	Activer le chiffrement de volume NetApp	« faux »
<code>securityStyle</code>	Style de sécurité pour les nouveaux volumes	“unix”
<code>tieringPolicy</code>	La stratégie de hiérarchisation à utiliser « none »	Snapshot uniquement pour une configuration SVM-DR pré-ONTAP 9.5



Avec Astra Trident, les groupes de règles de QoS doivent être utilisés avec ONTAP 9.8 ou version ultérieure. Il est recommandé d'utiliser un groupe de règles de qualité de service non partagé et de s'assurer que le groupe de règles est appliqué à chaque composant individuellement. Un groupe de règles de QoS partagé appliquera le plafond du débit total de toutes les charges de travail.

Voici un exemple avec des valeurs par défaut définies :

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password",
  "labels": {"k8scluster": "dev2", "backend": "dev2-sanbackend"},
  "storagePrefix": "alternate-trident",
  "igroupName": "custom",
  "debugTraceFlags": {"api":false, "method":true},
  "defaults": {
    "spaceReserve": "volume",
    "qosPolicy": "standard",
    "spaceAllocation": "false",
    "snapshotPolicy": "default",
    "snapshotReserve": "10"
  }
}
```



Pour tous les volumes créés à l'aide de `ontap-san` Avec d'autres pilotes, Astra Trident ajoute une capacité supplémentaire de 10 % au système FlexVol pour prendre en charge les métadonnées de LUN. La LUN sera provisionnée avec la taille exacte que l'utilisateur demande dans la demande de volume persistant. Astra Trident ajoute 10 % au système FlexVol (dont la taille disponible dans ONTAP). Les utilisateurs obtiennent à présent la capacité utilisable requise. Cette modification empêche également que les LUN ne soient en lecture seule, à moins que l'espace disponible soit pleinement utilisé. Cela ne s'applique pas à l'économie d'`ontap-san`.

Pour les systèmes back-end définis `snapshotReserve`, Astra Trident calcule la taille des volumes comme suit :

```
Total volume size = [(PVC requested size) / (1 - (snapshotReserve
percentage) / 100)] * 1.1
```

Le modèle 1.1 est le modèle 10 % d'Astra Trident supplémentaire qui s'ajoute à la baie FlexVol pour prendre en charge les métadonnées de la LUN. Pour `snapshotReserve` = 5 % et demande de volume persistant = 5

Gio, la taille totale du volume est de 5,7 Gio et la taille disponible est de 5,5 Gio. Le volume `show` la commande doit afficher des résultats similaires à cet exemple :

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e42ec6fe_3baa_4af6_996d_134adbbb8e6d	online	RW	5.79GB	5.50GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

3 entries were displayed.

Actuellement, le redimensionnement est le seul moyen d'utiliser le nouveau calcul pour un volume existant.

Exemples de configuration minimaux

Les exemples suivants montrent des configurations de base qui laissent la plupart des paramètres par défaut. C'est la façon la plus simple de définir un back-end.



Si vous utilisez Amazon FSX sur NetApp ONTAP avec Astra Trident, il est recommandé de spécifier des noms DNS pour les LIF au lieu d'adresses IP.

ontap-san pilote avec authentification par certificat

Il s'agit d'un exemple de configuration back-end minimal. `clientCertificate`, `clientPrivateKey`, et `trustedCACertificate` (Facultatif, si vous utilisez une autorité de certification approuvée) est renseigné `backend.json` Et prendre les valeurs codées en base64 du certificat client, de la clé privée et du certificat CA de confiance, respectivement.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "DefaultSANBackend",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz"
}
```

Il s'agit d'un exemple de configuration back-end minimal. Cette configuration de base crée un ontap-san backend avec useCHAP réglé sur true.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "labels": {"k8scluster": "test-cluster-1", "backend": "testcluster1-
sanbackend"},
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret"
}
```

```
{
  "version": 1,
  "storageDriverName": "ontap-san-economy",
  "managementLIF": "10.0.0.1",
  "svm": "svm_iscsi_eco",
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret"
}
```

Exemples de systèmes back-end avec pools de stockage virtuel

Dans l'exemple de fichier de définition backend ci-dessous, des valeurs par défaut spécifiques sont définies pour tous les pools de stockage, par exemple spaceReserve aucune, spaceAllocation lors de la fausse idée, et encryption faux. Les pools de stockage virtuels sont définis dans la section stockage.

Dans cet exemple, certains pools de stockage sont propriétaires de leur propre pool `spaceReserve`, `spaceAllocation`, et `encryption` les valeurs et certains pools remplacent les valeurs par défaut définies ci-dessus.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.3",
  "svm": "svm_iscsi",
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret",

  "defaults": {
    "spaceAllocation": "false",
    "encryption": "false",
    "qosPolicy": "standard"
  },
  "labels": {"store": "san_store", "kubernetes-cluster": "prod-cluster-1"},
  "region": "us_east_1",
  "storage": [
    {
      "labels": {"protection": "gold", "creditpoints": "40000"},
      "zone": "us_east_1a",
      "defaults": {
        "spaceAllocation": "true",
        "encryption": "true",
        "adaptiveQosPolicy": "adaptive-extreme"
      }
    },
    {
      "labels": {"protection": "silver", "creditpoints": "20000"},
      "zone": "us_east_1b",
      "defaults": {
        "spaceAllocation": "false",
        "encryption": "true",
        "qosPolicy": "premium"
      }
    }
  ],
}
```

```

    {
      "labels":{"protection":"bronze", "creditpoints":"5000"},
      "zone":"us_east_1c",
      "defaults": {
        "spaceAllocation": "true",
        "encryption": "false"
      }
    }
  ]
}

```

Voici un exemple iSCSI pour le `ontap-san-economy` pilote :

```

{
  "version": 1,
  "storageDriverName": "ontap-san-economy",
  "managementLIF": "10.0.0.1",
  "svm": "svm_iscsi_eco",
  "useCHAP": true,
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",
  "chapTargetUsername": "iJF4heBRT0TCwxyz",
  "chapUsername": "uh2aNCLSD6cNwxyz",
  "igroupName": "trident",
  "username": "vsadmin",
  "password": "secret",

  "defaults": {
    "spaceAllocation": "false",
    "encryption": "false"
  },
  "labels":{"store":"san_economy_store"},
  "region": "us_east_1",
  "storage": [
    {
      "labels":{"app":"oracledb", "cost":"30"},
      "zone":"us_east_1a",
      "defaults": {
        "spaceAllocation": "true",
        "encryption": "true"
      }
    },
    {
      "labels":{"app":"postgresdb", "cost":"20"},
      "zone":"us_east_1b",

```

```

        "defaults": {
            "spaceAllocation": "false",
            "encryption": "true"
        },
        {
            "labels": {"app": "mysqldb", "cost": "10"},
            "zone": "us_east_1c",
            "defaults": {
                "spaceAllocation": "true",
                "encryption": "false"
            }
        }
    ]
}

```

Mappage des systèmes back-end aux classes de stockage

Les définitions de classe de stockage suivantes font référence aux pools de stockage virtuels ci-dessus. À l'aide du `parameters.selector` Chaque classe de stockage indique quel(s) pool(s) virtuel(s) peut(s) être utilisé(s) pour héberger un volume. Les aspects définis dans le pool virtuel sélectionné seront définis pour le volume.

- La première classe de stockage (`protection-gold`) sera mappé sur le premier, deuxième pool de stockage virtuel dans le `ontap-nas-flexgroup` système back-end et le premier pool de stockage virtuel dans `ontap-san` back-end. Il s'agit du seul pool offrant une protection de niveau Gold.
- La deuxième classe de stockage (`protection-not-gold`) sera mappé sur le troisième, quatrième pool de stockage virtuel dans `ontap-nas-flexgroup` back-end et le deuxième, troisième pool de stockage virtuel dans `ontap-san` back-end. Ce sont les seuls pools offrant un niveau de protection autre que l'or.
- La troisième classe de stockage (`app-mysqldb`) sera mappé sur le quatrième pool de stockage virtuel dans `ontap-nas` back-end et le troisième pool de stockage virtuel dans `ontap-san-economy` back-end. Ce sont les seuls pools offrant une configuration de pool de stockage pour l'application de type `mysqldb`.
- La quatrième classe de stockage (`protection-silver-creditpoints-20k`) sera mappé sur le troisième pool de stockage virtuel dans `ontap-nas-flexgroup` back-end et le second pool de stockage virtuel dans `ontap-san` back-end. Ce sont les seules piscines offrant une protection de niveau or à 20000 points de solvabilité.
- La cinquième classe de stockage (`creditpoints-5k`) sera mappé sur le second pool de stockage virtuel dans `ontap-nas-economy` back-end et le troisième pool de stockage virtuel dans `ontap-san` back-end. Ce sont les seules offres de piscine à 5000 points de solvabilité.

Astra Trident va décider du pool de stockage virtuel sélectionné et s'assurer que les besoins en stockage sont satisfaits.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: netapp.io/trident
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

Configurer un système back-end avec les pilotes NAS ONTAP

Découvrez comment configurer un back-end ONTAP avec les pilotes ONTAP et NAS Cloud Volumes ONTAP.

- ["Préparation"](#)
- ["Configuration et exemples"](#)

Autorisations utilisateur

Astra Trident devrait être exécuté en tant qu'administrateur de ONTAP ou du SVM, généralement à l'aide du `admin` utilisateur du cluster ou un `vsadmin` Utilisateur d'un SVM ou un utilisateur avec un autre nom qui a le même rôle. Pour les déploiements Amazon FSX pour NetApp ONTAP, Astra Trident devrait être exécuté en tant qu'administrateur ONTAP ou SVM, à l'aide du cluster `fsxadmin` utilisateur ou un `vsadmin` Utilisateur d'un SVM ou un utilisateur avec un autre nom qui a le même rôle. Le `fsxadmin` l'utilisateur remplace limitée l'utilisateur administrateur du cluster.



Si vous utilisez le `limitAggregateUsage` paramètre, des autorisations d'administration du cluster sont requises. Avec Amazon FSX pour NetApp ONTAP avec Astra Trident, le `limitAggregateUsage` le paramètre ne fonctionne pas avec le `vsadmin` et `fsxadmin` comptes d'utilisateur. L'opération de configuration échoue si vous spécifiez ce paramètre.

S'il est possible de créer un rôle plus restrictif au sein de ONTAP qu'un pilote Trident peut utiliser, nous ne le recommandons pas. La plupart des nouvelles versions de Trident appellent des API supplémentaires qui devront être prises en compte, ce qui complique les mises à niveau et risque d'erreurs.

Préparation

Découvrez comment vous préparer à configurer un back-end ONTAP avec les pilotes NAS ONTAP. Pour tous les systèmes back-end ONTAP, Astra Trident requiert au moins un agrégat affecté à la SVM.

Pour tous les systèmes back-end ONTAP, Astra Trident requiert au moins un agrégat affecté à la SVM.

N'oubliez pas que vous pouvez également exécuter plusieurs pilotes et créer des classes de stockage qui pointent vers l'un ou l'autre. Par exemple, vous pouvez configurer une classe Gold qui utilise le `ontap-nas` Pilote et une classe Bronze qui utilise le `ontap-nas-economy` une seule.

Tous vos nœuds workers Kubernetes doivent avoir installé les outils NFS appropriés. Voir ["ici"](#) pour en savoir plus.

Authentification

Astra Trident propose deux modes d'authentification d'un système back-end ONTAP.

- Basé sur les informations d'identification : nom d'utilisateur et mot de passe pour un utilisateur ONTAP disposant des autorisations requises. Il est recommandé d'utiliser un rôle de connexion de sécurité prédéfini, par exemple `admin` ou `vsadmin` Pour garantir une compatibilité maximale avec les versions ONTAP.
- Basé sur des certificats : Astra Trident peut également communiquer avec un cluster ONTAP à l'aide d'un certificat installé sur le système back-end. Dans ce cas, la définition backend doit contenir des valeurs encodées Base64 du certificat client, de la clé et du certificat d'autorité de certification de confiance, le cas échéant (recommandé).

Les utilisateurs ont également la possibilité de mettre à jour les systèmes back-end existants, en choisissant de passer d'un système basé sur les identifiants à un système basé sur les certificats, et inversement. Si **les deux identifiants et certificats sont fournis**, Astra Trident utilisera par défaut les certificats tout en émettant un avertissement pour supprimer les identifiants de la définition du back-end.

Activer l'authentification basée sur les informations d'identification

Astra Trident nécessite les identifiants d'un administrateur SVM-scoped/cluster-scoped pour communiquer avec le ONTAP backend. Il est recommandé d'utiliser des rôles standard prédéfinis tels que `admin` ou `vsadmin`. Il est ainsi possible d'assurer une compatibilité avec les futures versions d'ONTAP et d'exposer les API de fonctionnalités à utiliser avec les futures versions d'Astra Trident. Un rôle de connexion de sécurité personnalisé peut être créé et utilisé avec Astra Trident, mais il n'est pas recommandé.

Voici un exemple de définition du back-end :

```
{
  "version": 1,
  "backendName": "ExampleBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret"
}
```

Gardez à l'esprit que la définition du back-end est le seul endroit où les informations d'identification sont stockées en texte brut. Une fois le système backend créé, les noms d'utilisateur/mots de passe sont codés avec Base64 et stockés sous forme de secrets Kubernetes. La création/la conversion d'un back-end est la seule étape qui nécessite la connaissance des informations d'identification. Il s'agit donc d'une opération uniquement administrative, qui doit être effectuée par l'administrateur Kubernetes/du stockage.

Activez l'authentification basée sur les certificats

Les systèmes back-end, nouveaux et existants, peuvent utiliser un certificat et communiquer avec le système back-end ONTAP. Trois paramètres sont requis dans la définition du back-end.

- `ClientCertificate` : valeur encodée en Base64 du certificat client.
- `ClientPrivateKey` : valeur encodée en Base64 de la clé privée associée.
- `TrustedCACertificate` : valeur encodée Base64 du certificat CA de confiance. Si vous utilisez une autorité de certification approuvée, ce paramètre doit être fourni. Ceci peut être ignoré si aucune autorité de certification approuvée n'est utilisée.

Un flux de travail type comprend les étapes suivantes.

Étapes

1. Générez un certificat client et une clé. Lors de la génération, définissez le nom commun (CN) sur l'utilisateur ONTAP pour qu'il s'authentifie.


```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout k8senv.key  
-out k8senv.pem -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=vsadmin"
```

2. Ajoutez un certificat d'autorité de certification de confiance au cluster ONTAP. Il se peut déjà que l'administrateur de stockage gère cet espace. Ignorer si aucune autorité de certification approuvée n'est utilisée.

```
security certificate install -type server -cert-name <trusted-ca-cert-  
name> -vserver <vserver-name>  
ssl modify -vserver <vserver-name> -server-enabled true -client-enabled  
true -common-name <common-name> -serial <SN-from-trusted-CA-cert> -ca  
<cert-authority>
```

3. Installez le certificat client et la clé (à partir de l'étape 1) sur le cluster ONTAP.

```
security certificate install -type client-ca -cert-name <certificate-  
name> -vserver <vserver-name>  
security ssl modify -vserver <vserver-name> -client-enabled true
```

4. Vérifiez que le rôle de connexion de sécurité ONTAP est pris en charge cert methode d'authentification.

```
security login create -user-or-group-name vsadmin -application ontapi  
-authentication-method cert -vserver <vserver-name>  
security login create -user-or-group-name vsadmin -application http  
-authentication-method cert -vserver <vserver-name>
```

5. Testez l'authentification à l'aide d'un certificat généré. Remplacer <ONTAP Management LIF> et <vserver name> par Management LIF IP et SVM name. Vous devez vous assurer que le LIF a sa politique de service définie sur default-data-management.

```
curl -X POST -Lk https://<ONTAP-Management-  
LIF>/servlets/netapp.servlets.admin.XMLrequest_filer --key k8senv.key  
--cert ~/k8senv.pem -d '<?xml version="1.0" encoding="UTF-8"?><netapp  
xmlns="http://www.netapp.com/filer/admin" version="1.21"  
vfiler="<vserver-name>"><vserver-get></vserver-get></netapp>'
```

6. Encodez le certificat, la clé et le certificat CA de confiance avec Base64.

```
base64 -w 0 k8senv.pem >> cert_base64  
base64 -w 0 k8senv.key >> key_base64  
base64 -w 0 trustedca.pem >> trustedca_base64
```

7. Créez le back-end à l'aide des valeurs obtenues à partir de l'étape précédente.

```
$ cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "clientCertificate": "Faaaakkkkeeee...Vaaalllluuuuueeee",
  "clientPrivateKey": "LS0tFaKE...0VaLuES0tLS0K",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
$ tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident
+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                UUID                |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |          9 |
+-----+-----+-----+-----+
+-----+-----+
```

Mettre à jour les méthodes d'authentification ou faire pivoter les informations d'identification

Vous pouvez mettre à jour un back-end existant pour utiliser une méthode d'authentification différente ou pour faire pivoter leurs informations d'identification. Cela fonctionne de deux manières : les systèmes back-end qui utilisent le nom d'utilisateur/mot de passe peuvent être mis à jour pour utiliser des certificats ; les systèmes back-end qui utilisent des certificats peuvent être mis à jour en fonction du nom d'utilisateur/mot de passe. Pour cela, utilisez une mise à jour `backend.json` fichier contenant les paramètres requis à exécuter `tridentctl backend update`.

```
$ cat cert-backend-updated.json
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "NasBackend",
  "managementLIF": "1.2.3.4",
  "dataLIF": "1.2.3.8",
  "svm": "vserver_test",
  "username": "vsadmin",
  "password": "secret",
  "storagePrefix": "myPrefix_"
}

#Update backend with tridentctl
$ tridentctl update backend NasBackend -f cert-backend-updated.json -n
trident

+-----+-----+-----+-----+
+-----+-----+
|      NAME      | STORAGE DRIVER |                      UUID                      |
STATE | VOLUMES |
+-----+-----+-----+-----+
+-----+-----+
| NasBackend | ontap-nas      | 98e19b74-aec7-4a3d-8dcf-128e5033b214 |
online |          9 |
+-----+-----+-----+-----+
+-----+-----+
```



Lors de la rotation des mots de passe, l'administrateur du stockage doit d'abord mettre à jour le mot de passe de l'utilisateur sur ONTAP. Cette opération est suivie d'une mise à jour du back-end. Lors de la rotation de certificats, plusieurs certificats peuvent être ajoutés à l'utilisateur. Le back-end est ensuite mis à jour pour utiliser le nouveau certificat, en suivant lequel l'ancien certificat peut être supprimé du cluster ONTAP.

La mise à jour d'un back-end n'interrompt pas l'accès aux volumes qui ont déjà été créés, et n'a aucun impact sur les connexions de volume effectuées après. Une mise à jour réussie indique qu'Astra Trident peut communiquer avec le système back-end ONTAP et gérer les opérations de volumes à venir.

Gestion des règles d'exportation NFS

Astra Trident utilise les règles d'exportation NFS pour contrôler l'accès aux volumes qu'il provisionne.

Astra Trident propose deux options pour l'utilisation des règles d'exportation :

- Astra Trident peut gérer la règle d'exportation de manière dynamique. Dans ce mode de fonctionnement, l'administrateur du stockage spécifie une liste de blocs CIDR qui représentent les adresses IP admissibles. Astra Trident ajoute automatiquement des adresses IP de nœud qui font partie de ces plages à la règle d'exportation. En outre, lorsqu'aucun CIDRS n'est spécifié, toute adresse IP unicast globale trouvée sur les nœuds est ajoutée à la règle d'exportation.

- Les administrateurs du stockage peuvent créer une export-policy et ajouter des règles manuellement. Astra Trident utilise la export policy par défaut, sauf si un nom différent de export policy est spécifié dans la configuration.

Gérez les règles d'exportation de manière dynamique

La version 20.04 de CSI Trident permet de gérer de manière dynamique les règles d'exportation pour les systèmes back-end ONTAP. Cela permet à l'administrateur du stockage de spécifier un espace d'adresse autorisé pour les adresses IP du nœud de travail, au lieu de définir manuellement des règles explicites. Il simplifie considérablement la gestion des export policy ; les modifications apportées à l'export policy ne nécessitent plus d'intervention manuelle sur le cluster de stockage. De plus, cela limite l'accès au cluster de stockage uniquement aux nœuds workers dont les adresses IP sont comprises dans la plage spécifiée, ce qui permet une gestion automatisée et précise.



La gestion dynamique des règles d'exportation n'est disponible que pour CSI Trident. Il est important de s'assurer que les nœuds de travail ne sont pas NATed.

Exemple

Deux options de configuration doivent être utilisées. Voici un exemple de définition du backend :

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap_nas_auto_export",
  "managementLIF": "192.168.0.135",
  "svm": "svm1",
  "username": "vsadmin",
  "password": "FaKePaSsWoRd",
  "autoExportCIDRs": ["192.168.0.0/24"],
  "autoExportPolicy": true
}
```



Lorsque vous utilisez cette fonctionnalité, vous devez vous assurer que la jonction root de votre SVM possède une export policy préétablie avec une règle d'exportation qui permet le bloc CIDR du nœud (comme la export policy par défaut). Suivez toujours la meilleure pratique recommandée par NetApp pour dédier un SVM à Astra Trident.

Voici une explication du fonctionnement de cette fonction à l'aide de l'exemple ci-dessus :

- `autoExportPolicy` est défini sur `true`. Cela signifie qu'Astra Trident va créer une export policy pour le `svm1` SVM et gère l'ajout et la suppression de règles à l'aide de `autoExportCIDRs` blocs d'adresse. Par exemple, un backend avec UUID `403b5326-8482-40db-96d0-d83fb3f4daec` et `autoExportPolicy` réglé sur `true` crée une export-policy nommée `trident-403b5326-8482-40db-96d0-d83fb3f4daec` Sur le SVM.
- `autoExportCIDRs` contient une liste de blocs d'adresses. Ce champ est facultatif et il prend par défaut la valeur `["0.0.0.0/0", "::0"]`. S'il n'est pas défini, Astra Trident ajoute toutes les adresses de diffusion individuelle à périmètre global présentes sur les nœuds du worker.

Dans cet exemple, le 192.168.0.0/24 l'espace d'adressage est fourni. Cela indique que les adresses IP des nœuds Kubernetes qui appartiennent à cette plage d'adresse seront ajoutées à la règle d'exportation créée par Astra Trident. Lorsque Astra Trident enregistre un nœud sur lequel il s'exécute, il récupère les adresses IP du nœud et les vérifie par rapport aux blocs d'adresse fournis dans `autoExportCIDRs`. Après avoir filtrage les adresses IP, Astra Trident crée des règles de politique d'exportation pour les adresses IP clientes qu'il détecte, avec une règle pour chaque nœud qu'il identifie.

Vous pouvez mettre à jour `autoExportPolicy` et `autoExportCIDRs` pour les systèmes back-end après leur création. Vous pouvez ajouter de nouveaux rapports CIDR pour un back-end qui est géré automatiquement ou supprimé des rapports CIDR existants. Faites preuve de prudence lors de la suppression des CIDR pour vous assurer que les connexions existantes ne sont pas tombées. Vous pouvez également choisir de désactiver `autoExportPolicy` pour un back-end et revient à une export policy créée manuellement. Pour ce faire, vous devrez définir le `exportPolicy` dans votre configuration backend.

Après la création ou la mise à jour d'Astra Trident, vous pouvez vérifier le système back-end à l'aide de `tridentctl` ou le correspondant `tridentbackend` CRD :

```
$ ./tridentctl get backends ontap_nas_auto_export -n trident -o yaml
items:
- backendUUID: 403b5326-8482-40db-96d0-d83fb3f4daec
  config:
    aggregate: ""
    autoExportCIDRs:
    - 192.168.0.0/24
    autoExportPolicy: true
    backendName: ontap_nas_auto_export
    chapInitiatorSecret: ""
    chapTargetInitiatorSecret: ""
    chapTargetUsername: ""
    chapUsername: ""
    dataLIF: 192.168.0.135
    debug: false
    debugTraceFlags: null
    defaults:
      encryption: "false"
      exportPolicy: <automatic>
      fileType: ext4
```

Lorsque des nœuds sont ajoutés à un cluster Kubernetes et enregistrés avec le contrôleur Trident Astra, les règles d'exportation des systèmes back-end existants sont mises à jour (à condition qu'elles tombent dans la plage d'adresse spécifiée dans la `autoExportCIDRs` pour le back-end).

Lorsqu'un nœud est retiré, Astra Trident vérifie tous les systèmes back-end en ligne afin de supprimer la règle d'accès du nœud. En supprimant cette IP de nœud des règles d'exportation des systèmes back-end gérés, Astra Trident empêche les montages erratiques, à moins que cette adresse IP soit réutilisée par un nouveau nœud du cluster.

Pour les systèmes back-end existants, mise à jour du système back-end avec `tridentctl update backend` S'assure qu'Astra Trident gère automatiquement les règles d'exportation. Cela créera une nouvelle

export policy nommée après l'UUID et les volumes du backend qui sont présents sur le back-end, utilisera la export policy nouvellement créée lorsqu'ils sont de nouveau montés.



La suppression d'un back-end avec des règles d'exportation gérées automatiquement supprimera l'export policy créée de manière dynamique. Si le back-end est recréés, il est traité comme un nouveau backend et entraîne la création d'une nouvelle export policy.

Si l'adresse IP d'un nœud actif est mise à jour, vous devez redémarrer le pod Astra Trident sur le nœud. Astra Trident va ensuite mettre à jour la règle d'exportation pour les systèmes back-end qu'il gère pour tenir compte de ce changement d'IP.

Exemples et options de configuration

Découvrez comment créer et utiliser des pilotes NAS ONTAP avec votre installation d'Astra Trident. Cette section présente des exemples de configuration du back-end et des détails sur le mappage des systèmes back-end aux classes de stockage.

Options de configuration du back-end

Voir le tableau suivant pour les options de configuration du back-end :

Paramètre	Description	Valeur par défaut
version		Toujours 1
storageDriverName	Nom du pilote de stockage	ontap-nas, ontap-nas-économie, ontap-nas-flexgroup, ontap-san », « ontap-san », « ontap-économie san »
backendName	Nom personnalisé ou système back-end de stockage	Nom du pilote + "_" + dataLIF
managementLIF	Adresse IP d'un cluster ou d'une LIF de gestion SVM	« 10.0.0.1 », « [2001:1234:abcd::fefe] »
dataLIF	Adresse IP de la LIF de protocole. Utilisez des crochets pour IPv6. Ne peut pas être mis à jour une fois que vous l'avez défini	Dérivé par la SVM sauf spécification
autoExportPolicy	Activer la création et la mise à jour automatiques des règles d'exportation [booléennes]	faux
autoExportCIDRs	Liste des CIDR pour filtrer les adresses IP du nœud Kubernetes par rapport à quand autoExportPolicy est activé	["0.0.0.0/0", "::/0"]
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	« »
clientCertificate	Valeur encodée en Base64 du certificat client. Utilisé pour l'authentification par certificat	« »

Paramètre	Description	Valeur par défaut
clientPrivateKey	Valeur encodée en Base64 de la clé privée du client. Utilisé pour l'authentification par certificat	« »
trustedCACertificate	Valeur encodée en Base64 du certificat CA de confiance. Facultatif. Utilisé pour l'authentification par certificat	« »
username	Nom d'utilisateur pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants	
password	Mot de passe pour la connexion au cluster/SVM. Utilisé pour l'authentification basée sur les identifiants	
svm	Serveur virtuel de stockage à utiliser	Dérivé d'un SVM managementLIF est spécifié
igroupName	Nom du groupe initiateur à utiliser pour les volumes SAN	Trident-<backend-UUID>
storagePrefix	Préfixe utilisé pour le provisionnement des nouveaux volumes dans la SVM. Ne peut pas être mis à jour une fois que vous l'avez défini	trident
limitAggregateUsage	Echec du provisionnement si l'utilisation est supérieure à ce pourcentage. Ne s'applique pas à Amazon FSX pour ONTAP	« » (non appliqué par défaut)
limitVolumeSize	Echec du provisionnement si la taille du volume demandé est supérieure à cette valeur.	« » (non appliqué par défaut)
lunsPerFlexvol	Nombre maximal de LUN par FlexVol, doit être compris dans la plage [50, 200]	"100"
debugTraceFlags	Indicateurs de débogage à utiliser lors du dépannage. Exemple, {"api":false, "méthode":true}	nul
nfsMountOptions	Liste des options de montage NFS séparée par des virgules	« »
qtreesPerFlexvol	Nombre maximal de qtrees par FlexVol, qui doit être compris dans la plage [50, 300]	"200"

Paramètre	Description	Valeur par défaut
useREST	Paramètre booléen pour utiliser les API REST de ONTAP. Aperçu technique	faux



useREST est fourni sous forme d'aperçu technique ** qui est recommandé pour les environnements de test et non pour les charges de travail de production. Lorsqu'il est réglé sur true, Astra Trident va utiliser les API REST de ONTAP pour communiquer avec le système back-end. Cette fonctionnalité requiert ONTAP 9.9 et versions ultérieures. En outre, le rôle de connexion ONTAP utilisé doit avoir accès au ontap client supplémentaire. Ceci est satisfait par le pré-défini vsadmin et cluster-admin rôles.

Pour communiquer avec le cluster ONTAP, vous devez fournir les paramètres d'authentification. Il peut s'agir du nom d'utilisateur/mot de passe d'une connexion de sécurité ou d'un certificat installé.



Si vous utilisez un système Amazon FSX pour le système back-end NetApp ONTAP, ne spécifiez pas le système limitAggregateUsage paramètre. Le fsxadmin et vsadmin Les rôles fournis par Amazon FSX pour NetApp ONTAP ne contiennent pas les autorisations d'accès requises pour récupérer l'utilisation des agrégats et le limiter via Astra Trident.



Ne pas utiliser debugTraceFlags à moins que vous ne soyez en mesure de déboguer et que vous ayez besoin d'un vidage détaillé des journaux.



Lors de la création d'un back-end, n'oubliez pas que le dataLIF et storagePrefix ne peut pas être modifié après sa création. Pour mettre à jour ces paramètres, vous devez créer un nouveau back-end.

Un nom de domaine complet (FQDN) peut être spécifié pour le managementLIF option. Un FQDN peut également être spécifié pour le dataLIF Option, dans ce cas, le FQDN sera utilisé pour les opérations de montage NFS. Cette méthode vous permet de créer un DNS cyclique pour équilibrer la charge entre plusieurs LIF de données.

```
`managementLIF` Pour tous les pilotes ONTAP peuvent également être définis sur des adresses IPv6. Veuillez à installer Astra Trident avec le `--use-ipv6` drapeau. Il faut veiller à définir le `managementLIF` Adresse IPv6 entre crochets.
```



Lorsque vous utilisez des adresses IPv6, assurez-vous de managementLIF et dataLIF (si inclus dans votre définition de back-end) sont définis entre crochets, tels que [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si dataLIF N'est pas fourni, Astra Trident va récupérer les LIF de données IPv6 à partir du SVM.

À l'aide du autoExportPolicy et autoExportCIDRs CSI Trident peut gérer automatiquement les règles d'exportation. Ceci est pris en charge pour tous les pilotes ontap-nas-.*.

Pour le ontap-nas-economy conducteur, le limitVolumeSize Elle restreindra également la taille maximale des volumes qu'elle gère pour les qtrees et les LUN, ainsi que qtreesPerFlexvol L'option permet

de personnaliser le nombre maximal de qtrees par FlexVol.

Le `nfsMountOptions` ce paramètre peut être utilisé pour spécifier les options de montage. Les options de montage des volumes persistants Kubernetes sont généralement spécifiées dans les classes de stockage, mais si aucune option de montage n'est spécifiée dans une classe de stockage, Astra Trident utilisera les options de montage spécifiées dans le fichier de configuration du système de stockage back-end. Si aucune option de montage n'est spécifiée dans la classe de stockage ou le fichier de configuration, Astra Trident ne définit aucune option de montage sur un volume persistant associé.



Astra Trident définit les libellés de provisionnement dans le champ « Commentaires » de tous les volumes créés à l'aide de `(ontap-nas et(ontap-nas-flexgroup`. En fonction du pilote utilisé, les commentaires sont définis sur le FlexVol (`ontap-nas`) Ou FlexGroup (`ontap-nas-flexgroup`). Astra Trident copiera toutes les étiquettes présentes sur un pool de stockage sur le volume de stockage au moment de son provisionnement. Les administrateurs de stockage peuvent définir des étiquettes par pool de stockage et regrouper tous les volumes créés dans un pool de stockage. Cela permet de différencier facilement les volumes en fonction d'un ensemble d'étiquettes personnalisables fournies dans la configuration back-end.

Options de configuration back-end pour les volumes de provisionnement

Vous pouvez contrôler la façon dont chaque volume est provisionné par défaut à l'aide de ces options dans une section spéciale de la configuration. Pour un exemple, voir les exemples de configuration ci-dessous.

Paramètre	Description	Valeur par défaut
<code>spaceAllocation</code>	Allocation d'espace pour les LUN	« vrai »
<code>spaceReserve</code>	Mode de réservation d'espace ; "none" (fin) ou "volume" (épais)	« aucun »
<code>snapshotPolicy</code>	Règle Snapshot à utiliser	« aucun »
<code>qosPolicy</code>	QoS policy group à affecter pour les volumes créés. Choisissez une de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> par pool de stockage/back-end	« »
<code>adaptiveQosPolicy</code>	Groupe de règles de QoS adaptative à attribuer aux volumes créés. Choisissez une de <code>qosPolicy</code> ou <code>adaptiveQosPolicy</code> par pool de stockage/back-end. Non pris en charge par l'économie <code>ontap-nas</code> .	« »
<code>snapshotReserve</code>	Pourcentage du volume réservé pour les instantanés "0"	Si <code>snapshotPolicy</code> est « aucun », sinon « »
<code>splitOnClone</code>	Séparer un clone de son parent lors de sa création	« faux »
<code>encryption</code>	Activer le chiffrement de volume NetApp	« faux »
<code>securityStyle</code>	Style de sécurité pour les nouveaux volumes	"unix"

Paramètre	Description	Valeur par défaut
tieringPolicy	La stratégie de hiérarchisation à utiliser « none »	Snapshot uniquement pour une configuration SVM-DR pré-ONTAP 9.5
Autorisations unix	Mode pour les nouveaux volumes	"777"
Dir. Des snapshots	Contrôle la visibilité du .snapshot répertoire	« faux »
ExportPolicy	Export policy à utiliser	« par défaut »
SecurityStyle	Style de sécurité pour les nouveaux volumes	"unix"



Avec Astra Trident, les groupes de règles de QoS doivent être utilisés avec ONTAP 9.8 ou version ultérieure. Il est recommandé d'utiliser un groupe de règles de qualité de service non partagé et de s'assurer que le groupe de règles est appliqué à chaque composant individuellement. Un groupe de règles de QoS partagé appliquera le plafond du débit total de toutes les charges de travail.

Voici un exemple avec des valeurs par défaut définies :

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "customBackendName",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "labels": {"k8scluster": "dev1", "backend": "dev1-nasbackend"},
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "password",
  "limitAggregateUsage": "80%",
  "limitVolumeSize": "50Gi",
  "nfsMountOptions": "nfsvers=4",
  "debugTraceFlags": {"api":false, "method":true},
  "defaults": {
    "spaceReserve": "volume",
    "qosPolicy": "premium",
    "exportPolicy": "myk8scluster",
    "snapshotPolicy": "default",
    "snapshotReserve": "10"
  }
}
```

Pour `ontap-nas` et `ontap-nas-flexgroups`, Astra Trident utilise maintenant un nouveau calcul pour s'assurer que la FlexVol est correctement dimensionnée avec le pourcentage de snapshots et la demande de volume persistant. Lorsque l'utilisateur demande de volume persistant, Astra Trident crée le FlexVol d'origine

avec plus d'espace en utilisant le nouveau calcul. Ce calcul garantit que l'utilisateur reçoit l'espace inscriptible demandé dans la demande de volume persistant et qu'il ne dispose pas d'un espace minimal par rapport à ce qu'il a demandé. Avant le 21.07, lorsque l'utilisateur demande une demande de volume persistant (par exemple, 5 Gio), et le `snapshotReserve` à 50 %, ils ne bénéficient que d'un espace inscriptible de 2,5 Gio. En effet, le nom d'utilisateur requis correspond à l'intégralité du volume et `snapshotReserve` représente un pourcentage de cela. Avec Trident 21.07, il s'agit de l'espace inscriptible demandé par l'utilisateur et d'Astra Trident définit le `snapshotReserve` nombre comme pourcentage de l'intégralité du volume. Cela ne s'applique pas à `ontap-nas-economy`. Voir l'exemple suivant pour voir comment cela fonctionne :

Le calcul est le suivant :

```
Total volume size = (PVC requested size) / (1 - (snapshotReserve
percentage) / 100)
```

Pour les snapshots `Reserve = 50 %`, et demande en volume `PVC = 5 Gio`, la taille totale du volume est $2/0,5 = 10$ Gio et la taille disponible est de 5 Gio, ce que l'utilisateur a demandé dans la demande de demande de volume persistant. Le `volume show` la commande doit afficher des résultats similaires à cet exemple :

Vserver	Volume	Aggregate	State	Type	Size	Available	Used%
		_pvc_89f1c156_3801_4de4_9f9d_034d54c395f4	online	RW	10GB	5.00GB	0%
		_pvc_e8372153_9ad9_474a_951a_08ae15e1c0ba	online	RW	1GB	511.8MB	0%

2 entries were displayed.

Les systèmes back-end des installations précédentes provisionnent les volumes comme expliqué ci-dessus lors de la mise à niveau d'Astra Trident. Pour les volumes que vous avez créés avant la mise à niveau, vous devez redimensionner leurs volumes afin que la modification puisse être observée. Par exemple, un PVC de 2 Gio avec `snapshotReserve=50` Auparavant, un volume doté d'un espace inscriptible de 1 Gio. Le redimensionnement du volume à 3 Gio, par exemple, fournit l'application avec 3 Gio d'espace inscriptible sur un volume de 6 Gio.

Exemples de configuration minimaux

Les exemples suivants montrent des configurations de base qui laissent la plupart des paramètres par défaut. C'est la façon la plus simple de définir un back-end.



Si vous utilisez Amazon FSX sur NetApp ONTAP avec Trident, nous vous recommandons de spécifier des noms DNS pour les LIF au lieu d'adresses IP.

`ontap-nas` pilote avec authentification par certificat

Il s'agit d'un exemple de configuration back-end minimal. `clientCertificate`, `clientPrivateKey`, et `trustedCACertificate` (Facultatif, si vous utilisez une autorité de certification approuvée) est renseigné `backend.json` Et prendre les valeurs codées en base64 du certificat client, de la clé privée et du certificat CA de confiance, respectivement.

```
{
  "version": 1,
  "backendName": "DefaultNASBackend",
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.15",
  "svm": "nfs_svm",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz",
  "storagePrefix": "myPrefix_"
}
```

ontap-nas **pilote avec règle d'exportation automatique**

Cet exemple vous montre comment vous pouvez demander à Astra Trident d'utiliser des règles d'exportation dynamiques pour créer et gérer automatiquement la règle d'exportation. Cela fonctionne de la même manière pour le ontap-nas-economy et ontap-nas-flexgroup pilotes.

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "labels": {"k8scluster": "test-cluster-east-1a", "backend": "test1-
nasbackend"},
  "autoExportPolicy": true,
  "autoExportCIDRs": ["10.0.0.0/24"],
  "username": "admin",
  "password": "secret",
  "nfsMountOptions": "nfsvers=4",
}
```

ontap-nas-flexgroup **conducteur**

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-flexgroup",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "labels": {"k8scluster": "test-cluster-east-1b", "backend": "test1-ontap-cluster"},
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret",
}
```

ontap-nas **Pilote avec IPv6**

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "nas_ipv6_backend",
  "managementLIF": "[5c5d:5edf:8f:7657:bef8:109b:1b41:d491]",
  "labels": {"k8scluster": "test-cluster-east-1a", "backend": "test1-ontap-ipv6"},
  "svm": "nas_ipv6_svm",
  "username": "vsadmin",
  "password": "netapp123"
}
```

ontap-nas-economy **conducteur**

```
{
  "version": 1,
  "storageDriverName": "ontap-nas-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret"
}
```

Exemples de systèmes back-end avec pools de stockage virtuel

Dans l'exemple de fichier de définition backend ci-dessous, des valeurs par défaut spécifiques sont définies pour tous les pools de stockage, par exemple `spaceReserve` aucune, `spaceAllocation` lors de la fausse idée, et `encryption` faux. Les pools de stockage virtuels sont définis dans la section `stockage`.

Dans cet exemple, certains pools de stockage sont propriétaires de leur propre pool `spaceReserve`, `spaceAllocation`, et `encryption` les valeurs et certains pools remplacent les valeurs par défaut définies ci-dessus.

ontap-nas **conducteur**

```
{
  {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "managementLIF": "10.0.0.1",
    "dataLIF": "10.0.0.2",
    "svm": "svm_nfs",
    "username": "admin",
    "password": "secret",
    "nfsMountOptions": "nfsvers=4",

    "defaults": {
      "spaceReserve": "none",
      "encryption": "false",
      "qosPolicy": "standard"
    },
    "labels": {"store": "nas_store", "k8scluster": "prod-cluster-1"},
    "region": "us_east_1",
    "storage": [
      {
        "labels": {"app": "msoffice", "cost": "100"},
        "zone": "us_east_1a",
        "defaults": {
          "spaceReserve": "volume",
          "encryption": "true",
          "unixPermissions": "0755",
          "adaptiveQosPolicy": "adaptive-premium"
        }
      },
      {
        "labels": {"app": "slack", "cost": "75"},
        "zone": "us_east_1b",
        "defaults": {
          "spaceReserve": "none",
          "encryption": "true",
          "unixPermissions": "0755"
        }
      },
      {
        "labels": {"app": "wordpress", "cost": "50"},
```

```

    "zone": "us_east_1c",
    "defaults": {
      "spaceReserve": "none",
      "encryption": "true",
      "unixPermissions": "0775"
    }
  },
  {
    "labels": {"app": "mysqldb", "cost": "25"},
    "zone": "us_east_1d",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "false",
      "unixPermissions": "0775"
    }
  }
]
}

```

ontap-nas-flexgroup **conducteur**

```

{
  "version": 1,
  "storageDriverName": "ontap-nas-flexgroup",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret",

  "defaults": {
    "spaceReserve": "none",
    "encryption": "false"
  },
  "labels": {"store": "flexgroup_store", "k8scluster": "prod-cluster-1"},
  "region": "us_east_1",
  "storage": [
    {
      "labels": {"protection": "gold", "creditpoints": "50000"},
      "zone": "us_east_1a",
      "defaults": {
        "spaceReserve": "volume",
        "encryption": "true",
        "unixPermissions": "0755"
      }
    }
  ]
}

```

```

    },
    {
      "labels":{"protection":"gold", "creditpoints":"30000"},
      "zone":"us_east_1b",
      "defaults": {
        "spaceReserve": "none",
        "encryption": "true",
        "unixPermissions": "0755"
      }
    },
    {
      "labels":{"protection":"silver", "creditpoints":"20000"},
      "zone":"us_east_1c",
      "defaults": {
        "spaceReserve": "none",
        "encryption": "true",
        "unixPermissions": "0775"
      }
    },
    {
      "labels":{"protection":"bronze", "creditpoints":"10000"},
      "zone":"us_east_1d",
      "defaults": {
        "spaceReserve": "volume",
        "encryption": "false",
        "unixPermissions": "0775"
      }
    }
  ]
}

```

ontap-nas-economy **conducteur**

```

{
  "version": 1,
  "storageDriverName": "ontap-nas-economy",
  "managementLIF": "10.0.0.1",
  "dataLIF": "10.0.0.2",
  "svm": "svm_nfs",
  "username": "vsadmin",
  "password": "secret",

  "defaults": {
    "spaceReserve": "none",
    "encryption": "false"
  }
}

```



```

},
"labels":{"store":"nas_economy_store"},
"region": "us_east_1",
"storage": [
  {
    "labels":{"department":"finance", "creditpoints":"6000"},
    "zone":"us_east_1a",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "true",
      "unixPermissions": "0755"
    }
  },
  {
    "labels":{"department":"legal", "creditpoints":"5000"},
    "zone":"us_east_1b",
    "defaults": {
      "spaceReserve": "none",
      "encryption": "true",
      "unixPermissions": "0755"
    }
  },
  {
    "labels":{"department":"engineering", "creditpoints":"3000"},
    "zone":"us_east_1c",
    "defaults": {
      "spaceReserve": "none",
      "encryption": "true",
      "unixPermissions": "0775"
    }
  },
  {
    "labels":{"department":"humanresource",
"creditpoints":"2000"},
    "zone":"us_east_1d",
    "defaults": {
      "spaceReserve": "volume",
      "encryption": "false",
      "unixPermissions": "0775"
    }
  }
]
}

```

Mappage des systèmes back-end aux classes de stockage

Les définitions de classe de stockage suivantes font référence aux pools de stockage virtuels ci-dessus. À l'aide du `parameters.selector` Chaque classe de stockage indique quel(s) pool(s) virtuel(s) peut(s) être utilisé(s) pour héberger un volume. Les aspects définis dans le pool virtuel sélectionné seront définis pour le volume.

- La première classe de stockage (`protection-gold`) sera mappé sur le premier, deuxième pool de stockage virtuel dans le `ontap-nas-flexgroup` système back-end et le premier pool de stockage virtuel dans `ontap-san` back-end. Il s'agit du seul pool offrant une protection de niveau Gold.
- La deuxième classe de stockage (`protection-not-gold`) sera mappé sur le troisième, quatrième pool de stockage virtuel dans `ontap-nas-flexgroup` back-end et le deuxième, troisième pool de stockage virtuel dans `ontap-san` back-end. Ce sont les seuls pools offrant un niveau de protection autre que l'or.
- La troisième classe de stockage (`app-mysqldb`) sera mappé sur le quatrième pool de stockage virtuel dans `ontap-nas` back-end et le troisième pool de stockage virtuel dans `ontap-san-economy` back-end. Ce sont les seuls pools offrant une configuration de pool de stockage pour l'application de type `mysqldb`.
- La quatrième classe de stockage (`protection-silver-creditpoints-20k`) sera mappé sur le troisième pool de stockage virtuel dans `ontap-nas-flexgroup` back-end et le second pool de stockage virtuel dans `ontap-san` back-end. Ce sont les seules piscines offrant une protection de niveau or à 20000 points de solvabilité.
- La cinquième classe de stockage (`creditpoints-5k`) sera mappé sur le second pool de stockage virtuel dans `ontap-nas-economy` back-end et le troisième pool de stockage virtuel dans `ontap-san` back-end. Ce sont les seules offres de piscine à 5000 points de solvabilité.

Astra Trident va décider du pool de stockage virtuel sélectionné et s'assurer que les besoins en stockage sont satisfaits.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-not-gold
provisioner: netapp.io/trident
parameters:
  selector: "protection!=gold"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: app-mysqldb
provisioner: netapp.io/trident
parameters:
  selector: "app=mysqldb"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: protection-silver-creditpoints-20k
provisioner: netapp.io/trident
parameters:
  selector: "protection=silver; creditpoints=20000"
  fsType: "ext4"
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: creditpoints-5k
provisioner: netapp.io/trident
parameters:
  selector: "creditpoints=5000"
  fsType: "ext4"

```

Utilisez Astra Trident avec Amazon FSX pour NetApp ONTAP

"Amazon FSX pour NetApp ONTAP", Est un service AWS entièrement géré qui permet aux clients de lancer et d'exécuter des systèmes de fichiers optimisés par le système d'exploitation du stockage ONTAP de NetApp. La solution Amazon FSX pour NetApp ONTAP vous permet d'exploiter les fonctionnalités, les performances et les capacités administratives de NetApp que vous connaissez déjà, tout en bénéficiant de la simplicité, de l'agilité, de la sécurité et de l'évolutivité du stockage de données sur AWS. FSX prend en charge de nombreuses fonctionnalités de système de fichiers et API d'administration d'ONTAP.

Un système de fichiers est la ressource principale d'Amazon FSX, similaire à un cluster ONTAP sur site. Au sein de chaque SVM, vous pouvez créer un ou plusieurs volumes, qui sont des conteneurs de données qui stockent les fichiers et les dossiers dans votre système de fichiers. Avec Amazon FSX pour NetApp ONTAP, Data ONTAP sera fourni en tant que système de fichiers géré dans le cloud. Le nouveau type de système de fichiers est appelé **NetApp ONTAP**.

Avec Astra Trident avec Amazon FSX pour NetApp ONTAP, vous pouvez vous assurer que les clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS) peuvent provisionner des volumes persistants de bloc et de fichier sauvegardés par ONTAP.

Création de votre système de fichiers Amazon FSX pour ONTAP

Les volumes créés sur des systèmes de fichiers Amazon FSX dont les sauvegardes automatiques sont activées ne peuvent pas être supprimés par Trident. Pour supprimer des demandes de volume persistant, vous devez supprimer manuellement le volume PV et le volume FSX pour ONTAP.

Pour éviter ce problème :

- N'utilisez pas **création rapide** pour créer le système de fichiers FSX pour ONTAP. Le flux de création rapide active les sauvegardes automatiques et ne propose pas d'option de désinscription.
- Lorsque vous utilisez **création standard**, désactivez la sauvegarde automatique. La désactivation des sauvegardes automatiques permet à Trident de supprimer un volume sans intervention manuelle supplémentaire.



▼ Backup and maintenance - *optional*

Daily automatic backup [Info](#)

Amazon FSx can protect your data through daily backups

☐ Enabled

☒ Disabled

Découvrez Astra Trident

Si vous découvrez Astra Trident, familiarisez-vous avec les liens ci-dessous :

- ["FAQ"](#)

- ["Exigences d'utilisation d'Astra Trident"](#)
- ["Déployez Astra Trident"](#)
- ["Meilleures pratiques de configuration de ONTAP, Cloud Volumes ONTAP et Amazon FSX pour NetApp ONTAP"](#)
- ["Intégrez Astra Trident"](#)
- ["Configuration SAN backend ONTAP"](#)
- ["Configuration NAS backend ONTAP"](#)

En savoir plus sur les capacités des pilotes ["ici"](#).

Utilisation d'Amazon FSX pour NetApp ONTAP ["FabricPool"](#) pour gérer les niveaux de stockage. Elle vous permet de stocker les données au niveau le plus important, selon que celles-ci sont fréquemment utilisées.

Astra Trident devrait être exécuté en tant que A. `vsadmin` Utilisateur SVM ou en tant qu'utilisateur avec un nom différent qui a le même rôle. Amazon FSX pour NetApp ONTAP en a un `fsxadmin` Utilisateur qui remplace le ONTAP de manière limitée `admin` utilisateur du cluster. Il n'est pas recommandé d'utiliser le `fsxadmin` Avec Trident, en tant que A. `vsadmin` Les utilisateurs du SVM ont accès à d'autres fonctionnalités Trident d'Astra,

Pilotes

Vous pouvez intégrer Astra Trident avec Amazon FSX pour NetApp ONTAP à l'aide des pilotes suivants :

- `ontap-san`: Chaque volume persistant provisionné est un LUN au sein de son propre volume Amazon FSX pour NetApp ONTAP.
- `ontap-san-economy`: Chaque volume persistant provisionné est un LUN avec un nombre configurable de LUN par Amazon FSX pour le volume NetApp ONTAP.
- `ontap-nas`: Chaque volume persistant provisionné est un volume Amazon FSX complet pour NetApp ONTAP.
- `ontap-nas-economy`: Chaque volume persistant provisionné est un `qtree`, avec un nombre configurable de `qtrees` par Amazon FSX pour le volume NetApp ONTAP.
- `ontap-nas-flexgroup`: Chaque volume persistant provisionné est un volume Amazon FSX complet pour NetApp ONTAP FlexGroup.

Authentification

Astra Trident propose deux modes d'authentification :

- Basé sur des certificats : Astra Trident communiquera avec le SVM sur votre système de fichiers FSX à l'aide d'un certificat installé sur votre SVM.
- Basé sur les identifiants : vous pouvez utiliser le `fsxadmin` utilisateur pour votre système de fichiers ou `vsadmin` Configuré pour votre SVM.



Nous vous recommandons vivement d'utiliser le `vsadmin` utilisateur au lieu du `fsxadmin` pour configurer votre système backend. Astra Trident communiquera avec le système de fichiers FSX à l'aide de ce nom d'utilisateur et de ce mot de passe.

Pour en savoir plus sur l'authentification, consultez les liens suivants :

- "NAS ONTAP"
- "SAN ONTAP"

Déployez et configurez Astra Trident sur EKS avec Amazon FSX pour NetApp ONTAP

Ce dont vous avez besoin

- Un cluster Amazon EKS existant ou un cluster Kubernetes autogéré avec `kubectl` installé.
- Un système de fichiers Amazon FSX pour NetApp ONTAP existant et une machine virtuelle de stockage (SVM) accessible depuis les nœuds workers de votre cluster.
- Nœuds worker prêts pour "NFS et/ou iSCSI".



Assurez-vous de suivre les étapes de préparation des nœuds requises pour Amazon Linux et Ubuntu "Images de machine Amazon" (AMIS) en fonction de votre type ami EKS.

Pour connaître les autres exigences d'Astra Trident, consultez le site ["ici"](#).

Étapes

1. Déployez Astra Trident avec l'un des `../trident-get-Started/kubernetes-Deploy.html`[méthodes de déploiement^].
2. Configurez Astra Trident comme suit :
 - a. Collectez le nom DNS de la LIF de gestion de votre SVM. Par exemple, en utilisant l'interface de ligne de commandes AWS, recherchez le `DNSName` entrée sous `Endpoints` → `Management` après avoir exécuté la commande suivante :

```
aws fsx describe-storage-virtual-machines --region <file system region>
```

3. Créer et installer des certificats pour l'authentification. Si vous utilisez un `ontap-san` back-end, voir ["ici"](#). Si vous utilisez un `ontap-nas` back-end, voir ["ici"](#).



Vous pouvez vous connecter à votre système de fichiers (par exemple pour installer des certificats) à l'aide de SSH à partir de n'importe quel endroit qui peut atteindre votre système de fichiers. Utilisez le `fsxadmin` User, le mot de passe que vous avez configuré lors de la création de votre système de fichiers et le nom DNS de gestion à partir de `aws fsx describe-file-systems`.

4. Créer un fichier backend en utilisant vos certificats et le nom DNS de votre LIF de gestion, comme indiqué dans l'exemple ci-dessous :

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "customBackendName",
  "managementLIF": "svm-XXXXXXXXXXXXXXXXX.fs-XXXXXXXXXXXXXXXXX.fsx.us-east-2.aws.internal",
  "svm": "svm01",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz",
}
```

Pour plus d'informations sur la création des systèmes back-end, voir les liens suivants :

- ["Configurer un système back-end avec les pilotes NAS ONTAP"](#)
- ["Configurer un système back-end avec les pilotes SAN ONTAP"](#)



Ne pas spécifier `dataLIF` pour le `ontap-san` et `ontap-san-economy` Pilotes permettant à Astra Trident d'utiliser le chemin d'accès multivoie.



Le `limitAggregateUsage` le paramètre ne fonctionne pas avec le `vsadmin` et `fsxadmin` comptes d'utilisateur. L'opération de configuration échoue si vous spécifiez ce paramètre.

Après le déploiement, suivez les étapes pour créer un ["classe de stockage, provisionnez un volume et montez le volume dans un pod"](#).

Trouvez plus d'informations

- ["Documentation Amazon FSX pour NetApp ONTAP"](#)
- ["Billet de blog sur Amazon FSX pour NetApp ONTAP"](#)

Informations sur le copyright

Copyright © 2024 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.