



Amazon FSx for NetApp ONTAP

Trident

NetApp
July 01, 2026

Sommaire

Amazon FSx for NetApp ONTAP	1
Utilisez Trident avec Amazon FSx for NetApp ONTAP	1
Exigences	1
Considérations	1
Authentification	2
Amazon Machine Images (AMIs) testées	2
Pour plus d'informations	3
Créez un rôle IAM et un secret AWS	3
Créer un secret AWS Secrets Manager	4
Créer une stratégie IAM	4
Installer Trident	9
Installez Trident via helm	9
Installez Trident via le module complémentaire EKS	11
Configurer une classe de stockage	17
Créer un objet StorageClass	17
Provisionner des volumes SMB	26
Configuration avancée du backend et exemples	27
Options de configuration backend pour le provisionnement des volumes	31
Configurer un PVC	33
Créer le PVC	33
Déployer une application	34
Déployer une application exemple	34
Configurez le module complémentaire Trident EKS sur un cluster EKS	36
Prérequis	36
Étapes	36
Installez/désinstallez l'add-on Trident EKS à l'aide de la CLI	39

Amazon FSx for NetApp ONTAP

Utilisez Trident avec Amazon FSx for NetApp ONTAP

"Amazon FSx for NetApp ONTAP" est un service AWS entièrement géré qui exécute des systèmes de fichiers alimentés par le système d'exploitation de stockage NetApp ONTAP. Il fournit les fonctionnalités, les performances et l'administration d'ONTAP avec l'évolutivité et la simplicité opérationnelle d'AWS. Un système de fichiers est la ressource principale dans Amazon FSx et est analogue à un cluster ONTAP sur site. Chaque système de fichiers contient une ou plusieurs machines virtuelles de stockage (SVM), et chaque SVM contient un ou plusieurs volumes qui stockent des fichiers et des répertoires. Cette intégration permet aux clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS) de provisionner des volumes persistants basés sur ONTAP pour les charges de travail bloc et fichier.

Exigences

En plus de "[Exigences de Trident](#)", pour intégrer FSx for ONTAP avec Trident, vous avez besoin de :

- Un cluster Amazon EKS existant ou un cluster Kubernetes autogéré avec `kubectl` installé.
- Un système de fichiers Amazon FSx for NetApp ONTAP existant et une machine virtuelle de stockage (SVM) accessibles depuis les nœuds de travail de votre cluster.
- Nœuds de travail préparés pour "[NFS ou iSCSI](#)".



Assurez-vous de suivre les étapes de préparation des nœuds requises pour Amazon Linux et Ubuntu "[Amazon Machine Images](#)" (AMIs) en fonction de votre type d'AMI EKS.

Considérations

- Volumes SMB :
 - Les volumes SMB sont pris en charge à l'aide du pilote `ontap-nas` uniquement.
 - Les volumes SMB ne sont pas pris en charge avec l'add-on Trident EKS.
 - Trident prend uniquement en charge les volumes SMB montés sur des pods exécutés sur des nœuds Windows. Consultez "[Préparez-vous à provisionner des volumes SMB](#)" pour plus de détails.
- Avant Trident 24.02, les volumes créés sur les systèmes de fichiers Amazon FSx avec les sauvegardes automatiques activées ne pouvaient pas être supprimés par Trident. Pour éviter ce problème dans Trident 24.02 ou version ultérieure, spécifiez le `fsxFilesystemID`, `AWS apiRegion`, `AWS apiKey`, et `AWS secretKey` dans le fichier de configuration du backend pour AWS FSx for ONTAP.



Si vous spécifiez un rôle IAM à Trident, vous pouvez omettre de spécifier les champs `apiRegion`, `apiKey`, et `secretKey` à Trident explicitement. Pour plus d'informations, consultez "[Options de configuration et exemples pour FSx for ONTAP](#)".

Utilisation simultanée de Trident SAN/iSCSI et du pilote EBS-CSI

Si vous prévoyez d'utiliser des pilotes ontap-san (par exemple, iSCSI) avec AWS (EKS, ROSA, EC2 ou toute autre instance), la configuration multipath requise sur les nœuds peut entrer en conflit avec le pilote CSI Amazon Elastic Block Store (EBS). Pour garantir que le multipath fonctionne sans interférer avec les disques EBS sur le même nœud, vous devez exclure EBS de votre configuration multipath. Cet exemple montre un fichier `multipath.conf` qui inclut les paramètres Trident requis tout en excluant les disques EBS du multipath :

```
defaults {
    find_multipaths no
}
blacklist {
    device {
        vendor "NVME"
        product "Amazon Elastic Block Store"
    }
}
```

Authentification

Trident propose deux modes d'authentification.

- Authentification par identifiants (recommandée) : stocke les identifiants en toute sécurité dans AWS Secrets Manager. Vous pouvez utiliser l'utilisateur `fsxadmin` de votre système de fichiers ou l'utilisateur `vsadmin` configuré pour votre SVM.



Trident s'attend à être exécuté en tant qu'utilisateur `vsadmin` SVM ou en tant qu'utilisateur portant un nom différent mais ayant le même rôle. Amazon FSx for NetApp ONTAP dispose d'un utilisateur `fsxadmin` qui est un remplacement limité de l'utilisateur du cluster ONTAP `admin`. Nous recommandons fortement d'utiliser `vsadmin` avec Trident.

- Basé sur un certificat : Trident communiquera avec la SVM de votre système de fichiers FSx à l'aide d'un certificat installé sur votre SVM.

Pour plus d'informations sur l'activation de l'authentification, reportez-vous à l'authentification pour votre type de pilote :

- ["Authentification NAS ONTAP"](#)
- ["Authentification SAN ONTAP"](#)

Amazon Machine Images (AMIs) testées

Le cluster EKS prend en charge différents systèmes d'exploitation, mais AWS a optimisé certaines images machine Amazon (AMIs) pour les conteneurs et EKS. Les AMIs suivantes ont été testées avec NetApp Trident 25.02.

AMI	NAS	NAS-economy	iSCSI	iSCSI-economy
-----	-----	-------------	-------	---------------

AL2023_x86_64_ST ANDARD	Oui	Oui	Oui	Oui
AL2_x86_64	Oui	Oui	Oui*	Oui*
BOTTLEROCKET_x 86_64	Oui**	Oui	S/O	S/O
AL2023_ARM_64_S TANDARD	Oui	Oui	Oui	Oui
AL2_ARM_64	Oui	Oui	Oui*	Oui*
BOTTLEROCKET_A RM_64	Oui**	Oui	S/O	S/O

- * Impossible de supprimer le PV sans redémarrer le nœud
- ** Ne fonctionne pas avec NFSv3 avec Trident version 25.02.



Si l'AMI que vous recherchez ne figure pas dans cette liste, cela ne signifie pas qu'elle n'est pas prise en charge ; cela signifie simplement qu'elle n'a pas été testée. Cette liste sert de guide pour les AMI dont le fonctionnement est avéré.

Tests effectués avec:

- EKS version : 1.32
- Méthode d'installation : Helm 25.06 et en tant qu'AWS add-On 25.06
- Pour NAS, les protocoles NFSv3 et NFSv4.1 ont été testés.
- Pour le SAN, seul l'iSCSI a été testé, pas le NVMe-oF.

Tests effectués :

- Créer : Storage Class, pvc, pod
- Supprimer : pod, pvc (standard, qtree/lun – économique, NAS avec sauvegarde AWS)

Pour plus d'informations

- ["Documentation Amazon FSx for NetApp ONTAP"](#)
- ["Article de blog sur Amazon FSx for NetApp ONTAP"](#)

Créez un rôle IAM et un secret AWS

Vous pouvez configurer les pods Kubernetes pour accéder aux ressources AWS en s'authentifiant en tant que rôle AWS IAM au lieu de fournir des identifiants AWS explicites.



Pour vous authentifier à l'aide d'un rôle AWS IAM, vous devez disposer d'un cluster Kubernetes déployé à l'aide d'EKS.

Créer un secret AWS Secrets Manager

Étant donné que Trident utilisera des API sur un vserver FSx pour gérer le stockage pour vous, il aura besoin d'identifiants pour le faire. La méthode sécurisée pour transmettre ces identifiants consiste à utiliser un secret AWS Secrets Manager. Par conséquent, si vous n'en possédez pas déjà un, vous devrez créer un secret AWS Secrets Manager contenant les identifiants du compte vsadmin.

Cet exemple crée un secret AWS Secrets Manager pour stocker les informations d'identification Trident CSI :

```
aws secretsmanager create-secret --name trident-secret --description
"Trident CSI credentials"\
  --secret-string
"{\"username\": \"vsadmin\", \"password\": \"<svmpassword>\"}"
```

Créer une stratégie IAM

Trident a également besoin des autorisations AWS pour fonctionner correctement. Par conséquent, vous devez créer une stratégie qui donne à Trident les autorisations dont il a besoin.

Les exemples suivants créent une stratégie IAM à l'aide de l'AWS CLI :

```
aws iam create-policy --policy-name AmazonFSxNCSIDriverPolicy --policy
-document file://policy.json
  --description "This policy grants access to Trident CSI to FSxN and
Secrets manager"
```

Exemple de JSON de stratégie :

```

{
  "Statement": [
    {
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeVolumes",
        "fsx:CreateVolume",
        "fsx:RestoreVolumeFromSnapshot",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:UntagResource",
        "fsx:UpdateVolume",
        "fsx:TagResource",
        "fsx>DeleteVolume"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": "secretsmanager:GetSecretValue",
      "Effect": "Allow",
      "Resource": "arn:aws:secretsmanager:<aws-region>:<aws-account-id>:secret:<aws-secret-manager-name>*"
    }
  ],
  "Version": "2012-10-17"
}

```

Créer une identité de pod ou un rôle IAM pour l'association du compte de service (IRSA)

Vous pouvez configurer un compte de service Kubernetes pour qu'il assume un rôle AWS Identity and Access Management (IAM) avec EKS Pod Identity ou IAM role for Service account association (IRSA). Tous les Pods configurés pour utiliser le compte de service peuvent alors accéder à tout service AWS auquel le rôle a des autorisations d'accès.

Identité du pod

Les associations d'identité de pod Amazon EKS offrent la possibilité de gérer les informations d'identification de vos applications, de la même manière que les profils d'instance Amazon EC2 fournissent des informations d'identification aux instances Amazon EC2.

Installez Pod Identity sur votre cluster EKS :

Vous pouvez créer une identité de pod via la console AWS ou en utilisant la commande AWS CLI suivante :

```
aws eks create-addon --cluster-name <EKS_CLUSTER_NAME> --addon-name
eks-pod-identity-agent
```

Pour plus d'informations, consultez ["Configurer l'agent d'identité du pod Amazon EKS"](#).

Créer trust-relationship.json:

Créez trust-relationship.json pour permettre au Service Principal EKS d'assumer ce rôle pour l'identité du pod. Créez ensuite un rôle avec cette stratégie d'approbation :

```
aws iam create-role \
  --role-name fsxn-csi-role --assume-role-policy-document file://trust-
relationship.json \
  --description "fsxn csi pod identity role"
```

Fichier trust-relationship.json:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "pods.eks.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ]
    }
  ]
}
```

Associez la stratégie de rôle au rôle IAM:

Associez la stratégie de rôle de l'étape précédente au rôle IAM qui a été créé :

```
aws iam attach-role-policy \  
  --policy-arn arn:aws:iam::aws:111122223333:policy/fsxn-csi-policy \  
  --role-name fsxn-csi-role
```

Créer une association d'identité de pod :

Créer une association d'identité de pod entre le rôle IAM et le compte de service Trident (trident-controller)

```
aws eks create-pod-identity-association \  
  --cluster-name <EKS_CLUSTER_NAME> \  
  --role-arn arn:aws:iam::111122223333:role/fsxn-csi-role \  
  --namespace trident --service-account trident-controller
```

Rôle IAM pour l'association de compte de service (IRSA)

Utilisation de l'interface de ligne de commande AWS :

```
aws iam create-role --role-name AmazonEKS_FSxN_CSI_DriverRole \  
  --assume-role-policy-document file://trust-relationship.json
```

Fichier trust-relationship.json :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::<account_id>:oidc-
provider/<oidc_provider>"
      },
      "Action": "sts:AssumeRoleWithWebIdentity",
      "Condition": {
        "StringEquals": {
          "<oidc_provider>:aud": "sts.amazonaws.com",
          "<oidc_provider>:sub":
"system:serviceaccount:trident:trident-controller"
        }
      }
    }
  ]
}
```

Mettez à jour les valeurs suivantes dans le fichier `trust-relationship.json` :

- **<account_id>** - Votre ID de compte AWS
- **<oidc_provider>** - L'OIDC de votre cluster EKS. Vous pouvez obtenir le `oidc_provider` en exécutant :

```
aws eks describe-cluster --name my-cluster --query
"cluster.identity.oidc.issuer" \
  --output text | sed -e "s/^https:\\/\\/"
```

Associez le rôle IAM à la stratégie IAM:

Une fois le rôle créé, associez la stratégie (qui a été créée à l'étape ci-dessus) au rôle à l'aide de cette commande :

```
aws iam attach-role-policy --role-name my-role --policy-arn <IAM policy
ARN>
```

Vérifiez que le fournisseur OICD est associé:

Vérifiez que votre fournisseur OIDC est associé à votre cluster. Vous pouvez le vérifier à l'aide de cette commande :

```
aws iam list-open-id-connect-providers | grep $oidc_id | cut -d "/" -f4
```

Si le résultat est vide, utilisez la commande suivante pour associer IAM OIDC à votre cluster :

```
eksctl utils associate-iam-oidc-provider --cluster $cluster_name  
--approve
```

Si vous utilisez eksctl, utilisez l'exemple suivant pour créer un rôle IAM pour le compte de service dans EKS :

```
eksctl create iamserviceaccount --name trident-controller --namespace  
trident \  
  --cluster <my-cluster> --role-name AmazonEKS_FSxN_CSI_DriverRole  
--role-only \  
  --attach-policy-arn <IAM-Policy ARN> --approve
```

Installer Trident

Trident simplifie la gestion du stockage Amazon FSx for NetApp ONTAP dans Kubernetes afin de permettre à vos développeurs et administrateurs de se concentrer sur le déploiement des applications. Vous pouvez installer Trident en utilisant l'une des méthodes suivantes :

- Helm
- Module complémentaire EKS

Si vous souhaitez utiliser la fonctionnalité de snapshot, installez l'add-on CSI snapshot controller. Consultez ["Activer la fonctionnalité de snapshot pour les volumes CSI"](#) pour plus d'informations.

Installez Trident via helm

Identité du pod

1. Ajoutez le dépôt Trident Helm :

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Installez Trident en utilisant l'exemple suivant :

```
helm install trident-operator netapp-trident/trident-operator --version 100.2502.1 --namespace trident --create-namespace
```

Vous pouvez utiliser la commande `helm list` pour consulter les détails de l'installation tels que le nom, l'espace de noms, le chart, l'état, la version de l'application et le numéro de révision.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14
14:31:22.463122 +0300	IDT	deployed	trident-operator-
100.2502.0	25.02.0		

Association de compte de service (IRSA)

1. Ajoutez le dépôt Trident Helm :

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Définissez les valeurs pour **fournisseur de cloud** et **cloud identity** :

```
helm install trident-operator netapp-trident/trident-operator --version 100.2502.1 \ --set cloudProvider="AWS" \ --set cloudIdentity="'eks.amazonaws.com/role-arn:arn:aws:iam::<accountID>:role/<AmazonEKS_FSxN_CSI_DriverRole>'" \ --namespace trident \ --create-namespace
```

Vous pouvez utiliser la commande `helm list` pour consulter les détails de l'installation tels que le nom, l'espace de noms, le chart, l'état, la version de l'application et le numéro de révision.

```
helm list -n trident
```

NAME	NAMESPACE	REVISION	UPDATED
STATUS	CHART		APP VERSION
trident-operator	trident	1	2024-10-14
14:31:22.463122 +0300	IDT	deployed	trident-operator-
100.2510.0	25.10.0		

Si vous prévoyez d'utiliser iSCSI, assurez-vous que iSCSI est activé sur votre machine cliente. Si vous utilisez AL2023 Worker node OS, vous pouvez automatiser l'installation du client iSCSI en ajoutant le paramètre `nodePrep` lors de l'installation avec `helm` :



```
helm install trident-operator netapp-trident/trident-operator  
--version 100.2502.1 --namespace trident --create-namespace --  
set nodePrep={iscsi}
```

Installez Trident via le module complémentaire EKS

L'add-on Trident EKS inclut les derniers correctifs de sécurité, les corrections de bogues et est validé par AWS pour fonctionner avec Amazon EKS. L'add-on EKS vous permet de garantir de manière cohérente que vos clusters Amazon EKS sont sécurisés et stables, et de réduire la quantité de travail nécessaire pour installer, configurer et mettre à jour les add-ons.

Prérequis

Assurez-vous de disposer des éléments suivants avant de configurer le module complémentaire Trident pour AWS EKS :

- Un compte de cluster Amazon EKS avec abonnement complémentaire
- Autorisations AWS pour la AWS marketplace :
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Type d'AMI : Amazon Linux 2 (AL2_x86_64) ou Amazon Linux 2 Arm(AL2_ARM_64)
- Type de nœud : AMD ou ARM
- Un système de fichiers Amazon FSx for NetApp ONTAP existant

Activez le module complémentaire Trident pour AWS

Console de gestion

1. Ouvrez la console Amazon EKS à <https://console.aws.amazon.com/eks/home#/clusters>.
2. Dans le volet de navigation de gauche, sélectionnez **Clusters**.
3. Sélectionnez le nom du cluster pour lequel vous souhaitez configurer le module complémentaire NetApp Trident CSI.
4. Sélectionnez **Modules complémentaires** puis sélectionnez **Obtenir plus de modules complémentaires**.
5. Suivez ces étapes pour sélectionner le module complémentaire :
 - a. Faites défiler vers le bas jusqu'à la section **AWS Marketplace add-ons** et tapez **"Trident"** dans la zone de recherche.
 - b. Cochez la case à cocher située dans le coin supérieur droit de la boîte Trident by NetApp.
 - c. Sélectionnez **Next**.
6. Sur la page des paramètres **Configure selected add-ons**, procédez comme suit :



Ignorez ces étapes si vous utilisez l'association Pod Identity.

- a. Sélectionnez la **Versión** que vous souhaitez utiliser.
- b. Si vous utilisez l'authentification IRSA, assurez-vous de définir les valeurs de configuration disponibles dans les paramètres de configuration optionnels :
 - Sélectionnez la **Versión** que vous souhaitez utiliser.
 - Suivez le **schéma de configuration du module complémentaire** et définissez le paramètre **configurationValues** dans la section **Valeurs de configuration** sur le role-arn que vous avez créé à l'étape précédente (la valeur doit être au format suivant) :

```
{  
  
  "cloudIdentity": "'eks.amazonaws.com/role-arn: <role ARN>'",  
  "cloudProvider": "AWS"  
  
}
```

+

Si vous sélectionnez **Override** comme méthode de résolution des conflits, un ou plusieurs des paramètres de l'add-on existant peuvent être remplacés par les paramètres de l'add-on Amazon EKS. Si vous n'activez pas cette option et qu'il y a un conflit avec vos paramètres existants, l'opération échoue. Vous pouvez utiliser le message d'erreur résultant pour résoudre le conflit. Avant de sélectionner cette option, assurez-vous que l'add-on Amazon EKS ne gère pas des paramètres que vous devez gérer vous-même.

7. Choisissez **Suivant**.
8. Sur la page **Vérifier et ajouter**, choisissez **Créer**.

Une fois l'installation du logiciel complémentaire terminée, vous voyez votre logiciel complémentaire installé.

AWS CLI

1. Créez le `add-on.json` fichier :

Pour l'identité du pod, utilisez le format suivant:



Utilisez le

```
{
  "clusterName": "<eks-cluster>",
  "addonName": "netapp_trident-operator",
  "addonVersion": "v25.6.0-eksbuild.1",
}
```

Pour l'authentification IRSA, utilisez le format suivant:

```
{
  "clusterName": "<eks-cluster>",
  "addonName": "netapp_trident-operator",
  "addonVersion": "v25.6.0-eksbuild.1",
  "serviceAccountRoleArn": "<role ARN>",
  "configurationValues": {
    "cloudIdentity": "'eks.amazonaws.com/role-arn: <role ARN>'",
    "cloudProvider": "AWS"
  }
}
```



Remplacez `<role ARN>` par l'ARN du rôle qui a été créé à l'étape précédente.

2. Installez le logiciel complémentaire Trident EKS.

```
aws eks create-addon --cli-input-json file://add-on.json
```

eksctl

La commande suivante permet d'installer le module complémentaire Trident EKS :

```
eksctl create addon --name netapp_trident-operator --cluster
<cluster_name> --force
```

Mettre à jour le module complémentaire Trident EKS

Console de gestion

1. Ouvrez la console Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters>.
2. Dans le volet de navigation de gauche, sélectionnez **Clusters**.
3. Sélectionnez le nom du cluster pour lequel vous souhaitez mettre à jour le logiciel complémentaire NetApp Trident CSI.
4. Sélectionnez l'onglet **Add-ons**.
5. Sélectionnez **Trident par NetApp** puis sélectionnez **Modifier**.
6. Sur la page **Configurer Trident par NetApp**, procédez comme suit :
 - a. Sélectionnez la **Version** que vous souhaitez utiliser.
 - b. Développez les **Paramètres de configuration optionnels** et modifiez-les si nécessaire.
 - c. Sélectionnez **Save changes**.

AWS CLI

L'exemple suivant met à jour le add-on EKS :

```
aws eks update-addon --cluster-name <eks_cluster_name> --addon-name
netapp_trident-operator --addon-version v25.6.0-eksbuild.1 \
  --service-account-role-arn <role-ARN> --resolve-conflict preserve \
  --configuration-values "{\"cloudIdentity\":":
\"'eks.amazonaws.com/role-arn: <role ARN>'\"}"
```

eksctl

- Vérifiez la version actuelle de votre add-on Trident CSI FSxN. Remplacez `my-cluster` par le nom de votre cluster.

```
eksctl get addon --name netapp_trident-operator --cluster my-cluster
```

Exemple de sortie :

NAME	VERSION	STATUS	ISSUES
IAMROLE	UPDATE AVAILABLE	CONFIGURATION VALUES	
netapp_trident-operator	v25.6.0-eksbuild.1	ACTIVE	0
{"cloudIdentity": "'eks.amazonaws.com/role-arn: arn:aws:iam::139763910815:role/AmazonEKS_FSXN_CSI_DriverRole'"}			

- Mettez à jour le logiciel complémentaire avec la version renvoyée sous UPDATE AVAILABLE dans le résultat de l'étape précédente.

```
eksctl update addon --name netapp_trident-operator --version
v25.6.0-eksbuild.1 --cluster my-cluster --force
```

Si vous supprimez l'option `--force` et que l'un des paramètres du module complémentaire Amazon EKS entre en conflit avec vos paramètres existants, la mise à jour du module complémentaire Amazon EKS échoue ; vous recevez un message d'erreur pour vous aider à résoudre le conflit. Avant de spécifier cette option, assurez-vous que le module complémentaire Amazon EKS ne gère pas de paramètres que vous devez gérer, car ces paramètres sont écrasés avec cette option. Pour plus d'informations sur les autres options de ce paramètre, consultez "[Modules complémentaires](#)". Pour plus d'informations sur la gestion des champs Kubernetes d'Amazon EKS, consultez "[Gestion des champs Kubernetes](#)".

Désinstallez/supprimez le module complémentaire Trident EKS

Vous avez deux options pour supprimer un add-on Amazon EKS :

- **Conserver le logiciel complémentaire sur votre cluster** – Cette option supprime la gestion de tous les paramètres par Amazon EKS. Elle supprime également la capacité d'Amazon EKS à vous notifier des mises à jour et à mettre à jour automatiquement le logiciel complémentaire Amazon EKS après que vous ayez initié une mise à jour. Cependant, elle conserve le logiciel complémentaire sur votre cluster. Cette option fait du logiciel complémentaire une installation autogérée, plutôt qu'un logiciel complémentaire Amazon EKS. Avec cette option, il n'y a pas d'interruption pour le logiciel complémentaire. Conservez l'option `--preserve` dans la commande pour préserver le logiciel complémentaire.
- **Supprimez entièrement le logiciel complémentaire de votre cluster** – NetApp recommande de supprimer le module complémentaire Amazon EKS de votre cluster uniquement s'il n'y a aucune ressource sur votre cluster qui en dépend. Supprimez l'option `--preserve` de la commande `delete` pour supprimer le logiciel complémentaire.



Si le logiciel complémentaire a un compte IAM associé, le compte IAM n'est pas supprimé.

Console de gestion

1. Ouvrez la console Amazon EKS à <https://console.aws.amazon.com/eks/home#/clusters>.
2. Dans le volet de navigation de gauche, sélectionnez **Clusters**.
3. Sélectionnez le nom du cluster pour lequel vous souhaitez supprimer le logiciel complémentaire Trident CSI NetApp.
4. Sélectionnez l'onglet **Add-ons** puis sélectionnez **Trident par NetApp**.*
5. Sélectionnez **Remove**.
6. Dans la boîte de dialogue **Remove netapp_trident-operator confirmation**, procédez comme suit :
 - a. Si vous souhaitez qu'Amazon EKS cesse de gérer les paramètres du logiciel complémentaire, sélectionnez **Conserver sur le cluster**. Procédez ainsi si vous souhaitez conserver le logiciel complémentaire sur votre cluster afin de pouvoir gérer vous-même tous les paramètres du logiciel complémentaire.
 - b. Saisissez **netapp_trident-operator**.
 - c. Sélectionnez **Remove**.

AWS CLI

Remplacez `my-cluster` par le nom de votre cluster, puis exécutez la commande suivante.

```
aws eks delete-addon --cluster-name my-cluster --addon-name  
netapp_trident-operator --preserve
```

eksctl

La commande suivante désinstalle le module complémentaire Trident EKS :

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

Configurer une classe de stockage

La "[Objet Kubernetes StorageClass](#)" identifie un provisionneur et lui indique comment provisionner les volumes. Cette section montre comment configurer un objet Kubernetes StorageClass qui spécifie Trident comme provisionneur.

Créer un objet StorageClass

Lorsque vous créez un StorageClass pour FSx for ONTAP, Trident créera automatiquement la configuration backend.



Si vous souhaitez configurer manuellement le stockage backend, veuillez vous référer à la section [\[create-a-kubernetes-storageclass-without-automatic-backend-configuration\]](#) pour savoir comment créer séparément le backend Trident et la classe de stockage.

Spécifiez les paramètres requis StorageClass

Les trois paramètres suivants doivent être définis lors de la création d'un StorageClass :

Paramètre	Obligatoire	Type	Description
fsxFilesystemID	Oui	chaîne	ID du système de fichiers FSx for NetApp ONTAP
storageDriverName	Oui	chaîne	Pilote de stockage Trident (par exemple, <code>ontap-nas</code> ou <code>ontap-san</code>)
credentialsName	Oui	chaîne	Nom du secret Kubernetes qui contient les informations d'identification FSx for ONTAP

Spécifiez les paramètres optionnels

Vous pouvez transmettre des paramètres backend optionnels via le StorageClass. Définissez toutes les valeurs optionnelles sous forme de chaînes dans la section `StorageClass parameters`. Pour une liste complète des paramètres du backend, voir : "[Configuration du backend FSx for NetApp ONTAP](#)".

Exemples de fichiers de configuration StorageClass.

L'exemple suivant montre un StorageClass qui déclenche une configuration automatique du backend.

YAML

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-fsx-demo
  annotations:
    description: "Demo StorageClass for FSx for NetApp ONTAP"
provisioner: csi.trident.netapp.io
parameters:
  fsxFilesystemID: "fs-0abc123"
  storageDriverName: "ontap-nas"
  credentialsName: trident-fsx-credentials
allowVolumeExpansion: true
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

JSON

```
{
  "apiVersion": "storage.k8s.io/v1",
  "kind": "StorageClass",
  "metadata": {
    "name": "ontap-fsx-demo",
    "annotations": {
      "description": "Demo StorageClass for FSx for NetApp ONTAP"
    }
  },
  "provisioner": "csi.trident.netapp.io",
  "parameters": {
    "fsxFilesystemID": "fs-0abc123",
    "storageDriverName": "ontap-nas",
    "credentialsName": "trident-fsx-credentials"
  },
  "allowVolumeExpansion": true,
  "reclaimPolicy": "Delete",
  "volumeBindingMode": "Immediate"
}
```

Créez le StorageClass

Une fois que vous avez créé votre fichier de configuration, exécutez la commande suivante pour créer la classe de stockage.

```
kubectl create -f storage-class-ontapnas.yaml
```

Vous devriez maintenant voir une classe de stockage **basic-csi** dans Kubernetes et Trident, et Trident devrait avoir découvert les pools sur le backend.

```
kubectl get sc basic-csi
```

NAME	PROVISIONER	AGE
basic-csi	csi.trident.netapp.io	15h

Après avoir appliqué le StorageClass, Trident crée automatiquement le backend. Vous pouvez ensuite créer des PersistentVolumeClaims qui référencent ce StorageClass.

Vérifier l'état de la configuration du backend

Trident enregistre le résultat de la création du backend dans les annotations StorageClass.

Annotation	Description
trident.netapp.io/configuratorStatus	Résultat de la configuration (Success ou Failure)
trident.netapp.io/configuratorMessage	Message d'état ou d'erreur détaillé
trident.netapp.io/configuratorName	Nom de la ressource du configurateur interne
trident.netapp.io/managed	Indique que le StorageClass est géré par Trident
trident.netapp.io/additionalStoragePools	Pools de stockage créés pour ce backend

Pour vérifier l'état, exécutez :

```
kubectl get storageclass ontap-fsx-demo -o yaml
```

Confirmez que `trident.netapp.io/configuratorStatus` est défini sur `Success`. Si la valeur est `Failure`, examinez `trident.netapp.io/configuratorMessage` pour l'erreur.

Ajouter des systèmes de fichiers FSxN supplémentaires

Si vous avez besoin de stockage supplémentaire tout en continuant à utiliser le même StorageClass, ajoutez des identifiants de système de fichiers FSxN supplémentaires.

Modifiez le StorageClass et ajoutez l'annotation suivante :

```
metadata:
  annotations:
    trident.netapp.io/additionalFsxnFileSystemID: '["fs-
xxxxxxxxxxxxxxxxxxxxx"]'
```

Une fois la modification appliquée, Trident met à jour la configuration du backend et met à jour les annotations StorageClass.

Considérations et limitations opérationnelles

- La suppression d'un StorageClass qui utilise la configuration automatique du backend supprime généralement le backend Trident associé. Cela peut perturber la connectivité du stockage et interrompre les charges de travail en cours. Validez l'impact avant de supprimer un StorageClass géré.
- La configuration automatique du backend est prise en charge uniquement pour AWS FSx pour NetApp ONTAP.

Créer un StorageClass Kubernetes sans configuration automatique du backend

Si vous souhaitez créer le backend Trident et le StorageClass séparément, suivez ces étapes.

Comprendre le fonctionnement de la configuration automatique du backend

Trident déduit la configuration du backend à partir de la définition de la StorageClass. Lorsque vous appliquez la StorageClass, Trident valide les paramètres requis, crée le backend et annote la StorageClass avec le statut.

Trident crée le VolumeSnapshotClass une seule fois. Trident réutilise le même VolumeSnapshotClass pour les StorageClasses suivants.

Créer le backend Trident

Pour créer un backend Trident, vous devez créer un fichier de configuration au format JSON ou YAML. Le fichier doit spécifier le type de stockage souhaité (NAS ou SAN), le système de fichiers, la SVM à utiliser et la méthode d'authentification. L'exemple suivant montre comment définir un stockage basé sur NAS et utiliser un secret AWS pour stocker les informations d'identification de la SVM que vous souhaitez utiliser :

YAML

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas
  namespace: trident
spec:
  version: 1
  storageDriverName: ontap-nas
  backendName: tbc-ontap-nas
  svm: svm-name
  aws:
    fsxFilesystemID: fs-xxxxxxxxxx
  credentials:
    name: "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name"
    type: awsarn
```

JSON

```
{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas"
    "namespace": "trident"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
      "fsxFilesystemID": "fs-xxxxxxxxxx"
    },
    "managementLIF": null,
    "credentials": {
      "name": "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name",
      "type": "awsarn"
    }
  }
}
```

Détails du pilote FSx for ONTAP

Vous pouvez intégrer Trident à Amazon FSx for NetApp ONTAP à l'aide des pilotes suivants :

Nom du pilote	Description
ontap-san	Chaque PV provisionné est un LUN au sein de son propre volume Amazon FSx for NetApp ONTAP. Recommandé pour le stockage bloc.
ontap-nas	Chaque PV provisionné est un volume Amazon FSx for NetApp ONTAP complet. Recommandé pour NFS et SMB.
ontap-san-economy	Chaque PV provisionné est un LUN avec un nombre configurable de LUN par Amazon FSx for NetApp ONTAP volume.
ontap-nas-economy	Chaque PV provisionné est un qtree, avec un nombre configurable de qtrees par volume Amazon FSx for NetApp ONTAP.
ontap-nas-flexgroup	Chaque PV provisionné est un volume Amazon FSx for NetApp ONTAP FlexGroup complet.

Pour plus de détails sur le conducteur, consultez "[Pilotes NAS](#)" et "[Pilotes SAN](#)".

Créer le backend

Après avoir créé le fichier de configuration, exécutez les commandes suivantes pour créer et valider la configuration du backend Trident (TBC) :

- Créez une configuration backend Trident (TBC) à partir d'un fichier yaml et exécutez la commande suivante :

```
kubectl create -f backendconfig.yaml -n trident
```

```
tridentbackendconfig.trident.netapp.io/backend-tbc-ontap-nas created
```

- Vérifiez que la configuration du backend trident (TBC) a été créée avec succès :

```
Kubectl get tbc -n trident
```

NAME	BACKEND NAME	BACKEND UUID
backend-tbc-ontap-nas	tbc-ontap-nas	933e0071-66ce-4324-b9ff-f96d916ac5e9
Bound	Success	

Pour plus d'informations sur les autres options de configuration, consultez la [\[Backend-advanced-configuration-and-examples\]](#) section ci-dessous.

Configurer une classe de stockage sans configuration automatique du backend

Voici des exemples de configurations de classes de stockage à utiliser avec Trident et FSx pour ONTAP.

Classe de stockage pour NFS

Vous pouvez utiliser cet exemple pour configurer StorageClass pour des volumes utilisant NFS (reportez-vous à la section Attributs Trident ci-dessous pour la liste complète des attributs) :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  provisioningType: "thin"
  snapshots: "true"
```

Classe de stockage pour iSCSI

Utilisez cet exemple pour configurer StorageClass pour des volumes utilisant iSCSI :

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  provisioningType: "thin"
  snapshots: "true"
```

Classe de stockage utilisant NFSv3 et AWS Bottlerocket

Pour provisionner des volumes NFSv3 sur AWS Bottlerocket, ajoutez les `mountOptions` requis à la classe de stockage :

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-gold
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
mountOptions:
  - nfsvers=3
  - nolock

```

Attributs de Trident StorageClass

Ces paramètres déterminent quels pools de stockage gérés par Trident doivent être utilisés pour provisionner des volumes d'un type donné.

Attribut	Type	Valeurs	Offre	Demande	Soutenu par
médias ¹	chaîne	hdd, hybride, ssd	Le pool contient des médias de ce type ; hybride signifie les deux	Type de média spécifié	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
provisioningType	chaîne	mince, épais	Pool prend en charge cette méthode de provisionnement	Méthode de provisionnement spécifiée	épais : all ontap ; mince : all ontap & solidfire-san
backendType	chaîne	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, azure-netapp-files, ontap-san-economy	Pool appartient à ce type de backend	Backend spécifié	Tous les drivers
instantanés	bool	vrai, faux	Pool prend en charge les volumes avec snapshots	Volume avec instantanés activés	ontap-nas, ontap-san, solidfire-san

Attribut	Type	Valeurs	Offre	Demande	Soutenu par
clones	bool	vrai, faux	Pool prend en charge le clonage des volumes	Volume avec clones activés	ontap-nas, ontap-san, solidfire-san
chiffrement	bool	vrai, faux	Pool prend en charge les volumes chiffrés	Volume avec chiffrement activé	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
Op E/S par sec	int	entier positif	Pool est capable de garantir des IOPS dans cette plage	Volume garanti ces IOPS	solidfire-san

¹ : Non pris en charge par ONTAP Select ou les systèmes FSx for ONTAP

Consultez "[Objets Kubernetes et Trident](#)" pour plus de détails sur la manière dont les classes de stockage interagissent avec le `PersistentVolumeClaim` et les paramètres permettant de contrôler la façon dont Trident provisionne les volumes.

Créer la classe de stockage

Une fois que vous avez configuré le `StorageClass`, vous pouvez le créer dans Kubernetes.

Étapes

1. Il s'agit d'un objet Kubernetes, utilisez donc `kubectl` pour le créer dans Kubernetes.

```
kubectl create -f storage-class-ontapnas.yaml
```

2. Vous devriez maintenant voir une classe de stockage **basic-csi** dans Kubernetes et Trident, et Trident devrait avoir découvert les pools sur le backend.

```
kubectl get sc basic-csi
```

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

Provisionner des volumes SMB

Vous pouvez provisionner des volumes SMB à l'aide du `ontap-nas` driver. Cependant, pour ce faire, vous devez effectuer ces étapes : "[Préparez-vous à provisionner des volumes SMB](#)".

Configuration avancée du backend et exemples

Consultez le tableau suivant pour les options de configuration du backend :

Paramètre	Description	Exemple
version		Toujours 1
storageDriverName	Nom du pilote de stockage	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy
backendName	Nom personnalisé ou le stockage backend	Nom du pilote + "_" + dataLIF
managementLIF	Adresse IP d'un cluster ou d'une LIF de gestion SVM. Un nom de domaine complet (FQDN) peut être spécifié. Il est possible de configurer l'utilisation d'adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, par exemple : [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si vous fournissez le <code>fsxFilesystemID</code> sous le champ <code>aws</code> , il n'est pas nécessaire de fournir le <code>managementLIF</code> car Trident récupère les informations SVM <code>managementLIF</code> depuis AWS. Vous devez donc fournir les identifiants d'un utilisateur sous la SVM (par exemple : <code>vsadmin</code>) et l'utilisateur doit avoir le rôle <code>vsadmin</code> .	"10.0.0.1", "[2001:1234:abcd::fefe]"

Paramètre	Description	Exemple
dataLIF	Adresse IP de l'interface logique de protocole (LIF). Pilotes ONTAP NAS : NetApp recommande de spécifier dataLIF. Si elle n'est pas fournie, Trident récupère les dataLIF depuis la SVM. Vous pouvez spécifier un nom de domaine complet (FQDN) à utiliser pour les opérations de montage NFS, ce qui vous permet de créer un DNS à répartition de charge (round-robin) entre plusieurs dataLIF. Peut être modifié après la configuration initiale. Pilotes ONTAP SAN : ne pas spécifier pour iSCSI. Trident utilise ONTAP Selective LUN Map pour découvrir les LIF iSCSI nécessaires à l'établissement d'une session multipath. Un avertissement est généré si dataLIF est explicitement défini. Il est possible de configurer l'utilisation d'adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, par exemple : [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	
autoExportPolicy	Activer la création et la mise à jour automatiques des règles d'export [Booléen]. En utilisant les options autoExportPolicy et autoExportCIDRs, Trident peut gérer les règles d'export automatiquement.	false
autoExportCIDRs	Liste des CIDR pour filtrer les adresses IP des nœuds Kubernetes lorsque autoExportPolicy est activé. En utilisant les options autoExportPolicy et autoExportCIDRs, Trident peut gérer les règles d'export automatiquement.	"["0.0.0.0/0", "::/0"]"
labels	Ensemble d'étiquettes arbitraires au format JSON à appliquer aux volumes	""

Paramètre	Description	Exemple
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 d'autorité de certification de confiance. Facultatif. Utilisé pour l'authentification par certificat.	""
username	Nom d'utilisateur pour se connecter au cluster ou à la SVM. Utilisé pour l'authentification par identifiants. Par exemple, vsadmin.	
password	Mot de passe permettant de se connecter au cluster ou à la SVM. Utilisé pour l'authentification par identifiants.	
svm	Machine virtuelle de stockage à utiliser	Dérivé si un LIF de gestion SVM est spécifié.
storagePrefix	Préfixe utilisé lors du provisionnement de nouveaux volumes dans la SVM. Ne peut pas être modifié après création. Pour mettre à jour ce paramètre, vous devrez créer un nouveau backend.	trident
limitAggregateUsage	Ne pas spécifier pour Amazon FSx for NetApp ONTAP. Les <code>fsxadmin</code> et <code>vsadmin</code> fournis ne contiennent pas les autorisations requises pour récupérer l'utilisation agrégée et la limiter à l'aide de Trident.	Ne pas utiliser.
limitVolumeSize	L'approvisionnement échoue si la taille du volume demandée dépasse cette valeur. Limite également la taille maximale des volumes qu'il gère pour les qtrees et les LUN, et l' <code>`qtreesPerFlexvol`</code> option permet de personnaliser le nombre maximal de qtrees par volume FlexVol	"" (non appliqué par défaut)
lunsPerFlexvol	Nombre maximal de LUN par volume FlexVol, doit être compris entre 50 et 200. SAN uniquement.	"100"

Paramètre	Description	Exemple
debugTraceFlags	Options de débogage à utiliser lors du dépannage. Exemple, {"api":false, "method":true} Ne pas utiliser debugTraceFlags sauf si vous effectuez un dépannage et avez besoin d'un journal détaillé.	null
nfsMountOptions	Liste d'options de montage NFS séparées par des virgules. Les options de montage pour les 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, Trident utilisera les options de montage spécifiées dans le fichier de configuration du backend de stockage. Si aucune option de montage n'est spécifiée ni dans la classe de stockage ni dans le fichier de configuration, Trident n'appliquera aucune option de montage au volume persistant associé.	""
nasType	Configurez la création de volumes NFS ou SMB. Les options sont <code>nfs</code> , <code>smb</code> ou <code>null</code> . Doit être défini sur <code>smb</code> pour les volumes SMB. La valeur <code>null</code> correspond par défaut à des volumes NFS.	<code>nfs</code>
qtreesPerFlexvol	Nombre maximal de Qtrees par volume FlexVol, doit être compris dans la plage [50, 300]	"200"
smbShare	Vous pouvez spécifier l'un des éléments suivants : le nom d'un partage SMB créé à l'aide de la console de gestion Microsoft ou de l'interface de ligne de commande ONTAP, ou un nom permettant à Trident de créer le partage SMB. Ce paramètre est requis pour les backends Amazon FSx for ONTAP.	<code>smb-share</code>

Paramètre	Description	Exemple
useREST	Paramètre booléen à utiliser pour les API REST ONTAP. Lorsqu'il est défini sur <code>true</code> , Trident utilisera les API REST ONTAP pour communiquer avec le backend. Cette fonctionnalité nécessite ONTAP 9.11.1 ou une version ultérieure. De plus, le rôle de connexion ONTAP utilisé doit avoir accès à l'application <code>ontap</code> . Cela est satisfait par les rôles prédéfinis <code>vsadmin</code> et <code>cluster-admin</code> .	<code>false</code>
aws	Vous pouvez spécifier les éléments suivants dans le fichier de configuration pour AWS FSx for ONTAP : - <code>fsxFilesystemID</code> : Spécifiez l'ID du système de fichiers AWS FSx. - <code>apiRegion</code> : Nom de la région de l'API AWS. - <code>apiKey</code> : Clé d'API AWS. - <code>secretKey</code> : Clé secrète AWS.	<code>""</code> <code>""</code> <code>""</code>
credentials	Spécifiez les informations d'identification de la SVM FSx à stocker dans AWS Secrets Manager. - <code>name</code> : Nom de ressource Amazon (ARN) du secret, qui contient les informations d'identification de la SVM. - <code>type</code> : Définissez sur <code>awsarn</code> . Consultez "Créer un secret AWS Secrets Manager" pour plus d'informations.	

Options de configuration backend pour le provisionnement des volumes

Vous pouvez contrôler le provisionnement par défaut à l'aide de ces options dans la section `defaults` de la configuration. Pour un exemple, consultez les exemples de configuration ci-dessous.

Paramètre	Description	Défaut
<code>spaceAllocation</code>	Allocation d'espace pour les LUNs	<code>true</code>
<code>spaceReserve</code>	Mode de réservation d'espace ; "none" (fin) ou "volume" (épais)	<code>none</code>
<code>snapshotPolicy</code>	Stratégie de snapshot à utiliser	<code>none</code>

Paramètre	Description	Défaut
qosPolicy	Groupe de règles QoS à attribuer aux volumes créés. Choisissez l'un des qosPolicy ou adaptiveQosPolicy par pool de stockage ou backend. L'utilisation des groupes de règles QoS avec Trident requiert ONTAP 9.8 ou une version ultérieure. Vous devez utiliser un groupe de règles QoS non partagé et vous assurer que le groupe de règles est appliqué individuellement à chaque composant. Un groupe de règles QoS partagé impose une limite au débit total de toutes les charges de travail.	""
adaptiveQosPolicy	Groupe de règles QoS adaptatives à attribuer aux volumes créés. Choisissez l'un des qosPolicy ou adaptiveQosPolicy par pool de stockage ou backend. Non pris en charge par ontap-nas-economy.	""
snapshotReserve	Pourcentage du volume réservé aux snapshots "0"	Si snapshotPolicy est none, `else`""
splitOnClone	Séparer un clone de son parent lors de sa création	false
encryption	Activez le chiffrement de volume NetApp (NVE) sur le nouveau volume ; la valeur par défaut est false. NVE doit être sous licence et activé sur le cluster pour utiliser cette option. Si NAE est activé sur le backend, tout volume provisionné dans Trident sera activé pour NAE. Pour plus d'informations, consultez : "Comment Trident fonctionne avec NVE et NAE" .	false
luksEncryption	Activez le chiffrement LUKS. Consultez "Utilisez Linux Unified Key Setup (LUKS)" . SAN uniquement.	""
tieringPolicy	Politique de hiérarchisation à utiliser none	
unixPermissions	Mode pour les nouveaux volumes. Laisser vide pour les volumes SMB.	""

Paramètre	Description	Défaut
securityStyle	Style de sécurité pour les nouveaux volumes. NFS prend en charge <code>mixed</code> et <code>unix</code> styles de sécurité. SMB prend en charge <code>mixed</code> et <code>ntfs</code> styles de sécurité.	La valeur par défaut de NFS est <code>unix</code> . La valeur par défaut de SMB est <code>ntfs</code> .

Configurer un PVC

Cette section explique comment créer un `PersistentVolumeClaim` (PVC) qui utilise la `StorageClass` Kubernetes configurée pour demander un PV. En cas de succès, vous pourrez ensuite monter le PV sur un pod.

Créer le PVC

Un "*PersistentVolumeClaim*" (PVC) est une demande d'accès au `PersistentVolume` sur le cluster. Le PVC peut être configuré pour demander un espace de stockage d'une certaine taille ou un certain mode d'accès. En utilisant la `StorageClass` associée, l'administrateur du cluster peut contrôler plus que la taille et le mode d'accès du `PersistentVolume`—comme les performances ou le niveau de service.

Après avoir créé le backend Trident et le `StorageClass`, vous pouvez créer un PVC. Après la création du PVC, vous pouvez monter le volume dans un pod.

Exemples de manifestes

Les exemples suivants illustrent les options de configuration de base du PVC.

PVC avec accès RWX

Cet exemple montre un PVC de base avec un accès RWX qui est associé à un `StorageClass` nommé `basic-csi`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-storage
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-gold
```

Exemple d'utilisation de PVC avec iSCSI

Cet exemple montre un PVC de base pour iSCSI avec accès RWO associé à un `StorageClass` nommé `protection-gold`.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: pvc-san
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: protection-gold
```

Créer un PVC

Étapes

1. Créez le PVC.

```
kubectl create -f pvc.yaml
```

2. Vérifiez l'état du PVC.

```
kubectl get pvc
```

NAME	STATUS	VOLUME	CAPACITY	ACCESS MODES	STORAGECLASS	AGE
pvc-storage	Bound	pv-name	2Gi	RWO		5m

Consultez ["Objets Kubernetes et Trident"](#) pour plus de détails sur la manière dont les classes de stockage interagissent avec le `PersistentVolumeClaim` et les paramètres permettant de contrôler la façon dont Trident provisionne les volumes.

Déployer une application

Une fois la classe de stockage et le PVC créés, vous pouvez monter le PV sur un pod. Cette section présente la commande et la configuration d'exemple pour associer le PV à un pod.

Déployer une application exemple

Étapes

1. Montez le volume dans un pod.

```
kubectl create -f pv-pod.yaml
```

Ces exemples montrent des configurations de base pour attacher le PVC à un pod : **Configuration de base** :

```
kind: Pod
apiVersion: v1
metadata:
  name: pv-pod
spec:
  volumes:
  - name: pv-storage
    persistentVolumeClaim:
      claimName: basic
  containers:
  - name: pv-container
    image: nginx
    ports:
    - containerPort: 80
      name: "http-server"
  volumeMounts:
  - mountPath: "/my/mount/path"
    name: pv-storage
```



Vous pouvez surveiller la progression en utilisant `kubectl get pod --watch`.

2. Vérifiez que le volume est monté sur `/my/mount/path`.

```
kubectl exec -it pv-pod -- df -h /my/mount/path
```

```
Filesystem                                                    Size
Used Avail Use% Mounted on
192.168.188.78:/trident_pvc_ae45ed05_3ace_4e7c_9080_d2a83ae03d06 1.1G
320K 1.0G 1% /my/mount/path
```

Vous pouvez maintenant supprimer le Pod. L'application Pod n'existera plus, mais le volume restera.

```
kubectl delete pod pv-pod
```

Configurez le module complémentaire Trident EKS sur un cluster EKS

NetApp Trident simplifie la gestion du stockage Amazon FSx for NetApp ONTAP dans Kubernetes afin de permettre à vos développeurs et administrateurs de se concentrer sur le déploiement des applications. L'add-on NetApp Trident EKS inclut les derniers correctifs de sécurité, les corrections de bogues, et est validé par AWS pour fonctionner avec Amazon EKS. L'add-on EKS vous permet de garantir de manière cohérente que vos clusters Amazon EKS sont sécurisés et stables, et de réduire la quantité de travail nécessaire pour installer, configurer et mettre à jour les add-ons.

Prérequis

Assurez-vous de disposer des éléments suivants avant de configurer le module complémentaire Trident pour AWS EKS :

- Un compte de cluster Amazon EKS disposant des autorisations nécessaires pour gérer les modules complémentaires. Consultez "[Modules complémentaires Amazon EKS](#)".
- Autorisations AWS pour la AWS marketplace :
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Type d'AMI : Amazon Linux 2 (AL2_x86_64) ou Amazon Linux 2 Arm(AL2_ARM_64)
- Type de nœud : AMD ou ARM
- Un système de fichiers Amazon FSx for NetApp ONTAP existant

Étapes

1. Veillez à créer un rôle IAM et un secret AWS pour permettre aux pods EKS d'accéder aux ressources AWS. Pour obtenir des instructions, consultez "[Créez un rôle IAM et un secret AWS](#)".
2. Sur votre cluster Kubernetes EKS, accédez à l'onglet **Add-ons**.

The screenshot shows the AWS EKS console interface for a cluster named 'tri-env-eks'. At the top, there are buttons for 'Delete cluster', 'Upgrade version', and 'View dashboard'. A notification banner indicates the end of standard support for Kubernetes version 1.30 on July 28, 2025, with an 'Upgrade now' button. Below this, the 'Cluster info' section displays: Status (Active), Kubernetes version (1.30), Support period (Standard support until July 28, 2025), and Provider (EKS). The 'Cluster health issues' and 'Upgrade insights' sections both show 0 issues. The navigation bar includes tabs for Overview, Resources, Compute, Networking, Add-ons (1), Access, Observability, Update history, and Tags. A notification banner states 'New versions are available for 1 add-on.' The 'Add-ons (3)' section features a search bar, filters for 'Any category' and 'Any status', and shows '3 matches'.

3. Accédez à **AWS Marketplace add-ons** et choisissez la catégorie *storage*.

The screenshot shows the AWS Marketplace add-ons interface. At the top, it says "AWS Marketplace add-ons (1)" and "Discover, subscribe to and configure EKS add-ons to enhance your EKS clusters." There is a search bar with "Find add-on" and filtering options for "Any category", "NetApp, Inc.", and "Any pricing model". A "Clear filters" button is also present. Below the filters, there is a "NetApp, Inc." tag. The main content area displays the "NetApp Trident" add-on. It includes a description: "NetApp Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows." There is a "Standard Contract" badge. Below the description, there are four columns of information: "Category" (storage), "Listed by" (NetApp, Inc.), "Supported versions" (1.31, 1.30, 1.29, 1.28, 1.27, 1.26, 1.25, 1.24, 1.23), and "Pricing starting at" (View pricing details). At the bottom right, there are "Cancel" and "Next" buttons.

4. Repérez **NetApp Trident** et cochez la case de l'extension Trident, puis cliquez sur **Suivant**.

5. Choisissez la version souhaitée du module complémentaire.

The screenshot shows the "Configure selected add-ons settings" page. It has a title "Configure selected add-ons settings" and a subtitle "Configure the add-ons for your cluster by selecting settings." The main content area is for "NetApp Trident". It shows "Listed by" as "NetApp", "Category" as "storage", and "Status" as "Ready to install". There is a "Remove add-on" button. Below this, there is a notification: "You're subscribed to this software. You can view the terms and pricing details for this product or choose another offer if one is available." with a "View subscription" button. There is a "Version" section with a dropdown menu showing "v25.6.0-eksbuild.1". Below the version dropdown, there is a section for "Optional configuration settings". At the bottom right, there are "Cancel", "Previous", and "Next" buttons.

6. Configurez les paramètres du module complémentaire requis.

Review and add

Step 1: Select add-ons

Edit

Selected add-ons (1)

Find add-on

Add-on name	Type	Status
netapp_trident-operator	storage	Ready to install

Step 2: Configure selected add-ons settings

Edit

Selected add-ons version (1)

Add-on name	Version	IAM role for service account (IRSA)
netapp_trident-operator	v24.10.0-eksbuild.1	Not set

EKS Pod Identity (0)

Add-on name	IAM role	Service account
No Pod Identity associations None of the selected add-on(s) have Pod Identity associations.		

Cancel

Previous

Create

- Si vous utilisez IRSA (IAM roles for service account), reportez-vous aux étapes de configuration supplémentaires "ici".
- Sélectionnez **Create**.
- Vérifiez que le statut du module complémentaire est *Active*.

Add-ons (1) Info

View details Edit Remove Get more add-ons

netapp

Any categ... Any status 1 match

NetApp **NetApp Trident**

NetApp Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to let your developers and administrators focus on application deployment. FSx for ONTAP flexibility, scalability, and integration capabilities make it the ideal choice for organizations seeking efficient containerized storage workflows. [Product details](#)

Category	Status	Version	EKS Pod Identity	IAM role for service account (IRSA)
storage	Active	v24.10.0-eksbuild.1	-	Not set

Listed by [NetApp, Inc.](#)

View subscription

- Exécutez la commande suivante pour vérifier que Trident est correctement installé sur le cluster :

```
kubectl get pods -n trident
```

11. Poursuivez l'installation et configurez le stockage backend. Pour plus d'informations, consultez "[Configurer le backend de stockage](#)".

Installez/désinstallez l'add-on Trident EKS à l'aide de la CLI

Installez le module complémentaire NetApp Trident EKS à l'aide de l'interface de ligne de commande :

La commande suivante installe le module complémentaire Trident EKS :

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.0-eksbuild.1 (avec une version dédiée)
```

L'exemple de commande suivant installe le Trident EKS add-on version 25.6.1 :

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.1-eksbuild.1 (avec une version dédiée)
```

L'exemple de commande suivant installe le Trident EKS add-on version 25.6.2 :

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.2-eksbuild.1 (avec une version dédiée)
```

Désinstallez le module complémentaire NetApp Trident EKS à l'aide de l'interface de ligne de commande :

La commande suivante désinstalle le module complémentaire Trident EKS :

```
eksctl delete addon --cluster K8s-arm --name netapp_trident-operator
```

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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