Amazon FSx for NetApp ONTAP

Trident

NetApp
January 15, 2026

Sommaire

Amazon FSx for NetApp ONTAP

Utiliser Trident avec Amazon FSx for NetApp ONTAP

"Amazon FSx for NetApp ONTAP"est un service AWS entièrement géré qui permet aux clients de lancer et d'exécuter des systèmes de fichiers alimentés par le système d'exploitation de stockage NetApp ONTAP . FSx for ONTAP vous permet de tirer parti des fonctionnalités, des performances et des capacités d'administration de NetApp que vous connaissez, tout en bénéficiant de la simplicité, de l'agilité, de la sécurité et de l'évolutivité du stockage des données sur AWS. FSx pour ONTAP prend en charge les fonctionnalités du système de fichiers ONTAP et les API d'administration.

Vous pouvez intégrer votre système de fichiers Amazon FSx for NetApp ONTAP avec Trident pour garantir que les clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS) peuvent provisionner des volumes persistants de blocs et de fichiers pris en charge par ONTAP.

Dans Amazon FSx, le système de fichiers est la ressource principale, analogue à un cluster ONTAP sur site. Au sein de chaque SVM, vous pouvez créer un ou plusieurs volumes, qui sont des conteneurs de données stockant les fichiers et les dossiers de votre système de fichiers. Avec Amazon FSx for NetApp ONTAP, un système de fichiers géré dans le cloud sera fourni. Le nouveau type de système de fichiers s'appelle * NetApp ONTAP*.

En utilisant Trident avec Amazon FSx for NetApp ONTAP, vous pouvez garantir que les clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS) peuvent provisionner des volumes persistants de blocs et de fichiers pris en charge par ONTAP.

Exigences

En plus de"exigences de Trident" Pour intégrer FSx for ONTAP à 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 et une machine virtuelle de stockage (SVM) existants, accessibles depuis les nœuds de travail de votre cluster.
- Les nœuds de travail qui sont préparés pour"NFS ou iSCSI" .

> ⓘ Veillez à suivre les étapes de préparation des nœuds requises pour Amazon Linux et Ubuntu. "Images de machines Amazon" (AMI) en fonction de votre type d'AMI EKS.

Considérations

- Volumes SMB :
  - Les volumes SMB sont pris en charge à l'aide de `ontap-nas` conducteur seulement.
  - Les volumes SMB ne sont pas pris en charge par l'extension Trident EKS.
  - Trident prend uniquement en charge les volumes SMB montés sur des pods exécutés sur des nœuds Windows. Se référer à "Préparez-vous à provisionner des volumes PME" pour plus de détails.
- Avant Trident 24.02, les volumes créés sur des systèmes de fichiers Amazon FSx dont les sauvegardes automatiques sont 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 backend pour AWS FSx pour ONTAP.

> Si vous spécifiez un rôle IAM pour Trident, vous pouvez omettre de spécifier le `apiRegion` , `apiKey` , et `secretKey` champs à Trident explicitement. Pour plus d'informations, veuillez consulter"Options et exemples de configuration de FSx pour ONTAP" .

Utilisation simultanée des pilotes Trident SAN/iSCSI et 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 multi-chemin requise sur les nœuds peut entrer en conflit avec le pilote CSI Amazon Elastic Block Store (EBS). Pour garantir que le multivoie fonctionne sans interférer avec les disques EBS sur le même nœud, vous devez exclure EBS dans votre configuration de multivoie. Cet exemple montre un `multipath.conf` fichier contenant les paramètres Trident requis tout en excluant les disques EBS du multipathing :

```
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 le `fsxadmin` utilisateur pour votre système de fichiers ou le `vsadmin` utilisateur configuré pour votre SVM.

> Trident prévoit d'être géré comme un `vsadmin` Utilisateur SVM ou en tant qu'utilisateur avec un nom différent mais ayant le même rôle. Amazon FSx for NetApp ONTAP possède un `fsxadmin` utilisateur qui remplace partiellement l' ONTAP `admin` utilisateur du cluster. Nous recommandons fortement d'utiliser `vsadmin` avec Trident.

- Communication par 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 la documentation relative à l'authentification de votre type de pilote :

- "Authentification ONTAP NAS"
- "Authentification SAN ONTAP"

Images machine Amazon (AMI) testées

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

AMI	NAS	NAS-économie	iSCSI	économie iSCSI
AL2023_x86_64_STANDARD	Oui	Oui	Oui	Oui
AL2_x86_64	Oui	Oui	Oui*	Oui*
BOTTLEROCKET_x86_64	Oui**	Oui	S/O	S/O
AL2023_ARM_64_STANDARD	Oui	Oui	Oui	Oui
AL2_ARM_64	Oui	Oui	Oui*	Oui*
BOTTLEROCKET_ARM_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 connues pour fonctionner.

Tests effectués avec :

- Version EKS : 1.32
- Méthode d'installation : Helm 25.06 et en tant que module complémentaire AWS 25.06
- Pour le NAS, les protocoles NFSv3 et NFSv4.1 ont été testés.
- Pour le SAN, seul l'iSCSI a été testé, et non le NVMe-oF.

Tests effectués :

- Créer : Classe de stockage, PVC, capsule
- Supprimer : pod, pvc (standard, qtree/lun – économique, NAS avec sauvegarde AWS)

Trouver 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 informations

d’identification 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 serveur virtuel FSx pour gérer le stockage à votre place, il aura besoin d’identifiants pour ce faire. La méthode la plus sûre pour transmettre ces informations d’identification 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 informations d’identification 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. Vous devez donc créer une politique qui accorde à Trident les autorisations nécessaires.

Les exemples suivants créent une stratégie IAM à l’aide de l’interface de ligne de commande AWS :

```
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 politique :

```
{
  "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 assumer un rôle AWS Identity and Access Management (IAM) avec EKS Pod Identity ou un rôle IAM pour l'association de compte de service (IRSA). Tous les pods configurés pour utiliser le compte de service peuvent alors accéder à n'importe quel service AWS auquel le rôle a 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.

Installer 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, veuillez consulter"Configurer l'agent d'identité du pod Amazon EKS" .

Créer trust-relationship.json :

Créez un fichier trust-relationship.json pour permettre au principal de service EKS d'assumer ce rôle pour l'identité du pod. Créez ensuite un rôle avec cette politique de confiance :

```
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 comptes 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 `trust-relationship.json` déposer:

- **<account_id>** - Votre ID de compte AWS
- **<oidc_provider>** - L'OIDC de votre cluster EKS. Vous pouvez obtenir le fournisseur oidc 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 (créée à l'étape précédente) 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 :

- Barre
- Module complémentaire EKS

Si vous souhaitez utiliser la fonctionnalité de capture d'instantané, installez l'extension CSI snapshot controller. Se référer à"Activer la fonctionnalité de snapshot pour les volumes CSI" pour plus d'informations.

Installez Trident via Helm.

Identité du pod

1. Ajouter 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 le `helm list` commande permettant de consulter les détails d'installation tels que le nom, l'espace de noms, le graphique, 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. Ajouter le dépôt Trident Helm :

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

2. Définissez les valeurs de **fournisseur de cloud** et **identité cloud** :

```
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 le `helm list` commande permettant de consulter les détails d'installation tels que le nom, l'espace de noms, le graphique, 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-
100.2506.0    25.06.0
```

Si vous prévoyez d'utiliser iSCSI, assurez-vous que iSCSI est activé sur votre machine cliente. Si vous utilisez le système d'exploitation du nœud de travail AL2023, vous pouvez automatiser l'installation du client iSCSI en ajoutant le paramètre node prep dans l'installation helm :

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

Installez Trident via l'extension EKS

Le module complémentaire Trident EKS inclut les derniers correctifs de sécurité et de bogues, et est validé par AWS pour fonctionner avec Amazon EKS. Le module complémentaire EKS vous permet de garantir en permanence la sécurité et la stabilité de vos clusters Amazon EKS et de réduire le travail nécessaire à l'installation, à la configuration et à la mise à jour des modules complémentaires.

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 place de marché AWS :
  `"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

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 **Obtenir plus de modules complémentaires**.
5. Suivez ces étapes pour sélectionner le module complémentaire :
   a. Faites défiler vers le bas jusqu'à la section **modules complémentaires AWS Marketplace** et tapez **"Trident"** dans la zone de recherche.
   b. Cochez la case située dans le coin supérieur droit de la boîte Trident by NetApp .
   c. Sélectionnez **Suivant**.
6. Sur la page des paramètres **Configurer les modules complémentaires sélectionnés**, procédez comme suit :

   Ignorez ces étapes si vous utilisez l'association d'identité de pod.

   a. Sélectionnez la **Version** 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 **Version** 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 rôle-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 Remplacer comme méthode de résolution des conflits, un ou plusieurs paramètres du module complémentaire existant peuvent être remplacés par les paramètres du module complémentaire Amazon EKS. Si vous n'activez pas cette option et qu'il y a un conflit avec vos paramètres existants, l'opération échouera. Vous pouvez utiliser le message d'erreur généré pour résoudre le conflit. Avant de sélectionner cette option, assurez-vous que le module complémentaire 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 module complémentaire terminée, vous verrez le module complémentaire installé.

AWS CLI

1. Créez le `add-on.json` déposer:

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

```
{
  "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"
  }
}
```

Remplacer `<role ARN>` avec l'ARN du rôle créé à l'étape précédente.

2. Installez le module 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 module complémentaire NetApp Trident CSI.
4. Sélectionnez l'onglet **Modules complémentaires**.
5. Sélectionnez * Trident by NetApp* puis sélectionnez **Modifier**.
6. Sur la page **Configurer Trident by NetApp**, procédez comme suit :
   a. Sélectionnez la **Version** que vous souhaitez utiliser.
   b. Développez la section **Paramètres de configuration optionnels** et modifiez-les selon vos besoins.
   c. Sélectionnez **Enregistrer les modifications**.

AWS CLI

L'exemple suivant met à jour le module complémentaire 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 module complémentaire FSxN Trident CSI. Remplacer `my-cluster` avec le nom de votre cluster.

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

  Exemple de résultat :

```
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 module complémentaire avec la version renvoyée sous MISE À JOUR DISPONIBLE 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 retirez le `--force` Si une option et l'un des paramètres du module complémentaire Amazon EKS entrent 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 des paramètres que vous devez gérer, car ces paramètres seront écrasés par 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 Amazon EKS Kubernetes, consultez"Gestion des champs Kubernetes" .

Désinstallez/supprimez le module complémentaire Trident EKS.

Vous avez deux options pour supprimer un module complémentaire Amazon EKS :

- **Conserver les logiciels complémentaires sur votre cluster** – Cette option supprime la gestion des paramètres par Amazon EKS. Cela supprime également la possibilité pour Amazon EKS de vous informer des mises à jour et de mettre à jour automatiquement le module complémentaire Amazon EKS après que vous ayez lancé une mise à jour. Toutefois, il préserve les logiciels complémentaires sur votre cluster. Cette option transforme l'extension en une installation autogérée, plutôt qu'en une extension Amazon EKS. Avec cette option, l'extension ne nécessite aucune interruption de service. Conservez le `--preserve` option dans la commande pour conserver le module complémentaire.
- **Supprimez complètement le logiciel complémentaire de votre cluster** – NetApp recommande de supprimer le module complémentaire Amazon EKS de votre cluster uniquement si aucune ressource de votre cluster n'en dépend. Retirez le `--preserve` l'option de l' `delete` commande pour supprimer l'extension.

Si le module complémentaire est associé à un compte IAM, ce 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 module complémentaire NetApp Trident CSI.
4. Sélectionnez l'onglet **Modules complémentaires** puis * Trident by NetApp*.
5. Sélectionnez **Supprimer**.
6. Dans la boîte de dialogue **Confirmation de suppression de netapp_trident-operator**, procédez comme suit :
   a. Si vous souhaitez qu'Amazon EKS cesse de gérer les paramètres de l'extension, sélectionnez **Conserver sur le cluster**. Faites ceci si vous souhaitez conserver le logiciel complémentaire sur votre cluster afin de pouvoir gérer vous-même tous les paramètres de ce module.
   b. Saisissez **netapp_trident-operator**.
   c. Sélectionnez **Supprimer**.

AWS CLI

Remplacer `my-cluster` avec 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 le système de stockage dorsal

Intégration des pilotes ONTAP SAN et NAS

Pour créer un système de stockage, vous devez créer un fichier de configuration au format JSON ou YAML. Le fichier doit préciser le type de stockage souhaité (NAS ou SAN), le système de fichiers, le SVM à partir duquel le récupérer et la méthode d'authentification. L'exemple suivant montre comment définir un stockage basé sur un 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:xxxxxxxx: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:xxxxxxxx:secret:secret-
name",
      "type": "awsarn"
    }
  }
}
```

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
PHASE   STATUS

backend-tbc-ontap-nas         tbc-ontap-nas         933e0071-66ce-4324-
b9ff-f96d916ac5e9   Bound   Success
```

Détails du pilote FSx pour ONTAP

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

- `ontap-san`Chaque PV provisionné est un LUN au sein de son propre volume Amazon FSx for NetApp ONTAP . Recommandé pour le stockage par blocs.
- `ontap-nas`Chaque PV provisionné est un volume Amazon FSx for NetApp ONTAP . Recommandé pour NFS et SMB.
- `ontap-san-economy`Chaque PV provisionné est un LUN avec un nombre configurable de LUN par volume Amazon FSx for NetApp ONTAP .
- `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 complet Amazon FSx for NetApp ONTAP FlexGroup .

Pour plus de détails sur le conducteur, veuillez consulter"Pilotes NAS" et"Pilotes SAN" .

Une fois le fichier de configuration créé, exécutez cette commande pour le créer dans votre EKS :

```
kubectl create -f configuration_file
```

Pour vérifier l'état, exécutez la commande suivante :

```
kubectl get tbc -n trident
```

```
NAME                    BACKEND NAME            BACKEND UUID
PHASE   STATUS
backend-fsx-ontap-nas   backend-fsx-ontap-nas   7a551921-997c-4c37-a1d1-
f2f4c87fa629   Bound   Success
```

Configuration avancée et exemples du backend

Consultez le tableau suivant pour connaître 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 système de stockage	Nom du conducteur + "_" + dataLIF
`managementLIF`	Adresse IP d'une interface de gestion de cluster ou SVM (LIF) Un nom de domaine pleinement qualifié (FQDN) peut être spécifié. Peut être configuré pour utiliser des adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, comme [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si vous fournissez le `fsxFilesystemID` sous le `aws` champ, vous n'avez pas besoin de le fournir `managementLIF` car Trident récupère le SVM `managementLIF` Informations provenant d'AWS. Vous devez donc fournir les identifiants d'un utilisateur sous SVM (par exemple : vsadmin), et cet utilisateur doit disposer des `vsadmin` rôle.	"10.0.0.1", "[2001:1234:abcd::fefe]"

Paramètre	Description	Exemple
`dataLIF`	Adresse IP du protocole LIF. * Pilotes NAS ONTAP * : NetApp recommande de spécifier dataLIF. Si aucune donnée n'est fournie, Trident récupère les dataLIF à partir du SVM. Vous pouvez spécifier un nom de domaine pleinement qualifié (FQDN) à utiliser pour les opérations de montage NFS, ce qui vous permet de créer un DNS à répartition circulaire pour équilibrer la charge sur plusieurs dataLIF. Peut être modifié après la configuration initiale. Se référer à . * Pilotes SAN ONTAP * : Ne pas spécifier pour iSCSI. Trident utilise ONTAP Selective LUN Map pour découvrir les LIF iSCI nécessaires à l'établissement d'une session multi-chemin. Un avertissement est généré si dataLIF est explicitement défini. Peut être configuré pour utiliser des adresses IPv6 si Trident a été installé avec l'option IPv6. Les adresses IPv6 doivent être définies entre crochets, comme [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	
`autoExportPolicy`	Activer la création et la mise à jour automatiques de la politique d'exportation [Booléen]. En utilisant le `autoExportPolicy` et `autoExportCIDRs` Avec certaines options, Trident peut gérer automatiquement les politiques d'exportation.	`false`
`autoExportCIDRs`	Liste des CIDR à utiliser pour filtrer les adresses IP des nœuds Kubernetes lorsque `autoExportPolicy` est activé. En utilisant le `autoExportPolicy` et `autoExportCIDRs` Avec certaines options, Trident peut gérer automatiquement les politiques d'exportation.	"["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 basée sur les informations d'identification. Par exemple, vsadmin.	
`password`	Mot de passe pour se connecter au cluster ou à la SVM. Utilisé pour l'authentification basée sur les informations d'identification.	
`svm`	machine virtuelle de stockage à utiliser	Dérivé si un LIF de gestion SVM est spécifié.
`storagePrefix`	Préfixe utilisé lors de la mise en service de nouveaux volumes dans la SVM. Ne peut être modifié après sa création. Pour mettre à jour ce paramètre, vous devrez créer un nouveau backend.	`trident`
`limitAggregateUsage`	**Ne pas spécifier pour Amazon FSx for NetApp ONTAP.** Le fourni `fsxadmin` et `vsadmin` 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 échouera si la taille du volume demandée est supérieure à cette valeur. Il limite également la taille maximale des volumes qu'il gère pour les qtrees et les LUN, et le `qtreesPerFlexvol` Cette option permet de personnaliser le nombre maximal d'arbres qtree par FlexVol volume	"" (non appliqué par défaut)
`lunsPerFlexvol`	Le nombre maximal de LUN par volume Flexvol doit être compris entre 50 et 200. SAN uniquement.	"100"

Paramètre	Description	Exemple
`debugTraceFlags`	Indicateurs 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.	nul
`nfsMountOptions`	Liste des options de montage NFS séparées par des virgules. Les options de montage des volumes persistants Kubernetes sont normalement 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 dans la classe de stockage ou dans le fichier de configuration, Trident ne définira aucune option de montage sur un volume persistant associé.	""
`nasType`	Configurer la création de volumes NFS ou SMB. Les options sont `nfs` , `smb` , ou nul. **Doit être réglé sur `smb` pour les volumes SMB.** La valeur nulle correspond par défaut aux volumes NFS.	`nfs`
`qtreesPerFlexvol`	Le nombre maximal d'arbres Q par FlexVol volume doit être compris entre 50 et 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 serveurs backend Amazon FSx pour ONTAP .	`smb-share`

Paramètre	Description	Exemple
`useREST`	Paramètre booléen pour utiliser les API REST ONTAP . Lorsqu'il est réglé sur `true` Trident utilisera les API REST ONTAP pour communiquer avec le système dorsal. Cette fonctionnalité nécessite ONTAP 9.11.1 et versions ultérieures. De plus, le rôle de connexion ONTAP utilisé doit avoir accès à `ontap` application. Ceci est satisfait par la définition prédéfinie `vsadmin` et `cluster-admin` rôles.	`false`
`aws`	Vous pouvez spécifier les éléments suivants dans le fichier de configuration d'AWS FSx pour ONTAP: - `fsxFilesystemID` : Spécifiez l'ID du système de fichiers AWS FSx. - `apiRegion` : Nom de la région de l'API AWS. - `apikey` : Clé API AWS. - `secretKey` : Clé secrète AWS.	`""` `""` `""`
`credentials`	Spécifiez les informations d'identification FSx SVM à stocker dans AWS Secrets Manager. - `name` : Nom de ressource Amazon (ARN) du secret, qui contient les informations d'identification de la SVM. - `type` : Définir sur `awsarn` . Se référer à"Créer un secret AWS Secrets Manager" pour plus d'informations.	

Options de configuration backend pour les volumes de provisionnement

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

Paramètre	Description	Défaut
`spaceAllocation`	Allocation d'espace pour les LUN	`true`
`spaceReserve`	Mode de réservation d'espace ; « aucun » (fin) ou « volume » (épais)	`none`
`snapshotPolicy`	Politique d'instantané à utiliser	`none`

Paramètre	Description	Défaut
`qosPolicy`	Groupe de stratégie QoS à attribuer aux volumes créés. Choisissez l'une des options qosPolicy ou adaptiveQosPolicy par pool de stockage ou backend. L'utilisation des groupes de politiques QoS avec Trident nécessite ONTAP 9.8 ou une version ultérieure. Vous devez utiliser un groupe de stratégies QoS non partagé et vous assurer que ce groupe de stratégies est appliqué individuellement à chaque composant. Un groupe de politiques QoS partagé impose un plafond au débit total de toutes les charges de travail.	""
`adaptiveQosPolicy`	Groupe de stratégie QoS adaptatif à attribuer aux volumes créés. Choisissez l'une des options qosPolicy ou adaptiveQosPolicy par pool de stockage ou backend. Non pris en charge par ontap-nas-economy.	""
`snapshotReserve`	Pourcentage du volume réservé aux instantanés « 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` . Pour utiliser cette option, NVE doit être sous licence et activé sur le cluster. Si NAE est activé sur le système dorsal, tout volume provisionné dans Trident sera compatible NAE. Pour plus d'informations, veuillez consulter :"Comment Trident fonctionne avec NVE et NAE" .	`false`
`luksEncryption`	Activer le chiffrement LUKS. Se référer à"Utiliser 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 `mixed` et `unix` Styles de sécurité. Les PME prennent en charge `mixed` et `ntfs` Styles de sécurité.	La valeur par défaut de NFS est `unix` . La valeur par défaut de SMB est `ntfs` .

Préparez-vous à provisionner des volumes PME

Vous pouvez provisionner des volumes SMB à l'aide de `ontap-nas` conducteur. Avant de terminerIntégration des pilotes ONTAP SAN et NAS Veuillez suivre les étapes suivantes.

Avant de commencer

Avant de pouvoir provisionner des volumes SMB à l'aide de `ontap-nas` Conducteur, vous devez avoir les éléments suivants.

- Un cluster Kubernetes avec un nœud contrôleur Linux et au moins un nœud de travail Windows exécutant Windows Server 2019. Trident prend uniquement en charge les volumes SMB montés sur des pods exécutés sur des nœuds Windows.
- Au moins un secret Trident contenant vos informations d'identification Active Directory. Générer des secrets `smbcreds` :

```
kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='password'
```

- Un proxy CSI configuré comme un service Windows. Pour configurer un `csi-proxy` , se référer à"GitHub : CSI Proxy" ou"GitHub : CSI Proxy pour Windows" pour les nœuds Kubernetes exécutés sous Windows.

Étapes

1. Créer des partages SMB. Vous pouvez créer les partages d'administration SMB de deux manières : soit en utilisant…"Console de gestion Microsoft" composant logiciel enfichable Dossiers partagés ou via l'interface de ligne de commande ONTAP . Pour créer les partages SMB à l'aide de l'interface de ligne de commande ONTAP :
   a. Si nécessaire, créez la structure de chemin d'accès au répertoire partagé.

      Le `vserver cifs share create` Cette commande vérifie le chemin spécifié dans l'option -path lors de la création du partage. Si le chemin spécifié n'existe pas, la commande échoue.

   b. Créer un partage SMB associé à la SVM spécifiée :

```
vserver cifs share create -vserver vserver_name -share-name
share_name -path path [-share-properties share_properties,...]
[other_attributes] [-comment text]
```

   c. Vérifiez que le partage a bien été créé :

```
vserver cifs share show -share-name share_name
```

Se référer à"Créer un partage SMB" pour plus de détails.

2. Lors de la création du backend, vous devez configurer les éléments suivants pour spécifier les volumes SMB. Pour connaître toutes les options de configuration du backend FSx pour ONTAP , veuillez vous référer à"Options et exemples de configuration de FSx pour ONTAP" .

Paramètre	Description	Exemple
`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 serveurs backend Amazon FSx pour ONTAP .	`smb-share`
`nasType`	**Doit être réglé sur `smb` .** Si la valeur est nulle, la valeur par défaut est `nfs` .	`smb`
`securityStyle`	Style de sécurité pour les nouveaux volumes. **Doit être réglé sur `ntfs` ou `mixed` pour les volumes SMB.**	`ntfs`ou `mixed` pour les volumes SMB
`unixPermissions`	Mode pour les nouveaux volumes. **Doit rester vide pour les volumes SMB.**	""

Configurez une classe de stockage et un PVC.

Configurez un objet StorageClass Kubernetes et créez la classe de stockage pour indiquer à Trident comment provisionner les volumes. Créez une PersistentVolumeClaim (PVC) qui utilise la StorageClass Kubernetes configurée pour demander l'accès au PV. Vous pouvez ensuite monter le panneau photovoltaïque sur un support.

Créer une classe de stockage

Configurer un objet StorageClass Kubernetes

Le "Objet StorageClass Kubernetes" L'objet identifie Trident comme le provisionneur utilisé pour cette classe et indique à Trident comment provisionner un volume. Utilisez cet exemple pour configurer Storageclass pour les volumes utilisant NFS (reportez-vous à la section Attribut 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"
```

Utilisez cet exemple pour configurer Storageclass pour les 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"
```

Pour provisionner des volumes NFSv3 sur AWS Bottlerocket, ajoutez les éléments requis. `mountOptions` 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
```

Se référer à"Objets Kubernetes et Trident" pour plus de détails sur la manière dont les classes de stockage interagissent avec le `PersistentVolumeClaim` et des paramètres permettant de contrôler les volumes de provisionnement de Trident .

Créer une classe de stockage

Étapes

1. Il s'agit d'un objet Kubernetes, donc utilisez-le `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 détecté les pools sur le backend.

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

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

Créer le PVC

UN "*PersistentVolumeClaim*" (PVC) est une demande d'accès au PersistentVolume sur le cluster.

Le PVC peut être configuré pour demander un stockage d'une certaine taille ou un certain mode d'accès. En utilisant la StorageClass associée, l'administrateur du cluster peut contrôler bien plus que la taille et le mode d'accès du PersistentVolume, comme par exemple les performances ou le niveau de service.

Une fois le PVC créé, vous pouvez monter le volume dans un boîtier.

Exemples de manifestes

Manifestes d'exemple de PersistentVolumeClaim

Ces exemples illustrent les options de configuration de base pour les installations en PVC.

PVC avec accès RWX

Cet exemple montre un PVC de base avec accès RWX associé à une StorageClass nommée `basic-csi`.

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

Exemple de PVC utilisant iSCSI

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

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

Créer PVC

Étapes

1. Créez le PVC.

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

2. Vérifier l'état du PVC.

```
kubectl get pvc
```

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

Se référer à"Objets Kubernetes et Trident" pour plus de détails sur la manière dont les classes de stockage interagissent avec le `PersistentVolumeClaim` et des paramètres permettant de contrôler les volumes de provisionnement de Trident .

attributs du Trident

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	disque dur, hybride, SSD	La piscine contient des médias de ce type ; hybride signifie à la fois	Type de média spécifié	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
type de provisionnement	chaîne	mince, épais	Pool prend en charge cette méthode d'approvisionnement	Méthode de provisionnement spécifiée	Épais : tous les produits Ontap ; mince : tous les produits Ontap et Solidfire-San
Type de backend	chaîne	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Pool appartient à ce type de backend	Backend spécifié	Tous les conducteurs
instantanés	booléen	vrai, faux	Pool prend en charge les volumes avec instantanés	Volume avec instantanés activés	ontap-nas, ontap-san, solidfire-san, gcp-cvs
clones	booléen	vrai, faux	Pool prend en charge les volumes de clonage	Volume avec clones activés	ontap-nas, ontap-san, solidfire-san, gcp-cvs

Attribut	Type	Valeurs	Offre	Demande	Soutenu par
cryptage	booléen	vrai, faux	Pool prend en charge les volumes chiffrés	Volume avec chiffrement activé	ontap-nas, ontap-nas-économie, ontap-nas-groupes flexibles, ontap-san
Op E/S par sec	int	entier positif	Pool est capable de garantir des IOPS dans cette plage.	Volume garanti pour ces IOPS	solidefire-san

[1] : Non pris en charge par les systèmes ONTAP Select

Déployer l'application exemple

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

Étapes

1. Montez le volume dans un boîtier.

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

Ces exemples montrent des configurations de base pour fixer le PVC à un module : **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 suivre les progrès 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. Le module complémentaire NetApp Trident EKS inclut

les derniers correctifs de sécurité et de bogues, et est validé par AWS pour fonctionner avec Amazon EKS. Le module complémentaire EKS vous permet de garantir en permanence la sécurité et la stabilité de vos clusters Amazon EKS et de réduire le travail nécessaire à l'installation, à la configuration et à la mise à jour des modules complémentaires.

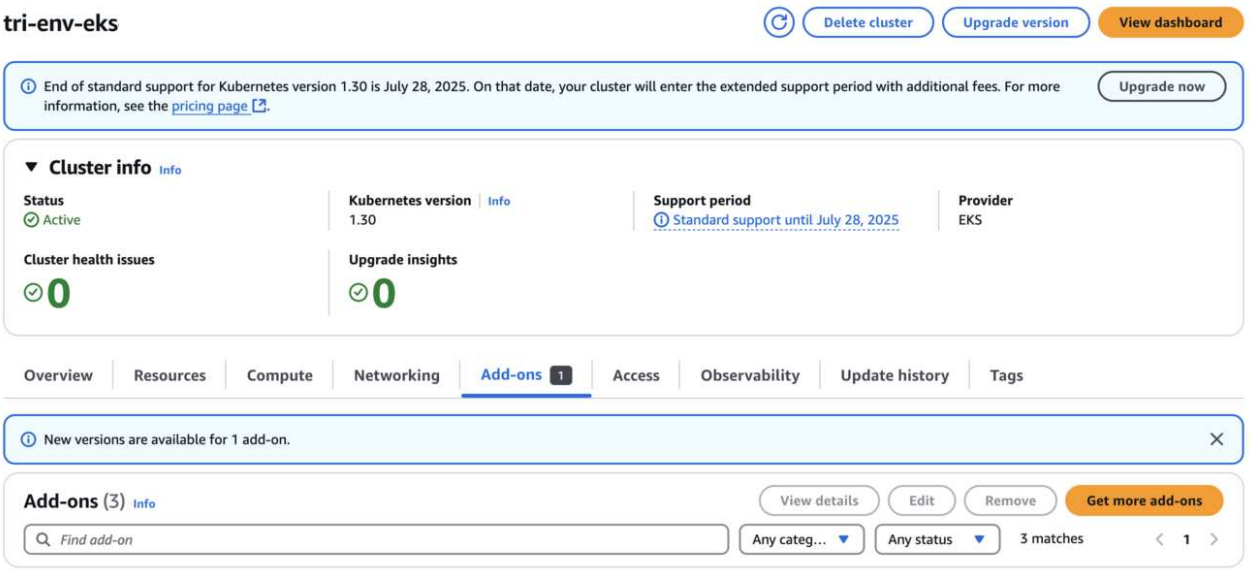
Prérequis

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

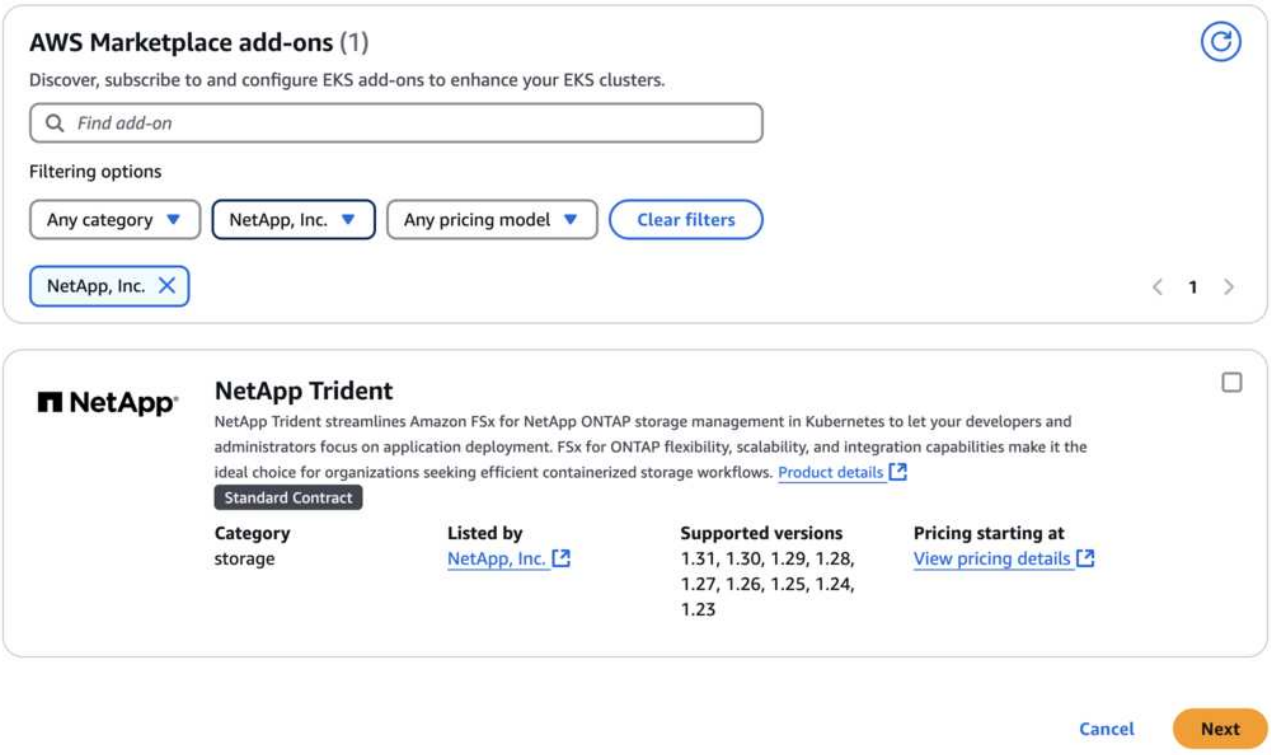
- Un compte de cluster Amazon EKS disposant des autorisations nécessaires pour utiliser des modules complémentaires. Se référer à"Modules complémentaires Amazon EKS" .
- Autorisations AWS pour la place de marché AWS :
  `"aws-marketplace:ViewSubscriptions",`
  `"aws-marketplace:Subscribe",`
  `"aws-marketplace:Unsubscribe`
- 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

Étapes

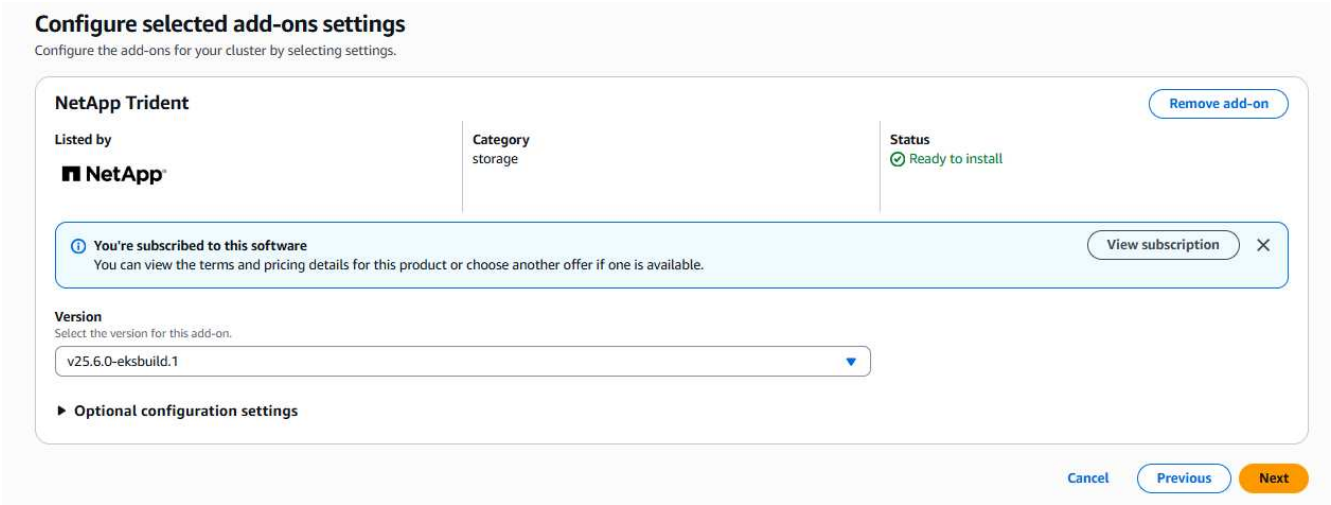
1. Veillez à créer un rôle IAM et un secret AWS pour permettre aux pods EKS d'accéder aux ressources AWS. Pour les instructions, voir"Créez un rôle IAM et un secret AWS." .
2. Sur votre cluster Kubernetes EKS, accédez à l'onglet **Modules complémentaires**.



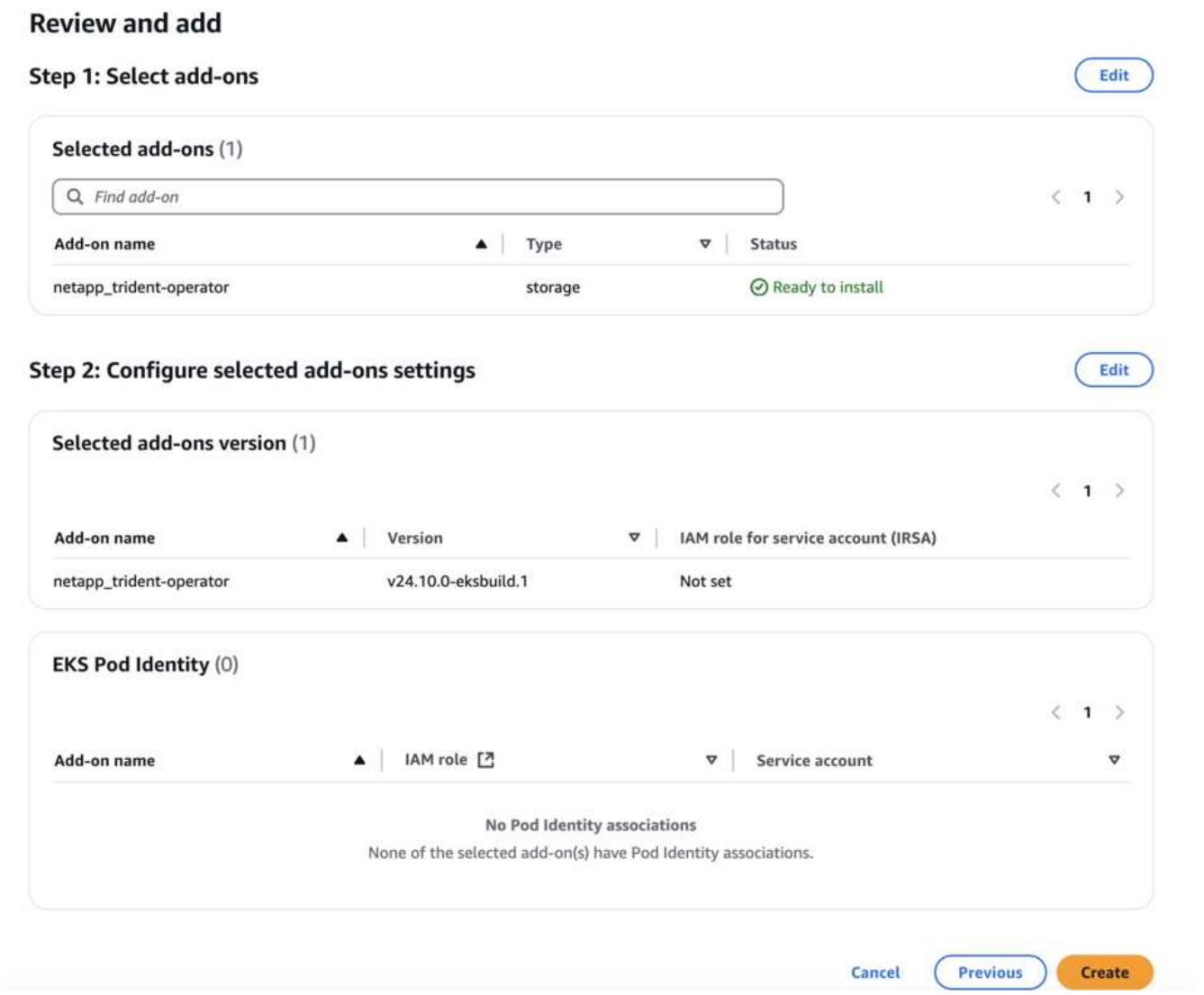
3. Accédez à **AWS Marketplace add-ons** et choisissez la catégorie *stockage*.



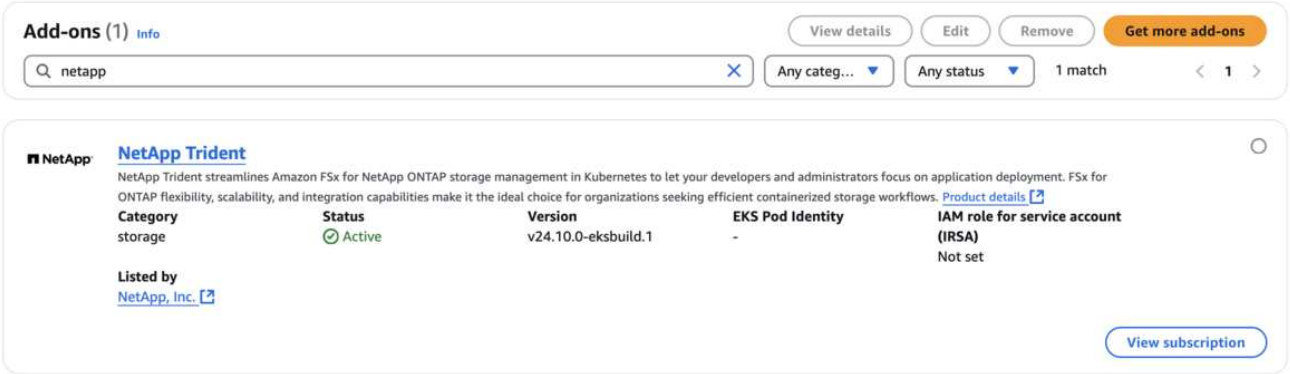
4. Localisez * NetApp Trident* et cochez la case correspondant au module complémentaire Trident , puis cliquez sur **Suivant**.
5. Choisissez la version souhaitée du module complémentaire.



6. Configurez les paramètres du module complémentaire requis.



7. Si vous utilisez IRSA (rôles IAM pour compte de service), reportez-vous aux étapes de configuration supplémentaires."ici" .
8. Sélectionnez **Créer**.
9. Vérifiez que le statut du module complémentaire est *Actif*.



10. 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 système de stockage. Pour plus d'informations, voir"Configurer le système de stockage dorsal" .

Installez/désinstallez l'extension Trident EKS via l'interface de ligne de commande (CLI).

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

La commande suivante permet d'installer le module complémentaire Trident EKS : `eksctl create addon --cluster clusterName --name netapp_trident-operator --version v25.6.0-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

Informations sur les marques commerciales