Amazon FSx for NetApp ONTAP

Trident

NetApp
January 15, 2026

Inhalt

Amazon FSx for NetApp ONTAP

Trident mit Amazon FSx for NetApp ONTAP verwenden

"Amazon FSx for NetApp ONTAP"ist ein vollständig verwalteter AWS-Service, der es Kunden ermöglicht, Dateisysteme zu starten und auszuführen, die auf dem Speicherbetriebssystem NetApp ONTAP basieren. FSx for ONTAP ermöglicht es Ihnen, die Ihnen vertrauten Funktionen, die Leistung und die administrativen Möglichkeiten von NetApp zu nutzen und gleichzeitig die Einfachheit, Agilität, Sicherheit und Skalierbarkeit der Datenspeicherung auf AWS in Anspruch zu nehmen. FSx für ONTAP unterstützt die Funktionen des ONTAP -Dateisystems und die Administrations-APIs.

Sie können Ihr Amazon FSx for NetApp ONTAP Dateisystem mit Trident integrieren, um sicherzustellen, dass Kubernetes-Cluster, die im Amazon Elastic Kubernetes Service (EKS) ausgeführt werden, persistente Block- und Dateivolumes bereitstellen können, die von ONTAP unterstützt werden.

Das Dateisystem ist die primäre Ressource in Amazon FSx, analog zu einem ONTAP Cluster vor Ort. Innerhalb jeder SVM können Sie ein oder mehrere Volumes erstellen. Dabei handelt es sich um Datencontainer, in denen die Dateien und Ordner Ihres Dateisystems gespeichert werden. Mit Amazon FSx for NetApp ONTAP wird ein verwaltetes Dateisystem in der Cloud bereitgestellt. Der neue Dateisystemtyp heißt * NetApp ONTAP*.

Durch die Verwendung von Trident mit Amazon FSx for NetApp ONTAP können Sie sicherstellen, dass Kubernetes-Cluster, die im Amazon Elastic Kubernetes Service (EKS) ausgeführt werden, persistente Block- und Dateivolumes bereitstellen können, die von ONTAP unterstützt werden.

Anforderungen

Zusätzlich zu"Trident Anforderungen" Um FSx für ONTAP mit Trident zu integrieren, benötigen Sie:

- Ein bestehender Amazon EKS-Cluster oder ein selbstverwalteter Kubernetes-Cluster mit `kubectl` installiert.
- Ein vorhandenes Amazon FSx for NetApp ONTAP Dateisystem und eine Storage Virtual Machine (SVM), die von den Worker-Knoten Ihres Clusters aus erreichbar ist.
- Worker-Knoten, die vorbereitet sind für"NFS oder iSCSI" .

> Stellen Sie sicher, dass Sie die für Amazon Linux und Ubuntu erforderlichen Schritte zur Knotenvorbereitung befolgen. "Amazon Machine Images" (AMIs) abhängig von Ihrem EKS-AMI-Typ.

Überlegungen

- SMB-Volumes:
  - SMB-Volumes werden mithilfe von `ontap-nas` Nur für den Fahrer.
  - SMB-Volumes werden vom Trident EKS-Add-on nicht unterstützt.
  - Trident unterstützt SMB-Volumes nur, wenn sie in Pods eingebunden sind, die auf Windows-Knoten laufen. Siehe "Bereiten Sie die Bereitstellung von SMB-Volumes vor" für Details.

- Vor Trident 24.02 konnten Volumes, die auf Amazon FSx Dateisystemen mit aktivierter automatischer Datensicherung erstellt wurden, von Trident nicht gelöscht werden. Um dieses Problem in Trident 24.02 oder höher zu vermeiden, geben Sie Folgendes an: `fsxFilesystemID` AWS `apiRegion` AWS `apikey` und AWS `secretKey` in der Backend-Konfigurationsdatei für AWS FSx für ONTAP.

> Wenn Sie Trident eine IAM-Rolle zuweisen, können Sie die Angabe der `apiRegion` , `apiKey` , Und `secretKey` Felder explizit an Trident übergeben. Weitere Informationen finden Sie unter"FSx für ONTAP: Konfigurationsoptionen und Beispiele" .

Gleichzeitige Nutzung von Trident SAN/iSCSI und EBS-CSI-Treiber

Wenn Sie Ontap-San-Treiber (z. B. iSCSI) mit AWS (EKS, ROSA, EC2 oder einer anderen Instanz) verwenden möchten, kann es bei der auf den Knoten erforderlichen Multipath-Konfiguration zu Konflikten mit dem CSI-Treiber von Amazon Elastic Block Store (EBS) kommen. Um sicherzustellen, dass Multipathing funktioniert, ohne EBS-Festplatten auf demselben Knoten zu beeinträchtigen, müssen Sie EBS aus Ihrem Multipathing-Setup ausschließen. Dieses Beispiel zeigt ein `multipath.conf` Datei, die die erforderlichen Trident Einstellungen enthält und gleichzeitig EBS-Festplatten vom Multipathing ausschließt:

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

Authentifizierung

Trident bietet zwei Authentifizierungsmodi an.

- Anmeldeinformationsbasiert (Empfohlen): Speichert Anmeldeinformationen sicher im AWS Secrets Manager. Sie können die `fsxadmin` Benutzer für Ihr Dateisystem oder die `vsadmin` Benutzerkonfiguriert für Ihre SVM.

> Trident geht davon aus, als ein `vsadmin` SVM-Benutzer oder als Benutzer mit einem anderen Namen, der die gleiche Rolle hat. Amazon FSx for NetApp ONTAP hat ein `fsxadmin` Benutzer, der einen eingeschränkten Ersatz für ONTAP darstellt. `admin` Clusterbenutzer. Wir empfehlen dringend die Verwendung `vsadmin` mit Trident.

- Zertifikatsbasiert: Trident kommuniziert mit der SVM auf Ihrem FSx-Dateisystem mithilfe eines auf Ihrer SVM installierten Zertifikats.

Einzelheiten zur Aktivierung der Authentifizierung finden Sie in der Dokumentation zur Authentifizierung für Ihren Treibertyp:

- "ONTAP NAS-Authentifizierung"

- "ONTAP SAN-Authentifizierung"

Getestete Amazon Machine Images (AMIs)

Der EKS-Cluster unterstützt verschiedene Betriebssysteme, aber AWS hat bestimmte Amazon Machine Images (AMIs) für Container und EKS optimiert. Die folgenden AMIs wurden mit NetApp Trident 25.02 getestet.

AMI	NAS	NAS-Wirtschaft	iSCSI	iSCSI-Economy
AL2023_x86_64_STANDARD	Ja	Ja	Ja	Ja
AL2_x86_64	Ja	Ja	Ja*	Ja*
BOTTLEROCKET_x86_64	Ja**	Ja	k. A.	k. A.
AL2023_ARM_64_STANDARD	Ja	Ja	Ja	Ja
AL2_ARM_64	Ja	Ja	Ja*	Ja*
BOTTLEROCKET_ARM_64	Ja**	Ja	k. A.	k. A.

- * Das Löschen des PV ist ohne Neustart des Knotens nicht möglich
- ** Funktioniert nicht mit NFSv3 mit Trident Version 25.02.

Wenn Ihr gewünschtes AMI hier nicht aufgeführt ist, bedeutet das nicht, dass es nicht unterstützt wird; es bedeutet lediglich, dass es nicht getestet wurde. Diese Liste dient als Leitfaden für AMIs, von denen bekannt ist, dass sie funktionieren.

Tests durchgeführt mit:

- EKS-Version: 1.32
- Installationsmethode: Helm 25.06 und als AWS-Add-On 25.06
- Für NAS wurden sowohl NFSv3 als auch NFSv4.1 getestet.
- Für SAN wurde nur iSCSI getestet, nicht NVMe-oF.

Durchgeführte Tests:

- Erstellen: Speicherklasse, PVC, Kapsel
- Löschen: Pod, PVC (regulär, Qtree/LUN – Economy, NAS mit AWS-Backup)

Weitere Informationen

- "Amazon FSx for NetApp ONTAP -Dokumentation"
- "Blogbeitrag über Amazon FSx for NetApp ONTAP"

Erstellen Sie eine IAM-Rolle und ein AWS-Geheimnis.

Sie können Kubernetes-Pods so konfigurieren, dass sie auf AWS-Ressourcen zugreifen, indem sie sich als AWS-IAM-Rolle authentifizieren, anstatt explizite AWS-Anmeldeinformationen anzugeben.

Zur Authentifizierung mit einer AWS IAM-Rolle benötigen Sie einen Kubernetes-Cluster, der mit EKS bereitgestellt wurde.

AWS Secrets Manager-Geheimnis erstellen

Da Trident APIs an einen FSx vServer ausgibt, um den Speicher für Sie zu verwalten, benötigt es hierfür Anmeldeinformationen. Die sicherste Methode zur Übermittlung dieser Zugangsdaten ist die Verwendung eines AWS Secrets Manager-Geheimnisses. Wenn Sie also noch keines haben, müssen Sie ein AWS Secrets Manager-Geheimnis erstellen, das die Anmeldeinformationen für das vsadmin-Konto enthält.

Dieses Beispiel erstellt ein AWS Secrets Manager-Geheimnis zum Speichern von Trident CSI-Anmeldeinformationen:

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

IAM-Richtlinie erstellen

Trident benötigt außerdem AWS-Berechtigungen, um korrekt ausgeführt werden zu können. Daher müssen Sie eine Richtlinie erstellen, die Trident die benötigten Berechtigungen erteilt.

Die folgenden Beispiele erstellen eine IAM-Richtlinie mithilfe der 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"
```

Beispiel für eine Richtlinien-JSON-Datei:

```
{
  "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"
}
```

Pod-Identität oder IAM-Rolle für die Dienstkontozuordnung (IRSA) erstellen

Sie können ein Kubernetes-Servicekonto so konfigurieren, dass es eine AWS Identity and Access Management (IAM)-Rolle mit EKS Pod Identity oder IAM role for Service account association (IRSA) übernimmt. Alle Pods, die für die Verwendung des Servicekontos konfiguriert sind, können dann auf jeden AWS-Service zugreifen, für den die Rolle Berechtigungen besitzt.

Pod-Identität

Amazon EKS Pod Identity-Zuordnungen bieten die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie Amazon EC2-Instanzprofile Anmeldeinformationen für Amazon EC2-Instanzen bereitstellen.

Installieren Sie Pod Identity auf Ihrem EKS-Cluster:

Sie können eine Pod-Identität über die AWS-Konsole oder mithilfe des folgenden AWS CLI-Befehls erstellen:

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

Weitere Informationen finden Sie unter"Amazon EKS Pod Identity Agent einrichten" .

Erstelle trust-relationship.json:

Erstellen Sie eine trust-relationship.json-Datei, um dem EKS-Dienstprinzipal zu ermöglichen, diese Rolle für die Pod-Identität zu übernehmen. Erstellen Sie anschließend eine Rolle mit dieser Vertrauensrichtlinie:

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

trust-relationship.json-Datei:

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

Die Rollenrichtlinie der IAM-Rolle zuordnen:

Weisen Sie der erstellten IAM-Rolle die Rollenrichtlinie aus dem vorherigen Schritt zu:

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

Eine Pod-Identitätszuordnung erstellen:

Erstellen einer Pod-Identitätszuordnung zwischen der IAM-Rolle und dem Trident -Dienstkonto (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
```

IAM-Rolle für die Dienstkontozuordnung (IRSA)

Verwendung der AWS CLI:

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

trust-relationship.json-Datei:

```
{
  "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"
        }
      }
    }
  ]
}
```

Aktualisieren Sie die folgenden Werte in der `trust-relationship.json` Datei:

- **<account_id>** - Ihre AWS-Konto-ID
- **<oidc_provider>** - Der OIDC Ihres EKS-Clusters. Sie können den oidc_provider durch Ausführen folgender Befehl erhalten:

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

Verknüpfen Sie die IAM-Rolle mit der IAM-Richtlinie:

Sobald die Rolle erstellt wurde, ordnen Sie die (im vorherigen Schritt erstellte) Richtlinie der Rolle mit diesem Befehl zu:

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

Überprüfen Sie, ob der OICD-Anbieter zugeordnet ist:

Vergewissern Sie sich, dass Ihr OIDC-Anbieter mit Ihrem Cluster verknüpft ist. Sie können dies mit diesem Befehl überprüfen:

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

Wenn die Ausgabe leer ist, verwenden Sie den folgenden Befehl, um IAM OIDC mit Ihrem Cluster zu verknüpfen:

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

Wenn Sie eksctl verwenden, nutzen Sie das folgende Beispiel, um eine IAM-Rolle für ein Dienstkonto in EKS zu erstellen:

```
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
```

Trident installieren

Trident optimiert die Amazon FSx for NetApp ONTAP in Kubernetes, damit sich Ihre Entwickler und Administratoren auf die Anwendungsbereitstellung konzentrieren können.

Sie können Trident mit einer der folgenden Methoden installieren:

- Helm
- EKS-Add-on

Wenn Sie die Snapshot-Funktionalität nutzen möchten, installieren Sie das CSI Snapshot Controller Add-on. Siehe"Snapshot-Funktionalität für CSI-Volumes aktivieren" für weitere Informationen.

Installieren Sie Trident über Helm

Pod-Identität

1. Fügen Sie das Trident Helm-Repository hinzu:

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

2. Installieren Sie Trident anhand des folgenden Beispiels:

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

Sie können die `helm list` Befehl zum Überprüfen von Installationsdetails wie Name, Namespace, Chart, Status, App-Version und Revisionsnummer.

```
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
```

Servicekonto-Zuordnung (IRSA)

1. Fügen Sie das Trident Helm-Repository hinzu:

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

2. Legen Sie die Werte für **Cloud-Anbieter** und **Cloud-Identität** fest:

```
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
```

Sie können die `helm list` Befehl zum Überprüfen von Installationsdetails wie Name, Namespace, Chart, Status, App-Version und Revisionsnummer.

```
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
```

Wenn Sie iSCSI verwenden möchten, stellen Sie sicher, dass iSCSI auf Ihrem Client-Rechner aktiviert ist. Wenn Sie AL2023 Worker Node OS verwenden, können Sie die Installation des iSCSI-Clients automatisieren, indem Sie den Parameter „node prep“ in die Helm-Installation einfügen:

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

Installieren Sie Trident über das EKS-Add-on

Das Trident EKS-Add-on enthält die neuesten Sicherheitspatches und Fehlerbehebungen und ist von AWS für die Verwendung mit Amazon EKS validiert. Mit dem EKS-Add-on können Sie sicherstellen, dass Ihre Amazon EKS-Cluster stets sicher und stabil sind und den Aufwand für die Installation, Konfiguration und Aktualisierung von Add-ons reduzieren.

Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben, bevor Sie das Trident Add-on für AWS EKS konfigurieren:

- Ein Amazon EKS-Clusterkonto mit Zusatzabonnement
- AWS-Berechtigungen für den AWS Marketplace:
  `"aws-marketplace:ViewSubscriptions",`
  `"aws-marketplace:Subscribe",`
  `"aws-marketplace:Unsubscribe`
- AMI-Typ: Amazon Linux 2 (AL2_x86_64) oder Amazon Linux 2 Arm (AL2_ARM_64)
- Knotentyp: AMD oder ARM
- Ein bestehendes Amazon FSx for NetApp ONTAP Dateisystem

Aktivieren Sie das Trident Add-on für AWS.

Verwaltungskonsole

1. Öffnen Sie die Amazon EKS-Konsole unter https://console.aws.amazon.com/eks/home#/clusters .
2. Im linken Navigationsbereich wählen Sie **Cluster** aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das NetApp Trident CSI-Add-on konfigurieren möchten.
4. Wählen Sie **Add-ons** und anschließend **Weitere Add-ons abrufen**.
5. Gehen Sie wie folgt vor, um das Add-on auszuwählen:
   a. Scrollen Sie nach unten zum Abschnitt **AWS Marketplace Add-ons** und geben Sie **"Trident"** in das Suchfeld ein.
   b. Aktivieren Sie das Kontrollkästchen in der oberen rechten Ecke des Feldes „Trident by NetApp“ .
   c. Wählen Sie **Weiter**.
6. Gehen Sie auf der Einstellungsseite **Ausgewählte Add-ons konfigurieren** wie folgt vor:

   Überspringen Sie diese Schritte, wenn Sie die Pod Identity-Zuordnung verwenden.

   a. Wählen Sie die **Version** aus, die Sie verwenden möchten.
   b. Wenn Sie die IRSA-Authentifizierung verwenden, stellen Sie sicher, dass Sie die in den optionalen Konfigurationseinstellungen verfügbaren Konfigurationswerte festlegen:
      - Wählen Sie die **Version** aus, die Sie verwenden möchten.
      - Folgen Sie dem **Add-on-Konfigurationsschema** und legen Sie den Parameter **configurationValues** im Abschnitt **Konfigurationswerte** auf den Rollen-ARN fest, den Sie im vorherigen Schritt erstellt haben (der Wert sollte folgendes Format haben):

```
{

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

}
```

+
Wenn Sie bei der Konfliktlösungsmethode die Option „Überschreiben“ auswählen, können eine oder mehrere Einstellungen des bestehenden Add-ons mit den Einstellungen des Amazon EKS-Add-ons überschrieben werden. Wenn Sie diese Option nicht aktivieren und es zu einem Konflikt mit Ihren bestehenden Einstellungen kommt, schlägt der Vorgang fehl. Sie können die resultierende Fehlermeldung zur Fehlerbehebung des Konflikts verwenden. Bevor Sie diese Option auswählen, vergewissern Sie sich, dass das Amazon EKS-Add-on keine Einstellungen verwaltet, die Sie selbst verwalten müssen.

7. Wählen Sie **Weiter**.
8. Auf der Seite **Überprüfen und hinzufügen** wählen Sie **Erstellen**.

   Nach Abschluss der Add-on-Installation wird Ihnen das installierte Add-on angezeigt.

AWS CLI

1. Erstellen Sie die `add-on.json` Datei:

Für die Pod-Identität verwenden Sie bitte folgendes Format:

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

Für die IRSA-Authentifizierung verwenden Sie bitte folgendes Format:

```
{
  "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"
  }
}
```

Ersetzen `<role ARN>` mit dem ARN der Rolle, die im vorherigen Schritt erstellt wurde.

2. Installieren Sie das Trident EKS-Add-on.

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

eksctl

Der folgende Beispielbefehl installiert das Trident EKS-Add-on:

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

Aktualisieren Sie das Trident EKS-Add-on

Verwaltungskonsole

1. Öffnen Sie die Amazon EKS-Konsole. https://console.aws.amazon.com/eks/home#/clusters .
2. Im linken Navigationsbereich wählen Sie **Cluster** aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das NetApp Trident CSI-Add-on aktualisieren möchten.
4. Wählen Sie den Reiter **Add-ons**.
5. Wählen Sie * Trident by NetApp* und anschließend **Bearbeiten**.
6. Führen Sie auf der Seite * Trident von NetApp konfigurieren* folgende Schritte aus:
   a. Wählen Sie die **Version** aus, die Sie verwenden möchten.
   b. Erweitern Sie die **Optionalen Konfigurationseinstellungen** und nehmen Sie bei Bedarf Anpassungen vor.
   c. Wählen Sie **Änderungen speichern**.

AWS CLI

Das folgende Beispiel aktualisiert das EKS-Add-on:

```
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

- Überprüfen Sie die aktuelle Version Ihres FSxN Trident CSI-Add-ons. Ersetzen `my-cluster` mit Ihrem Clusternamen.

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

  Beispielausgabe:

```
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'"}
```

- Aktualisieren Sie das Add-on auf die Version, die im Ergebnis des vorherigen Schritts unter UPDATE AVAILABLE angezeigt wurde.

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

Wenn Sie die `--force` Wenn eine der Optionen und eine der Einstellungen des Amazon EKS-Add-ons mit Ihren bestehenden Einstellungen in Konflikt steht und das Aktualisieren des Amazon EKS-Add-ons fehlschlägt, erhalten Sie eine Fehlermeldung, die Ihnen bei der Behebung des Konflikts hilft. Bevor Sie diese Option angeben, vergewissern Sie sich, dass das Amazon EKS-Add-on keine Einstellungen verwaltet, die Sie selbst verwalten müssen, da diese Einstellungen durch diese Option überschrieben werden. Weitere Informationen zu anderen Optionen für diese Einstellung finden Sie unter"Addons" . Weitere Informationen zur Feldverwaltung von Amazon EKS Kubernetes finden Sie unter"Kubernetes-Feldmanagement" .

Deinstallieren/entfernen Sie das Trident EKS-Add-on.

Sie haben zwei Möglichkeiten, ein Amazon EKS-Add-on zu entfernen:

- **Zusatzsoftware auf Ihrem Cluster beibehalten** – Diese Option entfernt die Verwaltung aller Einstellungen durch Amazon EKS. Außerdem entfällt dadurch die Möglichkeit für Amazon EKS, Sie über Aktualisierungen zu benachrichtigen und das Amazon EKS-Add-on automatisch zu aktualisieren, nachdem Sie eine Aktualisierung initiiert haben. Die Zusatzsoftware auf Ihrem Cluster bleibt jedoch erhalten. Diese Option macht das Add-on zu einer selbstverwalteten Installation und nicht zu einem Amazon EKS-Add-on. Bei dieser Option gibt es keine Ausfallzeiten für das Add-on. Behalten Sie die `--preserve` Option im Befehl zum Beibehalten des Add-ons.
- **Entfernen Sie die Add-on-Software vollständig aus Ihrem Cluster** – NetApp empfiehlt, das Amazon EKS-Add-on nur dann aus Ihrem Cluster zu entfernen, wenn keine Ressourcen in Ihrem Cluster davon abhängig sind. Entfernen Sie die `--preserve` Option aus der `delete` Befehl zum Entfernen des Add-ons.

Wenn dem Add-on ein IAM-Konto zugeordnet ist, wird das IAM-Konto nicht entfernt.

Verwaltungskonsole

1. Öffnen Sie die Amazon EKS-Konsole unter https://console.aws.amazon.com/eks/home#/clusters .
2. Im linken Navigationsbereich wählen Sie **Cluster** aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das NetApp Trident CSI-Add-on entfernen möchten.
4. Wählen Sie die Registerkarte **Add-ons** und anschließend * Trident by NetApp*.
5. Wählen Sie **Entfernen**.
6. Führen Sie im Dialogfeld „Bestätigung zum Entfernen des netapp_trident-Operators“ folgende Schritte aus:
   a. Wenn Sie nicht möchten, dass Amazon EKS die Einstellungen für das Add-on verwaltet, wählen Sie **Auf Cluster beibehalten**. Tun Sie dies, wenn Sie die Zusatzsoftware auf Ihrem Cluster behalten möchten, um alle Einstellungen des Zusatzes selbst verwalten zu können.
   b. Geben Sie **netapp_trident-operator** ein.
   c. Wählen Sie **Entfernen**.

AWS CLI

Ersetzen `my-cluster` mit dem Namen Ihres Clusters und führen Sie dann den folgenden Befehl aus.

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

eksctl

Der folgende Befehl deinstalliert das Trident EKS-Add-on:

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

Konfigurieren des Speicher-Backends

ONTAP SAN- und NAS-Treiberintegration

Um ein Speicher-Backend zu erstellen, müssen Sie eine Konfigurationsdatei entweder im JSON- oder im YAML-Format erstellen. Die Datei muss den gewünschten Speichertyp (NAS oder SAN), das Dateisystem und die SVM, von der die Daten bezogen werden sollen, sowie die Art der Authentifizierung angeben. Das folgende Beispiel zeigt, wie Sie NAS-basierten Speicher definieren und ein AWS-Secret verwenden, um die Anmeldeinformationen für die gewünschte SVM zu speichern:

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"
    }
  }
}
```

Führen Sie die folgenden Befehle aus, um die Trident Backend-Konfiguration (TBC) zu erstellen und zu validieren:

- Erstellen Sie eine Trident-Backend-Konfiguration (TBC) aus einer YAML-Datei und führen Sie folgenden Befehl aus:

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

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

- Überprüfen Sie, ob die Trident-Backend-Konfiguration (TBC) erfolgreich erstellt wurde:

```
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
```

FSx für ONTAP Treiberdetails

Sie können Trident mit Amazon FSx for NetApp ONTAP mithilfe der folgenden Treiber integrieren:

- `ontap-san`: Jedes bereitgestellte PV ist eine LUN innerhalb eines eigenen Amazon FSx for NetApp ONTAP Volumes. Empfohlen für Blockspeicherung.
- `ontap-nas`Jedes bereitgestellte PV ist ein vollständiges Amazon FSx for NetApp ONTAP -Volume. Empfohlen für NFS und SMB.
- `ontap-san-economy`Jedes bereitgestellte PV ist eine LUN mit einer konfigurierbaren Anzahl von LUNs pro Amazon FSx for NetApp ONTAP Volume.
- `ontap-nas-economy`Jedes bereitgestellte PV ist ein Qtree, wobei die Anzahl der Qtrees pro Amazon FSx for NetApp ONTAP Volume konfigurierbar ist.
- `ontap-nas-flexgroup`Jedes bereitgestellte PV ist ein vollständiges Amazon FSx for NetApp ONTAP FlexGroup Volume.

Weitere Fahrerdetails finden Sie unter"NAS-Treiber" Und"SAN-Treiber" .

Sobald die Konfigurationsdatei erstellt wurde, führen Sie diesen Befehl aus, um sie in Ihrem EKS zu erstellen:

```
kubectl create -f configuration_file
```

Um den Status zu überprüfen, führen Sie folgenden Befehl aus:

```
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
```

Erweiterte Backend-Konfiguration und Beispiele

Die folgenden Tabellen enthalten die Backend-Konfigurationsoptionen:

Parameter	Beschreibung	Beispiel
`version`		Immer 1
`storageDriverName`	Name des Speichertreibers	`ontap-nas`, `ontap-nas-economy` , `ontap-nas-flexgroup` , `ontap-san` , `ontap-san-economy`
`backendName`	Benutzerdefinierter Name oder das Speicher-Backend	Fahrername + "_" + dataLIF
`managementLIF`	IP-Adresse eines Clusters oder SVM-Management-LIF. Es kann ein vollqualifizierter Domänenname (FQDN) angegeben werden. Kann so eingestellt werden, dass IPv6-Adressen verwendet werden, wenn Trident mit dem IPv6-Flag installiert wurde. IPv6-Adressen müssen in eckigen Klammern angegeben werden, z. B. [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Wenn Sie die `fsxFilesystemID` unter dem `aws` Das Feld müssen Sie nicht angeben. `managementLIF` weil Trident die SVM abruft `managementLIF` Informationen von AWS. Sie müssen also Anmeldeinformationen für einen Benutzer unter der SVM angeben (z. B. vsadmin), und dieser Benutzer muss über die folgenden Berechtigungen verfügen: `vsadmin` Rolle.	„10.0.0.1“, „[2001:1234:abcd::fefe]“

Parameter	Beschreibung	Beispiel
`dataLIF`	IP-Adresse des Protokolls LIF. * ONTAP NAS-Treiber*: NetApp empfiehlt die Angabe von dataLIF. Falls keine Daten angegeben werden, ruft Trident die dataLIFs vom SVM ab. Sie können einen vollqualifizierten Domänennamen (FQDN) angeben, der für die NFS-Mount-Operationen verwendet werden soll. Dadurch können Sie ein Round-Robin-DNS erstellen, um die Last auf mehrere DataLIFs zu verteilen. Kann nach der Ersteinrichtung geändert werden. Siehe . * ONTAP SAN-Treiber*: Nicht für iSCSI angeben. Trident verwendet ONTAP Selective LUN Map, um die iSCI LIFs zu ermitteln, die zum Aufbau einer Multipath-Sitzung benötigt werden. Es wird eine Warnung generiert, wenn dataLIF explizit definiert ist. Kann so eingestellt werden, dass IPv6-Adressen verwendet werden, wenn Trident mit dem IPv6-Flag installiert wurde. IPv6-Adressen müssen in eckigen Klammern angegeben werden, z. B. [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	
`autoExportPolicy`	Automatische Erstellung und Aktualisierung von Exportrichtlinien aktivieren [Boolesch]. Verwenden des `autoExportPolicy` Und `autoExportCIDRs` Optionen: Trident kann Exportrichtlinien automatisch verwalten.	`false`
`autoExportCIDRs`	Liste der CIDRs, anhand derer die Kubernetes-Knoten-IPs gefiltert werden sollen, wenn `autoExportPolicy` ist aktiviert. Verwenden des `autoExportPolicy` Und `autoExportCIDRs` Optionen: Trident kann Exportrichtlinien automatisch verwalten.	"["0.0.0.0/0", "::/0"]"
`labels`	Satz beliebiger JSON-formatierter Bezeichnungen, die auf Datenträger angewendet werden sollen	""

Parameter	Beschreibung	Beispiel
`clientCertificate`	Base64-kodierter Wert des Clientzertifikats. Wird für zertifikatsbasierte Authentifizierung verwendet	""
`clientPrivateKey`	Base64-kodierter Wert des privaten Client-Schlüssels. Wird für zertifikatsbasierte Authentifizierung verwendet	""
`trustedCACertificate`	Base64-kodierter Wert des vertrauenswürdigen CA-Zertifikats. Optional. Wird für die zertifikatsbasierte Authentifizierung verwendet.	""
`username`	Benutzername für die Verbindung zum Cluster oder zur SVM. Wird für die auf Anmeldeinformationen basierende Authentifizierung verwendet. Zum Beispiel vsadmin.	
`password`	Passwort zum Verbinden mit dem Cluster oder der SVM. Wird für die auf Anmeldeinformationen basierende Authentifizierung verwendet.	
`svm`	Zu verwendende virtuelle Speichermaschine	Wird abgeleitet, wenn ein SVM managementLIF angegeben ist.
`storagePrefix`	Präfix, das beim Bereitstellen neuer Volumes in der SVM verwendet wird. Kann nach der Erstellung nicht mehr geändert werden. Um diesen Parameter zu aktualisieren, müssen Sie ein neues Backend erstellen.	`trident`
`limitAggregateUsage`	**Nicht für Amazon FSx for NetApp ONTAP angeben.** Die bereitgestellten `fsxadmin` Und `vsadmin` enthalten nicht die erforderlichen Berechtigungen, um die aggregierte Nutzung abzurufen und sie mit Trident einzuschränken.	Nicht verwenden.

Parameter	Beschreibung	Beispiel
`limitVolumeSize`	Die Bereitstellung schlägt fehl, wenn die angeforderte Volume-Größe diesen Wert überschreitet. Beschränkt außerdem die maximale Größe der von ihm verwalteten Volumes für Qtrees und LUNs, und die `qtreesPerFlexvol` Diese Option ermöglicht die Anpassung der maximalen Anzahl von Qtrees pro FlexVol volume.	"" (wird nicht standardmäßig erzwungen)
`lunsPerFlexvol`	Die maximale Anzahl an LUNs pro Flexvol-Volume muss im Bereich [50, 200] liegen. Nur SAN.	“100”
`debugTraceFlags`	Debug-Flags zur Verwendung bei der Fehlersuche. Beispiel: {"api":false, "method":true} Nicht verwenden `debugTraceFlags` Es sei denn, Sie befinden sich in der Fehlersuche und benötigen einen detaillierten Protokollauszug.	null
`nfsMountOptions`	Durch Kommas getrennte Liste der NFS-Mount-Optionen. Die Mount-Optionen für Kubernetes-persistente Volumes werden normalerweise in Speicherklassen angegeben. Wenn jedoch in einer Speicherklasse keine Mount-Optionen angegeben sind, greift Trident auf die in der Konfigurationsdatei des Speicher-Backends angegebenen Mount-Optionen zurück. Wenn in der Speicherklasse oder der Konfigurationsdatei keine Mount-Optionen angegeben sind, setzt Trident keine Mount-Optionen auf einem zugehörigen persistenten Volume.	""
`nasType`	Konfiguration der Erstellung von NFS- oder SMB-Volumes. Optionen sind `nfs` , `smb` oder null. **Muss eingestellt werden auf `smb` für SMB-Volumes.** Bei der Einstellung „null“ werden standardmäßig NFS-Volumes verwendet.	`nfs`
`qtreesPerFlexvol`	Die maximale Anzahl an Qtrees pro FlexVol volume muss im Bereich [50, 300] liegen.	`"200"`

Parameter	Beschreibung	Beispiel
`smbShare`	Sie können entweder den Namen einer SMB-Freigabe angeben, die mit der Microsoft Management Console oder der ONTAP CLI erstellt wurde, oder einen Namen, unter dem Trident die SMB-Freigabe erstellen kann. Dieser Parameter ist für Amazon FSx for ONTAP -Backends erforderlich.	`smb-share`
`useREST`	Boolescher Parameter zur Verwendung von ONTAP REST-APIs. Wenn eingestellt auf `true` Trident wird ONTAP REST APIs zur Kommunikation mit dem Backend verwenden. Diese Funktion erfordert ONTAP 9.11.1 und höher. Darüber hinaus muss die verwendete ONTAP Anmelderolle Zugriff auf die `ontap` Anwendung. Dies wird durch die vordefinierte Bedingung erfüllt. `vsadmin` Und `cluster-admin` Rollen.	`false`
`aws`	In der Konfigurationsdatei für AWS FSx für ONTAP können Sie Folgendes angeben: - `fsxFilesystemID` : Geben Sie die ID des AWS FSx-Dateisystems an. - `apiRegion` : Name der AWS-API-Region. - `apikey` : AWS-API-Schlüssel. - `secretKey` : AWS-Geheimschlüssel.	`""` `""` `""`
`credentials`	Geben Sie die FSx SVM-Anmeldeinformationen an, die im AWS Secrets Manager gespeichert werden sollen. - `name` : Amazon Resource Name (ARN) des Geheimnisses, das die Anmeldeinformationen von SVM enthält. - `type` : Aufstellen `awsarn` . Siehe"Erstellen Sie ein AWS Secrets Manager-Geheimnis" für weitere Informationen.	

Backend-Konfigurationsoptionen für die Bereitstellung von Volumes

Sie können die Standardbereitstellung mithilfe dieser Optionen steuern. `defaults` Abschnitt der Konfiguration. Ein Beispiel finden Sie in den folgenden Konfigurationsbeispielen.

Parameter	Beschreibung	Standard
`spaceAllocation`	Speicherplatzzuweisung für LUNs	`true`
`spaceReserve`	Platzreservierungsmodus; "keine" (dünn) oder "Volumen" (dick)	`none`
`snapshotPolicy`	Zu verwendende Snapshot-Richtlinie	`none`
`qosPolicy`	Die QoS-Richtliniengruppe soll den erstellten Volumes zugewiesen werden. Wählen Sie pro Speicherpool oder Backend entweder qosPolicy oder adaptiveQosPolicy aus. Die Verwendung von QoS-Richtliniengruppen mit Trident erfordert ONTAP 9.8 oder höher. Sie sollten eine nicht gemeinsam genutzte QoS-Richtliniengruppe verwenden und sicherstellen, dass die Richtliniengruppe auf jeden einzelnen Bestandteil angewendet wird. Eine gemeinsam genutzte QoS-Richtliniengruppe setzt die Obergrenze für den Gesamtdurchsatz aller Workloads durch.	""
`adaptiveQosPolicy`	Adaptive QoS-Richtliniengruppe, die den erstellten Volumes zugewiesen werden soll. Wählen Sie pro Speicherpool oder Backend entweder qosPolicy oder adaptiveQosPolicy aus. Wird von ontap-nas-economy nicht unterstützt.	""
`snapshotReserve`	Prozentsatz des für Snapshots reservierten Speichervolumens „0“	Wenn `snapshotPolicy` Ist `none` , `else` ""
`splitOnClone`	Beim Erstellen eines Klons diesen von seinem Elternklon trennen	`false`
`encryption`	Aktivieren Sie die NetApp Volumeverschlüsselung (NVE) auf dem neuen Volume; Standardwert ist `false` . Um diese Option nutzen zu können, muss NVE auf dem Cluster lizenziert und aktiviert sein. Wenn NAE im Backend aktiviert ist, wird jedes in Trident bereitgestellte Volume NAE-fähig sein. Weitere Informationen finden Sie unter:"Wie Trident mit NVE und NAE zusammenarbeitet" .	`false`

Parameter	Beschreibung	Standard
`luksEncryption`	LUKS-Verschlüsselung aktivieren. Siehe"Verwenden Sie Linux Unified Key Setup (LUKS)." . Nur SAN.	""
`tieringPolicy`	zu verwendende Stufenrichtlinie `none`	
`unixPermissions`	Modus für neue Volumes. **Für SMB-Volumes leer lassen.**	""
`securityStyle`	Sicherheitsstil für neue Bände. NFS unterstützt `mixed` Und `unix` Sicherheitsstile. SMB-Unterstützung `mixed` Und `ntfs` Sicherheitsstile.	NFS-Standard ist `unix` . SMB-Standard ist `ntfs` .

Bereiten Sie die Bereitstellung von SMB-Volumes vor

Sie können SMB-Volumes mithilfe von … bereitstellen. `ontap-nas` Treiber. Bevor Sie fertigstellenONTAP SAN- und NAS-Treiberintegration Führen Sie die folgenden Schritte aus.

Bevor Sie beginnen

Bevor Sie SMB-Volumes mithilfe von `ontap-nas` Als Fahrer benötigen Sie Folgendes:

- Ein Kubernetes-Cluster mit einem Linux-Controller-Knoten und mindestens einem Windows-Worker-Knoten, auf dem Windows Server 2019 ausgeführt wird. Trident unterstützt SMB-Volumes nur, wenn sie in Pods eingebunden sind, die auf Windows-Knoten laufen.
- Mindestens ein Trident Geheimnis, das Ihre Active Directory-Anmeldeinformationen enthält. Um Geheimnisse zu generieren `smbcreds` :

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

- Ein als Windows-Dienst konfigurierter CSI-Proxy. Um einen zu konfigurieren `csi-proxy` , siehe"GitHub: CSI-Proxy" oder"GitHub: CSI-Proxy für Windows" für Kubernetes-Knoten, die unter Windows laufen.

Schritte

1. SMB-Freigaben erstellen. Sie können die SMB-Administratorfreigaben auf zwei Arten erstellen, entweder mithilfe von"Microsoft Management Console" Über das Snap-In „Freigegebene Ordner“ oder über die ONTAP -Befehlszeilenschnittstelle. So erstellen Sie die SMB-Freigaben mithilfe der ONTAP -Befehlszeilenschnittstelle:
   a. Erstellen Sie gegebenenfalls die Verzeichnispfadstruktur für die Freigabe.

      Der `vserver cifs share create` Der Befehl überprüft den Pfad, der bei der Erstellung der Freigabe in der Option -path angegeben wurde. Wenn der angegebene Pfad nicht existiert, schlägt der Befehl fehl.

   b. Erstellen Sie eine SMB-Freigabe, die dem angegebenen SVM zugeordnet ist:

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

c. Überprüfen Sie, ob die Freigabe erstellt wurde:

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

Siehe"Erstellen einer SMB-Freigabe" Für alle Details.

2. Bei der Erstellung des Backends müssen Sie Folgendes konfigurieren, um SMB-Volumes anzugeben. Alle Konfigurationsoptionen für das FSx for ONTAP Backend finden Sie unter"FSx für ONTAP: Konfigurationsoptionen und Beispiele" .

Parameter	Beschreibung	Beispiel
`smbShare`	Sie können entweder den Namen einer SMB-Freigabe angeben, die mit der Microsoft Management Console oder der ONTAP CLI erstellt wurde, oder einen Namen, unter dem Trident die SMB-Freigabe erstellen kann. Dieser Parameter ist für Amazon FSx for ONTAP -Backends erforderlich.	`smb-share`
`nasType`	**Muss eingestellt werden auf `smb` .** Wenn null, wird standardmäßig der Wert verwendet. `nfs` .	`smb`
`securityStyle`	Sicherheitsstil für neue Bände. **Muss eingestellt sein auf `ntfs` oder `mixed` für SMB-Volumes.**	`ntfs`oder `mixed` für SMB-Volumes
`unixPermissions`	Modus für neue Volumes. **Muss bei SMB-Volumes leer bleiben.**	""

Konfigurieren Sie eine Speicherklasse und einen PVC.

Konfigurieren Sie ein Kubernetes StorageClass-Objekt und erstellen Sie die Storage-Klasse, um Trident anzuweisen, wie Volumes bereitgestellt werden sollen. Erstellen Sie einen PersistentVolumeClaim (PVC), der die konfigurierte Kubernetes StorageClass verwendet, um Zugriff auf das PV anzufordern. Anschließend können Sie die PV-Anlage an einem Pod montieren.

Erstellen einer Speicherklasse

Konfigurieren eines Kubernetes StorageClass-Objekts

Der "Kubernetes StorageClass-Objekt" Das Objekt identifiziert Trident als den für diese Klasse verwendeten Provisionierer und weist Trident an, wie ein Volume zu provisionieren ist. Verwenden Sie dieses Beispiel, um die Speicherklasse für Volumes mit NFS einzurichten (die vollständige Liste der Attribute finden Sie im Abschnitt „Trident -Attribute“ weiter unten):

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

Verwenden Sie dieses Beispiel, um die Speicherklasse für Volumes mit iSCSI einzurichten:

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

Um NFSv3-Volumes auf AWS Bottlerocket bereitzustellen, fügen Sie die erforderlichen Komponenten hinzu. `mountOptions` zur Speicherklasse:

```
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
```

Siehe"Kubernetes- und Trident Objekte" Einzelheiten darüber, wie Speicherklassen mit dem interagieren, finden Sie hier. `PersistentVolumeClaim` und Parameter zur Steuerung der Volumenbereitstellung Trident .

Erstellen einer Speicherklasse

Schritte

1. Dies ist ein Kubernetes-Objekt, also verwenden Sie `kubectl` um es in Kubernetes zu erstellen.

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

2. Sie sollten nun sowohl in Kubernetes als auch in Trident eine **basic-csi**-Speicherklasse sehen, und Trident sollte die Pools im Backend erkannt haben.

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

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

PVC erstellen

A "*PersistentVolumeClaim*" (PVC) ist eine Anfrage für den Zugriff auf das PersistentVolume im Cluster.

Das PVC kann so konfiguriert werden, dass es Speicherplatz einer bestimmten Größe oder einen bestimmten Zugriffsmodus anfordert. Mithilfe der zugehörigen StorageClass kann der Clusteradministrator mehr als nur die Größe und den Zugriffsmodus des PersistentVolumes steuern – beispielsweise die Leistung oder das Servicelevel.

Nachdem Sie das PVC erstellt haben, können Sie das Volumen in einem Gehäuse montieren.

Beispielmanifeste

Beispielmanifeste für PersistentVolumeClaim

Diese Beispiele zeigen grundlegende PVC-Konfigurationsoptionen.

PVC mit RWX-Zugang

Dieses Beispiel zeigt eine einfache PVC mit RWX-Zugriff, die einer StorageClass namens zugeordnet ist. `basic-csi` .

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

PVC mit iSCSI-Beispiel

Dieses Beispiel zeigt eine einfache PVC für iSCSI mit RWO-Zugriff, die einer StorageClass namens zugeordnet ist. `protection-gold` .

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

PVC erstellen

Schritte

1. Erstellen Sie die PVC.

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

2. Überprüfen Sie den PVC-Status.

```
kubectl get pvc
```

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

Siehe"Kubernetes- und Trident Objekte" Einzelheiten darüber, wie Speicherklassen mit dem interagieren, finden Sie hier. `PersistentVolumeClaim` und Parameter zur Steuerung der Volumenbereitstellung Trident .

Trident Eigenschaften

Diese Parameter legen fest, welche von Trident verwalteten Speicherpools zur Bereitstellung von Volumes eines bestimmten Typs verwendet werden sollen.

Attribut	Typ	Werte	Angebot	Anfrage	Unterstützt von
media[1]	Schnur	HDD, Hybrid, SSD	Der Pool enthält Medien dieses Typs; hybrid bedeutet beides	Medientyp angegeben	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
Bereitstellungstyp	Schnur	dünn, dick	Pool unterstützt diese Bereitstellungsmethode	Bereitstellungsmethode angegeben	dick: alles vom Fass; dünn: alles vom Fass & Solidfire-San
Backend-Typ	Schnur	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Pool gehört zu dieser Art von Backend.	Backend spezifiziert	Alle Fahrer
Momentaufnahmen	bool	wahr, falsch	Pool unterstützt Volumes mit Snapshots	Volume mit aktivierten Snapshots	ontap-nas, ontap-san, solidfire-san, gcp-cvs
Klone	bool	wahr, falsch	Pool unterstützt das Klonen von Volumes	Volume mit aktivierten Klonen	ontap-nas, ontap-san, solidfire-san, gcp-cvs

Attribut	Typ	Werte	Angebot	Anfrage	Unterstützt von
Verschlüsselung	bool	wahr, falsch	Pool unterstützt verschlüsselte Volumes	Volume mit aktivierter Verschlüsselung	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	int	positive ganze Zahl	Pool ist in der Lage, IOPS in diesem Bereich zu garantieren.	Volumen garantiert diese IOPS	solidfire-san

[1]: Wird von ONTAP Select -Systemen nicht unterstützt.

Beispielanwendung bereitstellen

Sobald die Speicherklasse und das PVC erstellt sind, können Sie das PV an einem Pod montieren. Dieser Abschnitt listet den Beispielbefehl und die Konfiguration zum Anhängen des PV an einen Pod auf.

Schritte

1. Montieren Sie das Volume in einem Gehäuse.

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

Diese Beispiele zeigen grundlegende Konfigurationen zum Anbringen des PVC an eine Kapsel:
Grundkonfiguration:

```
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
```

Sie können den Fortschritt überwachen mit `kubectl get pod --watch` .

2. Überprüfen Sie, ob das Volume eingebunden ist. `/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
```

Sie können den Pod jetzt löschen. Die Pod-Anwendung wird nicht mehr existieren, das Volume bleibt jedoch erhalten.

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

Konfigurieren Sie das Trident EKS-Add-on auf einem EKS-Cluster

NetApp Trident optimiert die Amazon FSx for NetApp ONTAP in Kubernetes, damit sich Ihre Entwickler und Administratoren auf die Anwendungsbereitstellung konzentrieren

können. Das NetApp Trident EKS-Add-on enthält die neuesten Sicherheitspatches und Fehlerbehebungen und ist von AWS für die Verwendung mit Amazon EKS validiert. Mit dem EKS-Add-on können Sie sicherstellen, dass Ihre Amazon EKS-Cluster stets sicher und stabil sind und den Aufwand für die Installation, Konfiguration und Aktualisierung von Add-ons reduzieren.

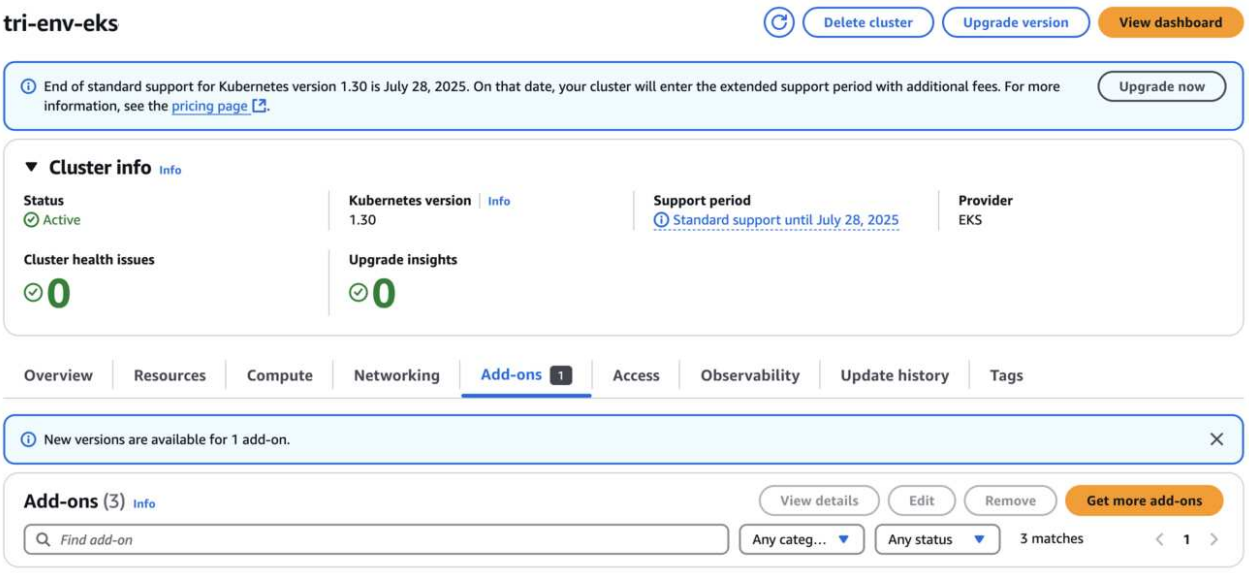
Voraussetzungen

Stellen Sie sicher, dass Sie Folgendes haben, bevor Sie das Trident Add-on für AWS EKS konfigurieren:

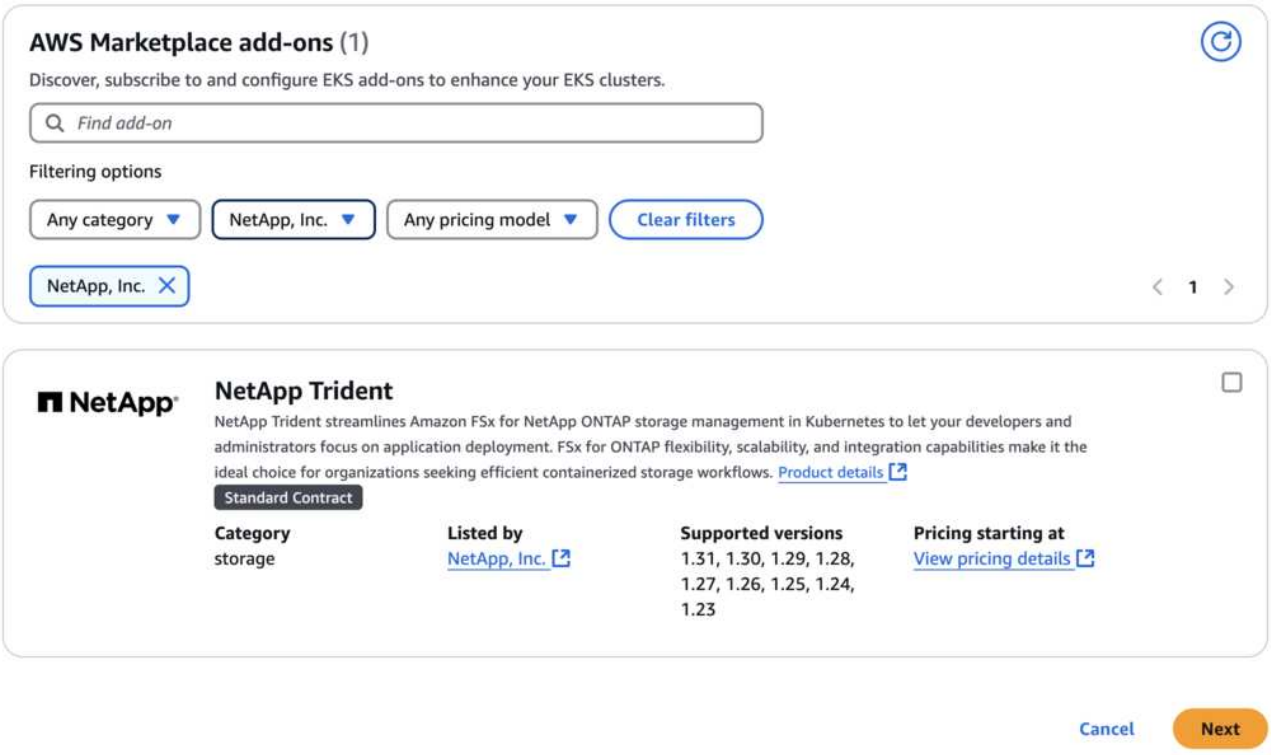
- Ein Amazon EKS-Cluster-Konto mit Berechtigungen zur Arbeit mit Add-ons. Siehe"Amazon EKS-Add-ons" .
- AWS-Berechtigungen für den AWS Marketplace:
  `"aws-marketplace:ViewSubscriptions",`
  `"aws-marketplace:Subscribe",`
  `"aws-marketplace:Unsubscribe`
- AMI-Typ: Amazon Linux 2 (AL2_x86_64) oder Amazon Linux 2 Arm (AL2_ARM_64)
- Knotentyp: AMD oder ARM
- Ein bestehendes Amazon FSx for NetApp ONTAP Dateisystem

Schritte

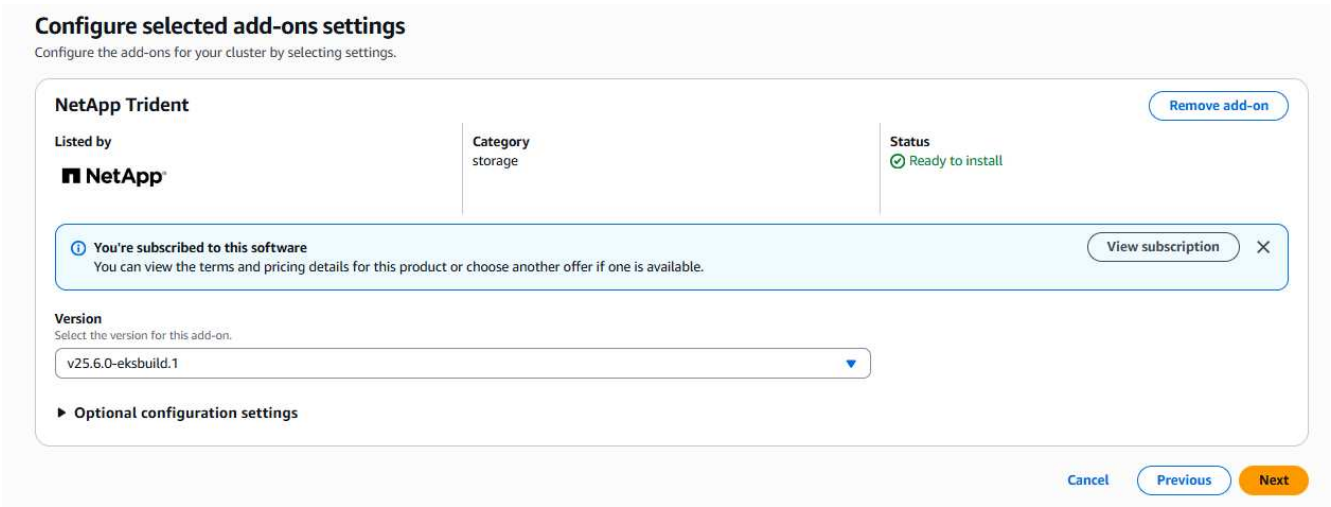
1. Stellen Sie sicher, dass Sie eine IAM-Rolle und ein AWS-Secret erstellen, damit EKS-Pods auf AWS-Ressourcen zugreifen können. Anweisungen finden Sie unter"Erstellen Sie eine IAM-Rolle und ein AWS-Geheimnis." .
2. Navigieren Sie in Ihrem EKS Kubernetes-Cluster zum Tab **Add-ons**.



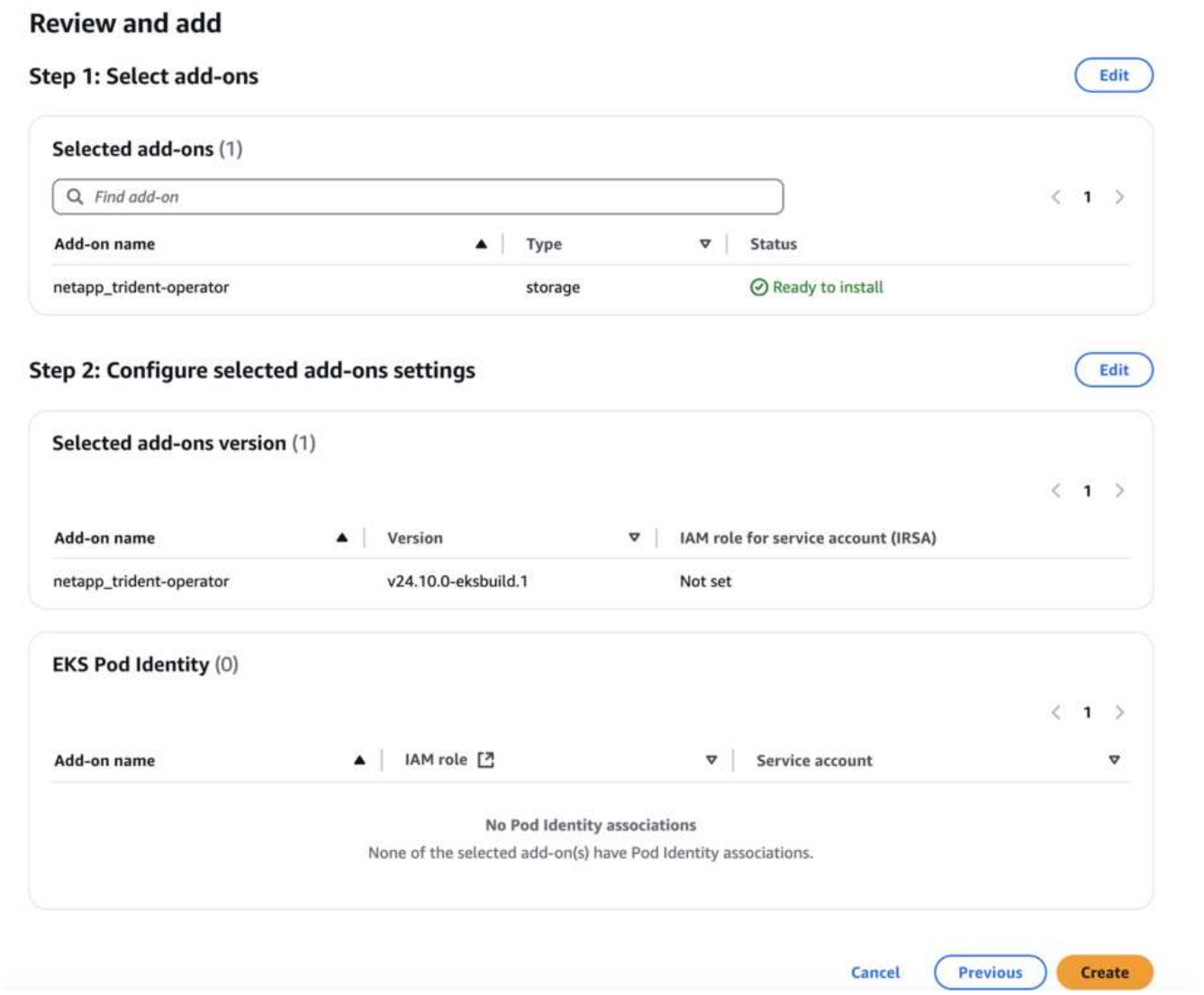
3. Gehen Sie zu **AWS Marketplace Add-ons** und wählen Sie die Kategorie *Speicher* aus.



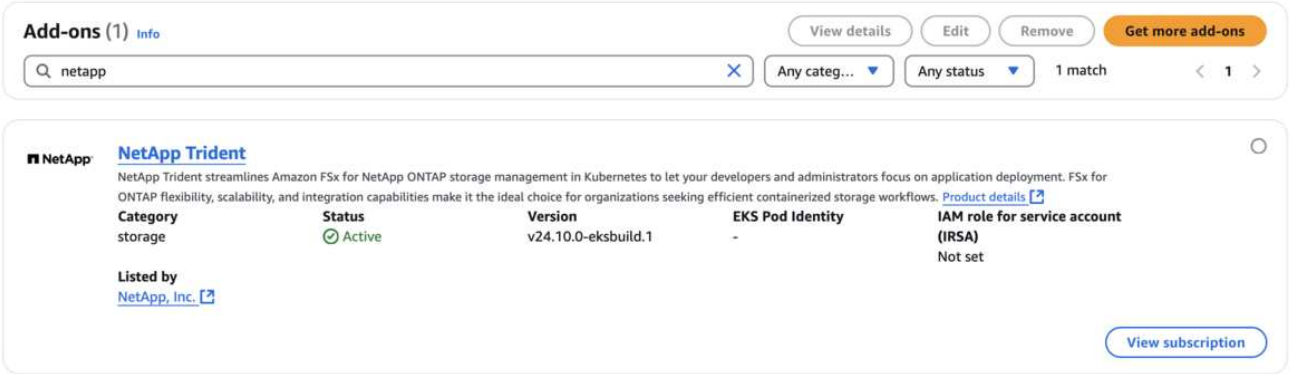
4. Suchen Sie * NetApp Trident* und aktivieren Sie das Kontrollkästchen für das Trident Add-on. Klicken Sie anschließend auf **Weiter**.
5. Wählen Sie die gewünschte Version des Add-ons.



6. Konfigurieren Sie die erforderlichen Add-On-Einstellungen.



7. Wenn Sie IRSA (IAM-Rollen für Dienstkonten) verwenden, beachten Sie die zusätzlichen Konfigurationsschritte."hier," .
8. Wählen Sie **Erstellen**.
9. Überprüfen Sie, ob der Status des Add-ons *Aktiv* lautet.



10. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Trident ordnungsgemäß auf dem Cluster installiert ist:

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

11. Setzen Sie die Einrichtung fort und konfigurieren Sie das Speicher-Backend. Weitere Informationen finden Sie unter"Konfigurieren des Speicher-Backends" .

Installation/Deinstallation des Trident EKS-Add-ons über die Befehlszeile

Installieren Sie das NetApp Trident EKS-Add-on über die Befehlszeile:

Der folgende Beispielbefehl installiert das Trident EKS-Add-on:
`eksctl create addon --cluster clusterName --name netapp_trident-operator --version v25.6.0-eksbuild.1` (mit einer speziellen Version)

Deinstallieren Sie das NetApp Trident EKS-Add-on über die Befehlszeile:

Der folgende Befehl deinstalliert das Trident EKS-Add-on:

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