



Amazon FSx for NetApp ONTAP

Trident

NetApp
October 29, 2026

Inhalt

Amazon FSx for NetApp ONTAP	1
Verwenden Sie Trident mit Amazon FSx for NetApp ONTAP	1
Anforderungen	1
Überlegungen	1
Authentifizierung	2
Getestete Amazon Machine Images (AMIs)	2
Weitere Informationen	3
Erstellen Sie eine IAM-Rolle und ein AWS-Geheimnis	3
AWS Secrets Manager-Geheimnis erstellen	3
IAM-Richtlinie erstellen	4
Trident installieren	8
Trident über helm installieren	8
Installieren Sie Trident über das EKS-Add-on	10
Konfigurieren einer Speicherklasse	14
Erstellen Sie ein StorageClass-Objekt	15
SMB-Volumen bereitstellen	22
Erweiterte Backend-Konfiguration und Beispiele	22
Backend-Konfigurationsoptionen für die Bereitstellung von Volumes	27
PVC konfigurieren	29
PVC erstellen	29
Eine Anwendung bereitstellen	30
Eine Beispielanwendung bereitstellen	31
Konfigurieren Sie das Trident EKS add-on auf einem EKS Cluster	32
Voraussetzungen	32
Schritte	32
Installieren/Deinstallieren des Trident EKS Add-ons über die CLI	35

Amazon FSx for NetApp ONTAP

Verwenden Sie Trident mit Amazon FSx for NetApp ONTAP

"Amazon FSx for NetApp ONTAP" ist ein vollständig verwalteter AWS-Service, der Dateisysteme betreibt, die vom NetApp ONTAP-Speicherbetriebssystem unterstützt werden. Er bietet ONTAP-Funktionen, Leistung und Administration mit der Skalierbarkeit und dem einfachen Betrieb von AWS. Ein Dateisystem ist die primäre Ressource in Amazon FSx und entspricht einem lokalen ONTAP-Cluster. Jedes Dateisystem enthält eine oder mehrere Storage Virtual Machines (SVMs), und jede SVM enthält ein oder mehrere Volumes, die Dateien und Verzeichnisse speichern. Diese Integration ermöglicht es Kubernetes-Clustern, die in Amazon Elastic Kubernetes Service (EKS) ausgeführt werden, ONTAP-gestützte persistente Volumes für Block- und Dateiworkloads bereitzustellen.

Anforderungen

Zusätzlich zu ["Trident-Anforderungen"](#) benötigen Sie zur Integration von FSx for ONTAP mit Trident Folgendes:

- 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 für ["NFS oder iSCSI"](#) vorbereitet sind.



Stellen Sie sicher, dass Sie die für Amazon Linux und Ubuntu ["Amazon Machine Images"](#) (AMIs) erforderlichen Node-Vorbereitungsschritte je nach Ihrem EKS-AMI-Typ befolgen.

Überlegungen

- SMB-Volumes:
 - SMB-Volumes werden nur mit dem `ontap-nas` Treiber unterstützt.
 - SMB-Volumes werden mit dem Trident EKS-Add-on nicht unterstützt.
 - Trident unterstützt SMB-Volumes nur, wenn sie in Pods eingebunden sind, die auf Windows-Knoten ausgeführt werden. Details sind in ["Bereiten Sie die Bereitstellung von SMB-Volumes vor"](#) zu finden.
- Vor Trident 24.02 konnten Volumes, die auf Amazon FSx-Dateisystemen mit aktivierten automatischen Backups erstellt wurden, nicht von Trident gelöscht werden. Um dieses Problem in Trident 24.02 oder höher zu verhindern, geben Sie die `fsxFilesystemID`, `AWS apiRegion`, `AWS apikey` und `AWS secretKey` in der Backend-Konfigurationsdatei für AWS FSx for ONTAP an.



Wenn Sie eine IAM-Rolle für Trident angeben, können Sie das explizite Angeben der Felder `apiRegion`, `apiKey` und `secretKey` für Trident weglassen. Weitere Informationen finden Sie unter ["FSx for ONTAP Konfigurationsoptionen und Beispiele"](#).

Gleichzeitige Verwendung 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 die erforderliche Multipath-Konfiguration auf den Knoten mit dem Amazon Elastic Block Store (EBS) CSI-Treiber in Konflikt geraten. Um sicherzustellen, dass Multipathing ohne Beeinträchtigung der EBS-Festplatten auf demselben Knoten funktioniert, müssen Sie EBS in Ihrer Multipathing-Konfiguration ausschließen. Dieses Beispiel zeigt eine `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 Modi der Authentifizierung.

- Anmeldeinformationsbasiert (Empfohlen): Speichert Anmeldeinformationen sicher im AWS Secrets Manager. Sie können den `fsxadmin` Benutzer für Ihr Dateisystem oder den `vsadmin` Benutzer, der für Ihre SVM konfiguriert ist, verwenden.



Trident erwartet, als `vsadmin` SVM-Benutzer oder als Benutzer mit einem anderen Namen, aber derselben Rolle ausgeführt zu werden. Amazon FSx for NetApp ONTAP hat einen `fsxadmin` Benutzer, der ein eingeschränkter Ersatz für den ONTAP `admin` Cluster-Benutzer ist. Wir empfehlen dringend, `vsadmin` mit Trident zu verwenden.

- Zertifikatsbasiert: Trident wird mit der SVM auf Ihrem FSx-Dateisystem unter Verwendung eines auf Ihrer SVM installierten Zertifikats kommunizieren.

Einzelheiten zur Aktivierung der Authentifizierung finden Sie in der 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-economy	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 PV kann nicht ohne Neustart des Knotens gelöscht werden
- ** 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 wurde lediglich noch nicht getestet. Diese Liste dient als Orientierungshilfe 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, pod
- Löschen: pod, pvc (regulär, qtree/lun – economy, NAS mit AWS backup)

Weitere Informationen

- ["Amazon FSx for NetApp ONTAP Dokumentation"](#)
- ["Blogpost zu 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 müssen Sie einen Kubernetes-Cluster haben, der mit EKS bereitgestellt wurde.

AWS Secrets Manager-Geheimnis erstellen

Da Trident APIs gegen einen FSx vserver ausführt, um den Speicher für Sie zu verwalten, benötigt es hierfür Anmeldeinformationen. Der sichere Weg, diese Anmeldeinformationen zu übermitteln, ist über ein AWS

Secrets Manager secret. Wenn Sie also noch keines haben, müssen Sie ein AWS Secrets Manager secret erstellen, das die Anmeldeinformationen für das vsadmin account enthält.

Dieses Beispiel erstellt ein AWS Secrets Manager secret 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 zu funktionieren. Daher müssen Sie eine Richtlinie erstellen, die Trident die erforderlichen 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"
```

Policy JSON-Beispiel:

```
{
  "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 Service account association (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 alle AWS-Services zugreifen, auf die die Rolle Berechtigungen hat.

Pod-Identität

Amazon EKS Pod Identity associations bieten die Möglichkeit, Anmeldeinformationen für Ihre Anwendungen zu verwalten, ähnlich wie Amazon EC2 instance profiles Anmeldeinformationen für Amazon EC2 instances bereitstellen.

Installieren Sie Pod Identity auf Ihrem EKS-Cluster:

Sie können eine Pod-Identität über die AWS-Konsole oder mit dem folgenden AWS CLI-Befehl erstellen:

```

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

```

Weitere Informationen finden Sie unter ["Richten Sie den Amazon EKS Pod Identity Agent ein"](#).

Erstellen Sie trust-relationship.json:

Erstellen Sie trust-relationship.json, um dem EKS Service Principal zu ermöglichen, diese Rolle für Pod Identity zu übernehmen. Erstellen Sie dann 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 an die IAM-Rolle anhängen:

Hängen Sie die Rollenrichtlinie aus dem vorherigen Schritt an die erstellte IAM-Rolle an:

```

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 Sie eine 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 role für Service account association (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>** - Die OIDC Ihres EKS-Clusters. Sie können den `oidc_provider` durch Ausführen des folgenden Befehls abrufen:

```

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, hängen Sie die Richtlinie (die im vorherigen Schritt erstellt wurde) mit diesem Befehl an die Rolle an:

```

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

```

Überprüfen Sie, ob der OICD provider zugeordnet ist:

Überprüfen Sie, ob 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, verwenden Sie das folgende Beispiel, um eine IAM-Rolle für das 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 Amazon FSx for NetApp ONTAP Speicherverwaltung 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. Weitere Informationen finden Sie unter ["Snapshot-Funktionalität für CSI-Volumes aktivieren"](#).

Trident über helm installieren

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 den `helm list` Befehl verwenden, um Installationsdetails wie Name, Namespace, Chart, Status, App-Version und Revisionsnummer zu überprüfen.

```
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		

Service-Account-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 provider** und **cloud identity** 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 den `helm list` Befehl verwenden, um Installationsdetails wie Name, Namespace, Chart, Status, App-Version und Revisionsnummer zu überprüfen.

```
helm list -n trident
```

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



Wenn Sie iSCSI verwenden möchten, stellen Sie sicher, dass iSCSI auf Ihrem Client-Rechner aktiviert ist. Wenn Sie das AL2023 Worker node OS verwenden, können Sie die Installation des iSCSI-Clients automatisieren, indem Sie den `node prep` Parameter in der helm Installation hinzufügen:

```
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, Fehlerbehebungen und ist von AWS für die Verwendung mit Amazon EKS validiert. Das EKS-Add-on ermöglicht es Ihnen, konsequent sicherzustellen, dass Ihre Amazon EKS-Cluster sicher und stabil sind, und reduziert den Arbeitsaufwand, den Sie für die Installation, Konfiguration und Aktualisierung von Add-ons aufwenden müssen.

Voraussetzungen

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

- Ein Amazon EKS-Clusterkonto mit Add-on-Abonnement
- AWS-Berechtigungen für den AWS Marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- AMI type: 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 file system

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. Wählen Sie im linken Navigationsbereich **Clusters** 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 dann **Weitere Add-ons abrufen**.
5. Führen Sie die folgenden Schritte aus, 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 Kästchen in der oberen rechten Ecke des Trident by NetApp-Feldes.
 - c. **Weiter** auswählen.
6. Gehen Sie auf der Seite **Ausgewählte Add-ons konfigurieren** wie folgt vor:



Überspringen Sie diese Schritte, wenn Sie die Pod Identity association 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 **configurationValues**-Parameter im Abschnitt **Konfigurationswerte** auf den role-arn fest, den Sie im vorherigen Schritt erstellt haben (Wert sollte folgendes Format haben):

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

+

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

7. Wählen Sie **Weiter**.
8. Auf der Seite **Review and add** wählen Sie **Create**.

Nach Abschluss der Add-on-Installation sehen Sie Ihr installiertes Add-on.

AWS CLI

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

Für Pod Identity verwenden Sie das folgende Format:



Verwenden Sie die

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

Für die IRSA-Authentifizierung verwenden Sie das folgende 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 Sie <role ARN> durch den 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

Verwaltungskonsolle

1. Öffnen Sie die Amazon EKS-Konsole <https://console.aws.amazon.com/eks/home#/clusters>.
2. Wählen Sie im linken Navigationsbereich **Clusters** aus.
3. Wählen Sie den Namen des Clusters aus, für den Sie das NetApp Trident CSI Add-on aktualisieren möchten.
4. Wählen Sie die Registerkarte **Add-ons** aus.
5. Wählen Sie **Trident by NetApp** und dann **Bearbeiten** aus.
6. Gehen Sie auf der Seite **Trident konfigurieren von NetApp** wie folgt vor:
 - a. Wählen Sie die **Version** aus, die Sie verwenden möchten.
 - b. Erweitern Sie die **Optional configuration settings** und nehmen Sie bei Bedarf Anpassungen vor.
 - c. **Änderungen speichern** auswählen.

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-on. Ersetzen Sie `my-cluster` durch Ihren 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 unter UPDATE AVAILABLE in der Ausgabe des vorherigen Schritts zurückgegeben wurde.

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

Wenn Sie die `--force` Option entfernen und eine der Amazon EKS Add-on-Einstellungen mit Ihren bestehenden Einstellungen in Konflikt steht, schlägt die Aktualisierung des Amazon EKS Add-ons fehl; Sie erhalten eine Fehlermeldung, die Ihnen hilft, den Konflikt zu beheben. Bevor Sie diese Option festlegen, stellen Sie sicher, dass das Amazon EKS Add-on keine Einstellungen verwaltet, die Sie verwalten müssen, da diese Einstellungen mit dieser Option überschrieben werden. Weitere Informationen zu anderen Optionen für diese Einstellung finden Sie unter ["Add-ons"](#). Weitere Informationen zur Amazon EKS Kubernetes-Feldverwaltung finden Sie unter ["Kubernetes-Feldmanagement"](#).

Deinstallieren/entfernen Sie das Trident EKS Add-on

Sie haben zwei Optionen, ein Amazon EKS add-on zu entfernen:

- **Add-on-Software auf Ihrem Cluster beibehalten** – Diese Option entfernt die Amazon EKS-Verwaltung aller Einstellungen. Außerdem wird die Möglichkeit entfernt, dass Amazon EKS Sie über Updates benachrichtigt und das Amazon EKS-Add-on nach einer Aktualisierung automatisch aktualisiert. Die Add-on-Software selbst bleibt jedoch auf Ihrem Cluster erhalten. Mit dieser Option wird das Add-on zu einer selbstverwalteten Installation, anstatt ein Amazon EKS-Add-on zu sein. Mit dieser Option gibt es keine Ausfallzeiten für das Add-on. Behalten Sie die `--preserve` Option im Befehl bei, um das Add-on beizubehalten.
- **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 auf Ihrem Cluster davon

abhängig sind. Entfernen Sie die `--preserve` Option aus dem `delete` Befehl, um das Add-on zu entfernen.



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

Verwaltungskontrolle

1. Öffnen Sie die Amazon EKS-Konsole unter <https://console.aws.amazon.com/eks/home#/clusters>.
2. Wählen Sie im linken Navigationsbereich **Clusters** 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 dann **Trident by NetApp**.*
5. Wählen Sie **Remove**.
6. Führen Sie im Dialogfeld **Remove netapp_trident-operator confirmation** die folgenden Schritte aus:
 - a. Wenn Amazon EKS die Einstellungen für das Add-on nicht mehr verwalten soll, wählen Sie **Preserve on cluster**. Tun Sie dies, wenn Sie die Add-on-Software auf Ihrem Cluster behalten und alle Einstellungen des Add-ons selbst verwalten möchten.
 - b. Geben Sie **netapp_trident-operator** ein.
 - c. Wählen Sie **Remove**.

AWS CLI

Ersetzen Sie `my-cluster` durch den 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 einer Speicherklasse

Der "**Kubernetes StorageClass-Objekt**" identifiziert einen Provisioner und weist den Provisioner an, wie Volumes bereitgestellt werden sollen. In diesem Abschnitt wird gezeigt, wie Sie ein Kubernetes-StorageClass-Objekt konfigurieren, das Trident als Provisioner angibt.

Erstellen Sie ein StorageClass-Objekt

Wenn Sie eine StorageClass für FSx for ONTAP erstellen, erstellt Trident automatisch die Backend-Konfiguration.



Wenn Sie das Speicher-Backend manuell konfigurieren möchten, lesen Sie bitte den [Erstellen Sie eine Kubernetes StorageClass ohne automatische Backend-Konfiguration](#) Abschnitt, um zu erfahren, wie Sie das Trident-Backend und die Speicherklasse separat erstellen.

Geben Sie die erforderlichen StorageClass-Parameter an

Die folgenden drei Parameter müssen beim Erstellen einer StorageClass definiert werden:

Parameter	Erforderlich	Typ	Beschreibung
fsxFileSystemID	Ja	Zeichenkette	FSx für NetApp ONTAP filesystem ID
storageDriverName	Ja	Zeichenkette	Trident-Speichertreiber (zum Beispiel, <code>ontap-nas</code> oder <code>ontap-san</code>)
credentialsName	Ja	Zeichenkette	Name des Kubernetes-Secrets, das die FSx for ONTAP Anmeldeinformationen enthält

Optionale Parameter angeben

Sie können optionale Backend-Parameter über die StorageClass übergeben. Definieren Sie alle optionalen Werte als Zeichenketten im StorageClass `parameters` Abschnitt. Eine vollständige Liste der Backend-Parameter finden Sie unter: ["FSx für NetApp ONTAP Backend-Konfiguration"](#).

Beispiel-StorageClass-Konfigurationsdateien.

Das folgende Beispiel zeigt eine StorageClass, die eine automatische Backend-Konfiguration auslöst.

YAML

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

JSON

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

Erstelle die StorageClass

Sobald Sie Ihre Konfigurationsdatei erstellt haben, führen Sie den folgenden Befehl aus, um die Speicherklasse zu erstellen.

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

Sie sollten nun eine **basic-csi** Storage-Class sowohl in Kubernetes als auch in Trident 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

Nachdem Sie die StorageClass angewendet haben, erstellt Trident das Backend automatisch. Sie können dann PersistentVolumeClaims erstellen, die auf diese StorageClass verweisen.

Überprüfen Sie den Status der Backend-Konfiguration

Trident speichert das Ergebnis der Backend-Erstellung in StorageClass-Annotationen.

Anmerkung	Beschreibung
<code>trident.netapp.io/configuratorStatus</code>	Konfigurationsergebnis (Success or Failure)
<code>trident.netapp.io/configuratorMessage</code>	Detaillierte Status- oder Fehlermeldung
<code>trident.netapp.io/configuratorName</code>	Name der internen Konfigurator-Ressource
<code>trident.netapp.io/managed</code>	Gibt an, dass die StorageClass von Trident verwaltet wird
<code>trident.netapp.io/additionalStoragePools</code>	Für dieses Backend erstellte Speicherpools

Um den Status zu überprüfen, führen Sie Folgendes aus:

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

Bestätigen Sie, dass `trident.netapp.io/configuratorStatus` auf `Success` gesetzt ist. Wenn der Wert `Failure` ist, überprüfen Sie `trident.netapp.io/configuratorMessage` auf den Fehler.

Fügen Sie zusätzliche FSxN-Dateisysteme hinzu

Wenn Sie zusätzliche Speicherkapazität benötigen, während Sie weiterhin dieselbe StorageClass verwenden, fügen Sie zusätzliche FSxN-Dateisystem-IDs hinzu.

Bearbeiten Sie die StorageClass und fügen Sie die folgende Anmerkung hinzu:

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

Nachdem Sie die Änderung angewendet haben, aktualisiert Trident die Backend-Konfiguration und die StorageClass-Annotationen.

Betriebliche Überlegungen und Einschränkungen

- Das Löschen einer StorageClass, die als automatische Backend-Konfiguration verwendet wird, löscht in der Regel auch das zugehörige Trident-Backend. Dies kann die Speicherkonnektivität beeinträchtigen und laufende Workloads unterbrechen. Prüfen Sie die Auswirkungen, bevor Sie eine verwaltete StorageClass löschen.
- Die automatische Backend-Konfiguration wird nur für AWS FSx für NetApp ONTAP unterstützt.

Erstellen Sie eine Kubernetes StorageClass ohne automatische Backend-Konfiguration

Wenn Sie das Trident Backend und StorageClass separat erstellen möchten, folgen Sie diesen Schritten.

Verstehen Sie, wie die automatische Backend-Konfiguration funktioniert

Trident leitet die Backend-Konfiguration aus der StorageClass-Definition ab. Wenn Sie die StorageClass anwenden, validiert Trident die erforderlichen Parameter, erstellt das Backend und versieht die StorageClass

mit dem Status.

Trident erstellt die VolumeSnapshotClass nur einmal. Trident verwendet dieselbe VolumeSnapshotClass für nachfolgende StorageClasses wieder.

Erstelle das Trident Backend

Um ein Trident-Backend zu erstellen, benötigen Sie eine Konfigurationsdatei im JSON- oder YAML-Format. Die Datei muss den gewünschten Speichertyp (NAS oder SAN), das Dateisystem, die SVM, von der Sie es beziehen möchten, und die Authentifizierungsmethode angeben. Das folgende Beispiel zeigt, wie Sie NAS-basierten Speicher definieren und mithilfe eines AWS-Secrets die Anmeldeinformationen für die SVM speichern, die Sie verwenden möchten:

YAML

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

JSON

```
{
  "apiVersion": "trident.netapp.io/v1",
  "kind": "TridentBackendConfig",
  "metadata": {
    "name": "backend-tbc-ontap-nas"
    "namespace": "trident"
  },
  "spec": {
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "tbc-ontap-nas",
    "svm": "svm-name",
    "aws": {
```

```

    "fsxFileSystemID": "fs-xxxxxxxxxx"
  },
  "managementLIF": null,
  "credentials": {
    "name": "arn:aws:secretsmanager:us-west-2:xxxxxxx:secret:secret-
name",
    "type": "awsarn"
  }
}
}

```

FSx for ONTAP-Treiberdetails

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

Treibername	Beschreibung
ontap-san	Jedes bereitgestellte PV ist eine LUN innerhalb eines eigenen Amazon FSx for NetApp ONTAP-Volumes. Empfohlen für Blockspeicher.
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 Informationen zum Treiber finden Sie unter ["NAS-Treiber"](#) und ["SAN-Treiber"](#).

Das Backend erstellen

Nach dem Erstellen der Konfigurationsdatei 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 den 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

Weitere Informationen zu anderen Konfigurationsoptionen finden Sie im [Erweiterte Backend Konfiguration und Beispiele](#) Abschnitt unten.

Konfigurieren einer Storage Class ohne automatische Backend-Konfiguration

Nachfolgend finden Sie Beispiele für Speicherklassenkonfigurationen zur Verwendung mit Trident und FSx für ONTAP.

Speicherklasse für NFS

Sie können dieses Beispiel verwenden, um StorageClass für Volumes mit NFS einzurichten (eine 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"
```

Speicherklasse für iSCSI

Verwenden Sie dieses Beispiel, um StorageClass 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"
```

Speicherklasse mit NFSv3 und AWS Bottlerocket

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

```
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
```

Trident StorageClass-Attribute

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
Medien ¹	Zeichenkette	hdd, hybrid, ssd	Pool enthält Medien dieses Typs; hybrid bedeutet beides	Medientyp angeben	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
provisioningType	Zeichenkette	dünn, dick	Pool unterstützt diese Bereitstellungsmethode	Bereitstellungsmethode angeben	dick: alle ontap; dünn: alle ontap & solidfire-san
backendType	Zeichenkette	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, azure-netapp-files, ontap-san-economy	Pool gehört zu dieser Art von Backend	Backend angeben	Alle Treiber
Momentaufnahmen	bool	wahr, falsch	Pool unterstützt Volumes mit Snapshots	Volume mit aktivierten Snapshots	ontap-nas, ontap-san, solidfire-san

Attribut	Typ	Werte	Angebot	Anfrage	Unterstützt von
Klone	bool	wahr, falsch	Pool unterstützt das Klonen von Volumes	Volume mit aktivierten Klonen	ontap-nas, ontap-san, solidfire-san
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	Volume garantiert diese IOPS	solidfire-san

¹: Wird von ONTAP Select oder FSx für ONTAP-Systeme nicht unterstützt

Siehe "[Kubernetes- und Trident-Objekte](#)" für Details dazu, wie Storage-Klassen mit dem PersistentVolumeClaim interagieren und Parameter zur Steuerung, wie Trident Volumes bereitstellt.

Erstellen Sie die Speicherklasse

Sobald Sie die StorageClass konfiguriert haben, können Sie sie in Kubernetes erstellen.

Schritte

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

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

2. Sie sollten nun eine **basic-csi** Storage-Class sowohl in Kubernetes als auch in Trident 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

SMB-Volumen bereitstellen

Sie können SMB-Volumes mithilfe des `ontap-nas` Treibers bereitstellen. Dazu müssen Sie jedoch die folgenden Schritte ausführen: "[Bereiten Sie die Bereitstellung von SMB-Volumes vor](#)".

Erweiterte Backend-Konfiguration und Beispiele

Siehe die folgende Tabelle für 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	Treibername + "_" + dataLIF
managementLIF	<p>IP-Adresse eines Clusters oder einer SVM-Management-LIF. Ein vollqualifizierter Domänenname (FQDN) kann 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, zum Beispiel [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Wenn Sie die <code>fsxFilesystemID</code> unter dem <code>aws</code> Feld angeben, müssen Sie die <code>managementLIF</code> nicht angeben, da Trident die SVM <code>managementLIF</code> Informationen von AWS abrufen. Sie müssen daher Anmeldeinformationen für einen Benutzer unter der SVM (zum Beispiel: <code>vsadmin</code>) angeben, und der Benutzer muss die <code>vsadmin</code> Rolle haben.</p>	"10.0.0.1", "[2001:1234:abcd::fefe]"

Parameter	Beschreibung	Beispiel
dataLIF	IP-Adresse des Protokoll-LIF. ONTAP NAS-Treiber: NetApp empfiehlt, dataLIF anzugeben. Falls nicht angegeben, ruft Trident dataLIFs vom SVM ab. Ein vollqualifizierter Domainname (FQDN) kann für die NFS-Mount-Operationen angegeben werden, wodurch die Erstellung eines Round-Robin-DNS zur Lastverteilung über mehrere dataLIFs ermöglicht wird. Kann nach der Ersteinrichtung geändert werden. ONTAP SAN-Treiber: Für iSCSI nicht angeben. Trident verwendet ONTAP Selective LUN Map, um die für den Aufbau einer Multipath-Sitzung benötigten iSCSI-LIFs zu ermitteln. Eine Warnung wird ausgegeben, 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, zum Beispiel [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	
autoExportPolicy	Automatische Erstellung und Aktualisierung von Exportrichtlinien aktivieren [Boolean]. Mit den Optionen autoExportPolicy und autoExportCIDRs kann Trident Exportrichtlinien automatisch verwalten.	false
autoExportCIDRs	Liste der CIDRs, anhand derer die Node-IPs von Kubernetes gefiltert werden, wenn autoExportPolicy aktiviert ist. Mit den Optionen autoExportPolicy und autoExportCIDRs kann Trident Exportrichtlinien automatisch verwalten.	"["0.0.0.0/0", "::/0"]"
labels	Satz beliebiger JSON-formatierter Bezeichnungen, die auf Volumes angewendet werden sollen	""

Parameter	Beschreibung	Beispiel
clientCertificate	Base64-kodierter Wert des Clientzertifikats. Wird für zertifikatbasierte Authentifizierung verwendet	""
clientPrivateKey	Base64-kodierter Wert des privaten Client-Schlüssels. Wird für zertifikatbasierte Authentifizierung verwendet	""
trustedCACertificate	Base64-kodierter Wert des vertrauenswürdigen CA-Zertifikats. Optional. Wird für zertifikatbasierte Authentifizierung verwendet.	""
username	Benutzername für die Verbindung zum Cluster oder zur SVM. Wird für die anmeldeinformationsbasierte Authentifizierung verwendet. Zum Beispiel vsadmin.	
password	Passwort zur Verbindung mit dem Cluster oder der SVM. Wird für die anmeldeinformationsbasierte Authentifizierung verwendet.	
svm	Zu verwendende Storage Virtual Machine	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 für NetApp ONTAP angeben. Die bereitgestellten fsxadmin und vsadmin enthalten nicht die erforderlichen Berechtigungen, um die aggregierte Nutzung abzurufen und sie mit Trident zu begrenzen.	Nicht verwenden.

Parameter	Beschreibung	Beispiel
limitVolumeSize	Die Bereitstellung schlägt fehl, wenn die angeforderte Volume-Größe diesen Wert überschreitet. Außerdem wird die maximale Größe der von ihr verwalteten Volumes für qtrees und LUNs beschränkt, und die qtreesPerFlexvol Option ermöglicht die Anpassung der maximalen Anzahl von qtrees pro FlexVol volume.	"" (wird nicht standardmäßig erzwungen)
lunsPerFlexvol	Maximale 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} Verwenden Sie debugTraceFlags nicht, es sei denn, Sie führen eine Fehlersuche durch und benötigen eine detaillierte Protokollausgabe.	null
nfsMountOptions	Kommagetrennte Liste der NFS-Mountoptionen. Die Mountoptionen für persistente Kubernetes-Volumes werden normalerweise in Speicherklassen angegeben, aber wenn keine Mountoptionen in einer Speicherklasse angegeben sind, verwendet Trident die Mountoptionen, die in der Konfigurationsdatei des Storage-Backends angegeben sind. Wenn weder in der Speicherklasse noch in der Konfigurationsdatei Mountoptionen angegeben sind, setzt Trident keine Mountoptionen für das zugehörige persistente Volume.	""
nasType	Konfigurieren Sie die Erstellung von NFS- oder SMB-Volumes. Optionen sind nfs, smb oder null. Muss auf smb gesetzt werden für SMB-Volumes. Die Einstellung auf null verwendet standardmäßig NFS-Volumes.	nfs
qtreesPerFlexvol	Maximale 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 ONTAP CLI erstellt wurde, oder einen Namen, damit 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 auf <code>true</code> gesetzt, verwendet Trident ONTAP REST APIs, um mit dem Backend zu kommunizieren. Diese Funktion erfordert ONTAP 9.11.1 und höher. Zusätzlich muss die verwendete ONTAP-Anmelderolle Zugriff auf die <code>ontap</code> Anwendung haben. Dies wird durch die vordefinierten <code>vsadmin</code> und <code>cluster-admin</code> Rollen erfüllt.	false
aws	Sie können Folgendes in der Konfigurationsdatei für AWS FSx for ONTAP angeben: - fsxFilesystemID: Geben Sie die ID des AWS FSx-Dateisystems an. - apiRegion: Name der AWS API-Region. - apikey: AWS API-Schlüssel. - secretKey: Geheimer AWS-Schlüssel.	"" "" ""
credentials	Geben Sie die FSx SVM-Anmeldeinformationen an, die im AWS Secrets Manager gespeichert werden sollen. - name: Amazon Resource Name (ARN) des Secrets, das die Anmeldeinformationen der SVM enthält. - type: Auf <code>awsarn</code> setzen. Weitere Informationen finden Sie unter "Erstellen Sie ein AWS Secrets Manager secret" .	

Backend-Konfigurationsoptionen für die Bereitstellung von Volumes

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

Parameter	Beschreibung	Standard
spaceAllocation	Speicherplatzzuweisung für LUNs	true
spaceReserve	Platzreservierungsmodus; "none" (dünn) oder "volume" (dick)	none
snapshotPolicy	Zu verwendende Snapshot-Richtlinie	none
qosPolicy	QoS-Richtliniengruppe, die für erstellte Volumes zugewiesen werden soll. Wählen Sie eine der qosPolicy oder adaptiveQosPolicy pro Speicherpool oder Backend. 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 jedes einzelne Element angewendet wird. Eine gemeinsam genutzte QoS-Richtliniengruppe erzwingt die Obergrenze für den Gesamtdurchsatz aller Workloads.	""
adaptiveQosPolicy	Adaptive QoS-Richtliniengruppe zur Zuweisung für erstellte Volumes. Wählen Sie eine der qosPolicy oder adaptiveQosPolicy pro Speicherpool oder Backend. Wird von ontap-nas-economy nicht unterstützt.	""
snapshotReserve	Prozentsatz des für Snapshots reservierten Volumens "0"	Wenn snapshotPolicy ist none, else ""
splitOnClone	Trennen Sie einen Klon bei seiner Erstellung von seinem übergeordneten Objekt	false
encryption	Aktivieren Sie NetApp Volume Encryption (NVE) auf dem neuen Volume; standardmäßig false. NVE muss auf dem Cluster lizenziert und aktiviert sein, damit diese Option verwendet werden kann. Wenn NAE im Backend aktiviert ist, wird jedes in Trident bereitgestellte Volume NAE-aktiviert. Weitere Informationen unter: "Wie Trident mit NVE und NAE zusammenarbeitet" .	false

Parameter	Beschreibung	Standard
luksEncryption	LUKS-Verschlüsselung aktivieren. Weitere Informationen enthält "Verwenden Sie Linux Unified Key Setup (LUKS)" . Nur SAN.	""
tieringPolicy	zu verwendende Tiering-Richtlinie none	
unixPermissions	Modus für neue Volumes. Für SMB-Volumes leer lassen.	""
securityStyle	Sicherheitsstil für neue Volumes. NFS unterstützt <code>mixed</code> und <code>unix</code> Sicherheitsstile. SMB unterstützt <code>mixed</code> und <code>ntfs</code> Sicherheitsstile.	NFS-Standard ist <code>unix</code> . SMB-Standard ist <code>ntfs</code> .

PVC konfigurieren

Dieser Abschnitt enthält Anweisungen zum Erstellen eines PersistentVolumeClaim (PVC), der die konfigurierte Kubernetes-StorageClass verwendet, um ein PV anzufordern. Im Erfolgsfall kann das PV anschließend in einen Pod eingebunden werden.

PVC erstellen

Ein ["PersistentVolumeClaim"](#) (PVC) ist eine Anfrage für den Zugriff auf das PersistentVolume im Cluster. Die PVC kann so konfiguriert werden, dass sie Speicherplatz einer bestimmten Größe oder eines bestimmten Zugriffsmodus anfordert. Mithilfe der zugehörigen StorageClass kann der Clusteradministrator mehr als nur PersistentVolume-Größe und Zugriffsmodus steuern – zum Beispiel Leistung oder Servicelevel.

Nachdem Sie das Trident-Backend und die StorageClass erstellt haben, können Sie ein PVC erstellen. Sobald das PVC erstellt ist, können Sie das Volume in einem Pod einbinden.

Beispielmanifeste

Die folgenden Beispiele zeigen grundlegende PVC-Konfigurationsoptionen.

PVC mit RWX-Zugriff

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

```
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 protection-gold zugeordnet ist.

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

PVC erstellen

Schritte

1. Die PVC wird erstellt.

```
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"](#) für Details dazu, wie Storage-Klassen mit dem PersistentVolumeClaim interagieren und Parameter zur Steuerung, wie Trident Volumes bereitstellt.

Eine Anwendung bereitstellen

Sobald die Storage Class und die PVC erstellt sind, können Sie das PV an einen Pod anhängen. In diesem Abschnitt finden Sie den Beispielbefehl und die Konfiguration, um das PV an einen Pod anzuhängen.

Eine Beispielanwendung bereitstellen

Schritte

1. Mountieren Sie das Volume in einem Pod.

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

Diese Beispiele zeigen grundlegende Konfigurationen, um das PVC an ein Pod anzuhängen:

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 mit `kubectl get pod --watch` überwachen.

2. Überprüfen Sie, ob das Volume auf `/my/mount/path` eingebunden ist.

```
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 nun löschen. Die Pod-Anwendung existiert dann nicht mehr, aber das Volume bleibt erhalten.

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

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

NetApp Trident vereinfacht die Verwaltung von Amazon FSx for NetApp ONTAP Storage in Kubernetes, sodass sich Ihre Entwickler und Administratoren auf die Anwendungsbereitstellung konzentrieren können. Das NetApp Trident EKS Add-on enthält die neuesten Sicherheitspatches, Fehlerbehebungen und ist von AWS für die Zusammenarbeit mit Amazon EKS validiert. Das EKS-Add-on ermöglicht es Ihnen, konsequent sicherzustellen, dass Ihre Amazon EKS-Cluster sicher und stabil sind, und reduziert den Arbeitsaufwand, den Sie für die Installation, Konfiguration und Aktualisierung von Add-ons aufwenden müssen.

Voraussetzungen

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

- Ein Amazon EKS-Clusterkonto mit Berechtigungen zur Verwendung von Add-ons. Weitere Informationen enthält ["Amazon EKS Add-ons"](#).
- AWS-Berechtigungen für den AWS Marketplace:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- AMI type: 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 file system

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 sich unter ["Erstellen Sie eine IAM-Rolle und ein AWS-Geheimnis"](#).
2. Navigieren Sie in Ihrem EKS Kubernetes-Cluster zur Registerkarte **Add-ons**.



① End of standard support for Kubernetes version 1.30 is July 28, 2025. On that date, your cluster will enter the extended support period with additional fees. For more information, see the [pricing page](#).

[Upgrade now](#)**▼ Cluster info** [Info](#)**Status**

✓ Active

Kubernetes version [Info](#)

1.30

Support period① [Standard support until July 28, 2025](#)**Provider**

EKS

Cluster health issues

✓ 0

Upgrade insights

✓ 0

Overview

Resources

Compute

Networking

Add-ons 1

Access

Observability

Update history

Tags

① New versions are available for 1 add-on.

✕

Add-ons (3) [Info](#)[View details](#)[Edit](#)[Remove](#)[Get more add-ons](#)

Any categ...

Any status

3 matches

< 1 >

3. Gehen Sie zu **AWS Marketplace add-ons** und wählen Sie die Kategorie *storage*.

AWS Marketplace add-ons (1)

Discover, subscribe to and configure EKS add-ons to enhance your EKS clusters.

Filtering options

Any category

NetApp, Inc.

Any pricing model

[Clear filters](#)

NetApp, Inc. ✕

< 1 >

**NetApp Trident**

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

Standard Contract**Category**
storage**Listed by**
[NetApp, Inc.](#)**Supported versions**
1.31, 1.30, 1.29, 1.28,
1.27, 1.26, 1.25, 1.24,
1.23**Pricing starting at**
[View pricing details](#)[Cancel](#)[Next](#)

4. Suchen Sie **NetApp Trident** und aktivieren Sie das Kontrollkästchen für das Trident-Add-on, und klicken Sie auf **Weiter**.

5. Wählen Sie die gewünschte Version des Add-on.

Configure selected add-ons settings

Configure the add-ons for your cluster by selecting settings.

NetApp Trident

Remove add-on

Listed by

Category

Status

NetApp

storage

Ready to install

You're subscribed to this software

View subscription

You can view the terms and pricing details for this product or choose another offer if one is available.

Version

Select the version for this add-on.

v25.6.0-eksbuild.1

Optional configuration settings

Cancel

Previous

Next

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

Review and add

Step 1: Select add-ons

Selected add-ons (1)

Find add-on

< 1 >

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

Step 2: Configure selected add-ons settings

Selected add-ons version (1)

< 1 >

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

EKS Pod Identity (0)

< 1 >

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

- Wenn Sie IRSA (IAM roles for service account) verwenden, beachten Sie die zusätzlichen Konfigurationsschritte ["hier"](#).
- Die Option **Create** wird ausgewählt.

9. Überprüfen Sie, ob der Status des Add-ons *Active* ist.

The screenshot shows the AWS EKS Add-ons console. At the top, there's a search bar with 'netapp' entered, showing '1 match'. Below the search bar, the 'NetApp Trident' add-on is listed. It is categorized as 'storage' and its status is 'Active' (indicated by a green checkmark). The version is 'v24.10.0-eksbuild.1'. The 'EKS Pod Identity' is set to '-', and the 'IAM role for service account (IRSA)' is 'Not set'. A 'View subscription' button is located at the bottom right of the add-on details card.

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

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

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

11. Fahren Sie mit der Einrichtung fort und konfigurieren Sie das Storage-Backend. Informationen finden sich unter "[Konfigurieren Sie das Storage-Backend](#)".

Installieren/Deinstallieren des Trident EKS Add-ons über die CLI

Installieren Sie das NetApp Trident EKS-Add-on mithilfe der CLI:

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 dedizierten Version)
```

Der folgende Beispielbefehl installiert das Trident EKS-Add-on Version 25.6.1:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.1-eksbuild.1 (mit einer dedizierten Version)
```

Der folgende Beispielbefehl installiert das Trident EKS-Add-on Version 25.6.2:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.2-eksbuild.1 (mit einer dedizierten Version)
```

Deinstallieren Sie das NetApp Trident EKS add-on über die CLI:

Der folgende Befehl deinstalliert das Trident EKS add-on:

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.