



Amazon FSx for NetApp ONTAP

Trident

NetApp

January 15, 2026

Sommario

Amazon FSx for NetApp ONTAP	1
Utilizzare Trident con Amazon FSx for NetApp ONTAP	1
Requisiti	1
Considerazioni	1
Autenticazione	2
Immagini macchina Amazon (AMI) testate	2
Trova maggiori informazioni	3
Crea un ruolo IAM e un segreto AWS	3
Crea il segreto di AWS Secrets Manager	4
Crea policy IAM	4
Installa Trident	8
Installa Trident tramite helm	9
Installa Trident tramite il componente aggiuntivo EKS	11
Configurare il backend di archiviazione	16
Integrazione dei driver ONTAP SAN e NAS	16
Dettagli del driver FSx per ONTAP	18
Configurazione avanzata del backend ed esempi	19
Opzioni di configurazione del backend per il provisioning dei volumi	23
Prepararsi al provisioning dei volumi SMB	25
Configurare una classe di archiviazione e PVC	26
Creare una classe di archiviazione	26
Creare il PVC	28
Attributi Trident	30
Distribuisci l'applicazione di esempio	31
Configurare il componente aggiuntivo Trident EKS su un cluster EKS	32
Prerequisiti	32
Passi	33
Installa/disinstalla il componente aggiuntivo Trident EKS tramite CLI	35

Amazon FSx for NetApp ONTAP

Utilizzare Trident con Amazon FSx for NetApp ONTAP

"Amazon FSx for NetApp ONTAP" è un servizio AWS completamente gestito che consente ai clienti di avviare ed eseguire file system basati sul sistema operativo di storage NetApp ONTAP . FSx for ONTAP ti consente di sfruttare le funzionalità, le prestazioni e le capacità amministrative NetApp che conosci, sfruttando al contempo la semplicità, l'agilità, la sicurezza e la scalabilità dell'archiviazione dei dati su AWS. FSx per ONTAP supporta le funzionalità del file system ONTAP e le API di amministrazione.

Puoi integrare il tuo file system Amazon FSx for NetApp ONTAP con Trident per garantire che i cluster Kubernetes in esecuzione in Amazon Elastic Kubernetes Service (EKS) possano fornire volumi persistenti a blocchi e file supportati da ONTAP.

Un file system è la risorsa principale in Amazon FSx, analogamente a un cluster ONTAP in locale. All'interno di ogni SVM è possibile creare uno o più volumi, ovvero contenitori di dati in cui vengono archiviati i file e le cartelle nel file system. Con Amazon FSx for NetApp ONTAP verrà fornito come file system gestito nel cloud. Il nuovo tipo di file system si chiama * NetApp ONTAP*.

Utilizzando Trident con Amazon FSx for NetApp ONTAP, puoi garantire che i cluster Kubernetes in esecuzione in Amazon Elastic Kubernetes Service (EKS) possano fornire volumi persistenti di file e blocchi supportati da ONTAP.

Requisiti

Inoltre "Requisiti Trident" Per integrare FSx per ONTAP con Trident, è necessario:

- Un cluster Amazon EKS esistente o un cluster Kubernetes autogestito con `kubectl` installato.
- Un file system Amazon FSx for NetApp ONTAP esistente e una macchina virtuale di storage (SVM) raggiungibile dai nodi worker del cluster.
- Nodi worker preparati per "NFS o iSCSI" .



Assicurati di seguire i passaggi di preparazione del nodo richiesti per Amazon Linux e Ubuntu "[Immagini della macchina Amazon](#)" (AMI) a seconda del tipo di AMI EKS.

Considerazioni

- Volumi SMB:
 - I volumi SMB sono supportati utilizzando `ontap-nas` solo conducente.
 - I volumi SMB non sono supportati dal componente aggiuntivo Trident EKS.
 - Trident supporta volumi SMB montati su pod in esecuzione solo su nodi Windows. Fare riferimento a "[Prepararsi al provisioning dei volumi SMB](#)" per i dettagli.
- Prima di Trident 24.02, i volumi creati sui file system Amazon FSx con backup automatici abilitati non potevano essere eliminati da Trident. Per evitare questo problema in Trident 24.02 o versioni successive, specificare `fsxFilesystemID`, `AWS apiRegion`, `AWS apiKey` e `AWS secretKey` nel file di configurazione backend per AWS FSx per ONTAP.



Se si specifica un ruolo IAM per Trident, è possibile omettere di specificare il `apiRegion`, `apiKey`, E `secretKey` campi a Trident in modo esplicito. Per maggiori informazioni, fare riferimento a "[Opzioni di configurazione ed esempi di FSx per ONTAP](#)".

Utilizzo simultaneo del driver Trident SAN/iSCSI ed EBS-CSI

Se si prevede di utilizzare i driver `ontap-san` (ad esempio, iSCSI) con AWS (EKS, ROSA, EC2 o qualsiasi altra istanza), la configurazione multipath richiesta sui nodi potrebbe entrare in conflitto con il driver CSI di Amazon Elastic Block Store (EBS). Per garantire che il multipathing funzioni senza interferire con i dischi EBS sullo stesso nodo, è necessario escludere EBS dalla configurazione del multipathing. Questo esempio mostra un `multipath.conf` file che include le impostazioni Trident richieste escludendo i dischi EBS dal multipathing:

```
defaults {
    find_multipaths no
}

blacklist {
    device {
        vendor "NVME"
        product "Amazon Elastic Block Store"
    }
}
```

Autenticazione

Trident offre due modalità di autenticazione.

- Basato su credenziali (consigliato): memorizza le credenziali in modo sicuro in AWS Secrets Manager. Puoi usare il `fsxadmin` utente per il tuo file system o il `vsadmin` utente configurato per il tuo SVM.



Trident si aspetta di essere gestito come un `vsadmin` Utente SVM o come utente con un nome diverso che ha lo stesso ruolo. Amazon FSx for NetApp ONTAP ha un `fsxadmin` utente che è una sostituzione limitata ONTAP `admin` utente del cluster. Consigliamo vivamente di utilizzare `vsadmin` con Trident.

- Basato su certificato: Trident comunicherà con l'SVM sul file system FSx utilizzando un certificato installato sull'SVM.

Per i dettagli sull'abilitazione dell'autenticazione, fare riferimento all'autenticazione per il tipo di driver:

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

Immagini macchina Amazon (AMI) testate

Il cluster EKS supporta vari sistemi operativi, ma AWS ha ottimizzato alcune Amazon Machine Image (AMI) per container ed EKS. Le seguenti AMI sono state testate con NetApp Trident 25.02.

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

AL2023_x86_64_STANDARD	Sì	Sì	Sì	Sì
AL2_x86_64	Sì	Sì	Sì*	Sì*
BOTTLEROCKET_x86_64	Sì**	Sì	N / A	N / A
AL2023_ARM_64_STANDARD	Sì	Sì	Sì	Sì
AL2_ARM_64	Sì	Sì	Sì*	Sì*
BOTTLEROCKET_ARM_64	Sì**	Sì	N / A	N / A

- * Impossibile eliminare il PV senza riavviare il nodo
- ** Non funziona con NFSv3 con Trident versione 25.02.



Se l'AMI desiderata non è elencata qui, non significa che non sia supportata; significa semplicemente che non è stata testata. Questo elenco serve come guida per gli AMI di cui è noto il funzionamento.

Test eseguiti con:

- Versione EKS: 1.32
- Metodo di installazione: Helm 25.06 e come componente aggiuntivo AWS 25.06
- Per NAS sono stati testati sia NFSv3 che NFSv4.1.
- Per SAN è stato testato solo iSCSI, non NVMe-oF.

Test eseguiti:

- Crea: Classe di archiviazione, pvc, pod
- Elimina: pod, pvc (normale, qtree/lun – economy, NAS con backup AWS)

Trova maggiori informazioni

- ["Documentazione Amazon FSx for NetApp ONTAP"](#)
- ["Post del blog su Amazon FSx for NetApp ONTAP"](#)

Crea un ruolo IAM e un segreto AWS

È possibile configurare i pod Kubernetes per accedere alle risorse AWS autenticandosi come ruolo AWS IAM anziché fornire credenziali AWS esplicite.



Per eseguire l'autenticazione tramite un ruolo AWS IAM, è necessario disporre di un cluster Kubernetes distribuito tramite EKS.

Crea il segreto di AWS Secrets Manager

Poiché Trident emetterà API su un server virtuale FSx per gestire l'archiviazione per te, avrà bisogno delle credenziali per farlo. Il modo sicuro per trasmettere tali credenziali è tramite un segreto AWS Secrets Manager. Pertanto, se non ne hai già uno, dovrai creare un segreto AWS Secrets Manager che contenga le credenziali per l'account vsadmin.

Questo esempio crea un segreto AWS Secrets Manager per archiviare le credenziali Trident CSI:

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

Crea policy IAM

Per funzionare correttamente, Trident necessita anche delle autorizzazioni AWS. Pertanto, è necessario creare una policy che fornisca a Trident le autorizzazioni di cui ha bisogno.

Gli esempi seguenti creano una policy IAM utilizzando l'AWS CLI:

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

Esempio di JSON della policy:

```

{
  "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"
}

```

Crea identità Pod o ruolo IAM per l'associazione dell'account di servizio (IRSA)

È possibile configurare un account di servizio Kubernetes affinché assuma un ruolo AWS Identity and Access Management (IAM) con EKS Pod Identity o un ruolo IAM per l'associazione dell'account di servizio (IRSA). Tutti i Pod configurati per utilizzare l'account di servizio possono quindi accedere a qualsiasi servizio AWS per il quale il ruolo dispone delle autorizzazioni di accesso.

Identità del pod

Le associazioni Amazon EKS Pod Identity consentono di gestire le credenziali per le applicazioni, in modo simile a come i profili delle istanze Amazon EC2 forniscono le credenziali alle istanze Amazon EC2.

Installa Pod Identity sul tuo cluster EKS:

Puoi creare l'identità del Pod tramite la console AWS o utilizzando il seguente comando AWS CLI:

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

Per maggiori informazioni fare riferimento a "[Configurare l'agente di identità del pod Amazon EKS](#)".

Crea trust-relationship.json:

Creare trust-relationship.json per consentire al Service Principal EKS di assumere questo ruolo per Pod Identity. Quindi crea un ruolo con questa policy di attendibilità:

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

file trust-relationship.json:

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

Associare la policy del ruolo al ruolo IAM:

Associa il criterio di ruolo del passaggio precedente al ruolo IAM creato:

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

Crea un'associazione di identità pod:

Crea un'associazione di identità pod tra il ruolo IAM e l'account del servizio Trident (trident-controller)

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

Ruolo IAM per l'associazione dell'account di servizio (IRSA)

Utilizzando l'AWS CLI:

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

file trust-relationship.json:

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

Aggiornare i seguenti valori nel trust-relationship.json file:

- <account_id> - ID del tuo account AWS
- <oidc_provider> - L'OIDC del cluster EKS. È possibile ottenere oidc_provider eseguendo:

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

Associare il ruolo IAM alla policy IAM:

Una volta creato il ruolo, associare il criterio (creato nel passaggio precedente) al ruolo utilizzando questo comando:

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

Verifica che il fornitore OICD sia associato:

Verifica che il tuo provider OIDC sia associato al tuo cluster. Puoi verificarlo usando questo comando:

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

Se l'output è vuoto, utilizzare il seguente comando per associare IAM OIDC al cluster:

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

Se si utilizza eksctl, utilizzare l'esempio seguente per creare un ruolo IAM per l'account di servizio in EKS:

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

Install Trident

Trident semplifica la gestione dello storage Amazon FSx for NetApp ONTAP in Kubernetes, consentendo a sviluppatori e amministratori di concentrarsi sulla

distribuzione delle applicazioni.

Puoi installare Trident utilizzando uno dei seguenti metodi:

- Timone
- Componente aggiuntivo EKS

Se si desidera utilizzare la funzionalità snapshot, installare il componente aggiuntivo CSI Snapshot Controller. Fare riferimento a "[Abilita la funzionalità snapshot per i volumi CSI](#)" per maggiori informazioni.

Install Trident tramite helm

Identità del pod

1. Aggiungere il repository Trident Helm:

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

2. Installa Trident utilizzando il seguente esempio:

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

Puoi usare il `helm list` comando per rivedere i dettagli dell'installazione quali nome, spazio dei nomi, grafico, stato, versione dell'app e numero di revisione.

```
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	100.2502.0	deployed	trident-operator-25.02.0

Associazione account di servizio (IRSA)

1. Aggiungere il repository Trident Helm:

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

2. Imposta i valori per **cloud provider** e **cloud identity**:

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

Puoi usare il `helm list` comando per rivedere i dettagli dell'installazione quali nome, spazio dei nomi, grafico, stato, versione dell'app e numero di revisione.

```
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	trident-operator-100.2506.0	deployed	trident-operator-25.06.0

Se intendi utilizzare iSCSI, assicurati che iSCSI sia abilitato sul tuo computer client. Se si utilizza il sistema operativo AL2023 Worker node, è possibile automatizzare l'installazione del client iSCSI aggiungendo il parametro `node_prep` nell'installazione di helm:



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

Installa Trident tramite il componente aggiuntivo EKS

Il componente aggiuntivo Trident EKS include le patch di sicurezza più recenti, le correzioni di bug ed è convalidato da AWS per funzionare con Amazon EKS. Il componente aggiuntivo EKS consente di garantire costantemente la sicurezza e la stabilità dei cluster Amazon EKS e di ridurre la quantità di lavoro necessaria per installare, configurare e aggiornare i componenti aggiuntivi.

Prerequisiti

Prima di configurare il componente aggiuntivo Trident per AWS EKS, assicurati di disporre di quanto segue:

- Un account cluster Amazon EKS con abbonamento aggiuntivo
- Autorizzazioni AWS per il marketplace AWS:
`"aws-marketplace:ViewSubscriptions",`
`"aws-marketplace:Subscribe",`
`"aws-marketplace:Unsubscribe"`
- Tipo AMI: Amazon Linux 2 (AL2_x86_64) o Amazon Linux 2 Arm (AL2_ARM_64)
- Tipo di nodo: AMD o ARM
- Un file system Amazon FSx for NetApp ONTAP esistente

Abilita il componente aggiuntivo Trident per AWS

Console di gestione

1. Aprire la console Amazon EKS all'indirizzo <https://console.aws.amazon.com/eks/home#/clusters> .
2. Nel riquadro di navigazione a sinistra, seleziona **Cluster**.
3. Selezionare il nome del cluster per il quale si desidera configurare il componente aggiuntivo NetApp Trident CSI.
4. Seleziona **Componenti aggiuntivi** e poi **Ottieni altri componenti aggiuntivi**.
5. Per selezionare il componente aggiuntivo, seguire questi passaggi:
 - a. Scorrere verso il basso fino alla sezione **Componenti aggiuntivi di AWS Marketplace** e digitare **"Trident"** nella casella di ricerca.
 - b. Selezionare la casella di controllo nell'angolo in alto a destra della casella Trident by NetApp .
 - c. Selezionare **Avanti**.
6. Nella pagina delle impostazioni **Configura componenti aggiuntivi selezionati**, procedi come segue:



Salta questi passaggi se utilizzi l'associazione Pod Identity.

- a. Seleziona la **Versione** che desideri utilizzare.
- b. Se si utilizza l'autenticazione IRSA, assicurarsi di impostare i valori di configurazione disponibili nelle impostazioni di configurazione facoltative:
 - Seleziona la **Versione** che desideri utilizzare.
 - Segui lo **schema di configurazione del componente aggiuntivo** e imposta il parametro **configurationValues** nella sezione **Valori di configurazione** sul role-arn creato nel passaggio precedente (il valore deve essere nel seguente formato):

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

+

Se si seleziona Sostituisci per il metodo di risoluzione dei conflitti, una o più impostazioni del componente aggiuntivo esistente possono essere sovrascritte con le impostazioni del componente aggiuntivo Amazon EKS. Se non si abilita questa opzione e si verifica un conflitto con le impostazioni esistenti, l'operazione fallisce. È possibile utilizzare il messaggio di errore risultante per risolvere il conflitto. Prima di selezionare questa opzione, assicurati che il componente aggiuntivo Amazon EKS non gestisca impostazioni che devi gestire autonomamente.

7. Selezionare **Avanti**.
8. Nella pagina **Revisiona e aggiungi**, seleziona **Crea**.

Una volta completata l'installazione del componente aggiuntivo, verrà visualizzato il componente aggiuntivo installato.

Interfaccia a riga di comando AWS

1. Crea il add-on.json file:

Per l'identità del pod, utilizzare il seguente formato:

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

Per l'autenticazione IRSA, utilizzare il seguente formato:

```
{  
  "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"  
  }  
}
```



Sostituire <role ARN> con l'ARN del ruolo creato nel passaggio precedente.

2. Installa il componente aggiuntivo Trident EKS.

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

eksctl

Il seguente comando di esempio installa il componente aggiuntivo Trident EKS:

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

Aggiorna il componente aggiuntivo Trident EKS

Console di gestione

1. Apri la console Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters> .
2. Nel riquadro di navigazione a sinistra, seleziona **Cluster**.
3. Selezionare il nome del cluster per il quale si desidera aggiornare il componente aggiuntivo NetApp Trident CSI.
4. Selezionare la scheda **Componenti aggiuntivi**.
5. Selezionare * Trident by NetApp* e quindi **Modifica**.
6. Nella pagina **Configura Trident di NetApp**, procedere come segue:
 - a. Seleziona la **Versione** che desideri utilizzare.
 - b. Espandi le **Impostazioni di configurazione facoltative** e modificalle secondo necessità.
 - c. Seleziona **Salva modifiche**.

Interfaccia a riga di comando AWS

L'esempio seguente aggiorna il componente aggiuntivo EKS:

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

eksctl

- Controlla la versione corrente del tuo componente aggiuntivo FSxN Trident CSI. Sostituire my-cluster con il nome del tuo cluster.

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

Esempio di output:

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'" }			

- Aggiornare il componente aggiuntivo alla versione restituita in AGGIORNAMENTO DISPONIBILE nell'output del passaggio precedente.

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

Se si rimuove il `--force` opzione e una qualsiasi delle impostazioni del componente aggiuntivo Amazon EKS è in conflitto con le impostazioni esistenti, l'aggiornamento del componente aggiuntivo Amazon EKS non riesce e viene visualizzato un messaggio di errore che consente di risolvere il conflitto. Prima di specificare questa opzione, assicurati che il componente aggiuntivo Amazon EKS non gestisca le impostazioni che devi gestire, perché tali impostazioni vengono sovrascritte con questa opzione. Per ulteriori informazioni sulle altre opzioni per questa impostazione, vedere "[Componenti aggiuntivi](#)". Per ulteriori informazioni sulla gestione sul campo di Amazon EKS Kubernetes, vedere "[Gestione del campo Kubernetes](#)".

Disinstallare/rimuovere il componente aggiuntivo Trident EKS

Per rimuovere un componente aggiuntivo Amazon EKS sono disponibili due opzioni:

- **Conserva il software aggiuntivo sul tuo cluster:** questa opzione rimuove la gestione di qualsiasi impostazione da parte di Amazon EKS. Rimuove inoltre la possibilità per Amazon EKS di notificare gli aggiornamenti e di aggiornare automaticamente il componente aggiuntivo Amazon EKS dopo aver avviato un aggiornamento. Tuttavia, mantiene il software aggiuntivo sul cluster. Questa opzione rende il componente aggiuntivo un'installazione autogestita, anziché un componente aggiuntivo Amazon EKS. Con questa opzione non ci saranno tempi di inattività per il componente aggiuntivo. Conservare il `--preserve` opzione nel comando per preservare il componente aggiuntivo.
- **Rimuovere completamente il software aggiuntivo dal cluster:** NetApp consiglia di rimuovere il componente aggiuntivo Amazon EKS dal cluster solo se nel cluster non sono presenti risorse che dipendono da esso. Rimuovere il `--preserve` opzione dal `delete` comando per rimuovere il componente aggiuntivo.



Se al componente aggiuntivo è associato un account IAM, l'account IAM non viene rimosso.

Console di gestione

1. Aprire la console Amazon EKS all'indirizzo <https://console.aws.amazon.com/eks/home#/clusters> .
2. Nel riquadro di navigazione a sinistra, seleziona **Cluster**.
3. Selezionare il nome del cluster per il quale si desidera rimuovere il componente aggiuntivo NetApp Trident CSI.
4. Selezionare la scheda **Componenti aggiuntivi** e quindi selezionare * Trident by NetApp*.*
5. Seleziona **Rimuovi**.
6. Nella finestra di dialogo **Rimuovi conferma netapp_trident-operator**, procedere come segue:
 - a. Se desideri che Amazon EKS interrompa la gestione delle impostazioni per il componente aggiuntivo, seleziona **Conserva nel cluster**. Eseguire questa operazione se si desidera mantenere il software aggiuntivo sul cluster, in modo da poter gestire autonomamente tutte le impostazioni dell'add-on.
 - b. Inserisci **netapp_trident-operator**.
 - c. Seleziona **Rimuovi**.

Interfaccia a riga di comando AWS

Sostituire `my-cluster` con il nome del tuo cluster, quindi esegui il seguente comando.

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

eksctl

Il seguente comando disinstalla il componente aggiuntivo Trident EKS:

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

Configurare il backend di archiviazione

Integrazione dei driver ONTAP SAN e NAS

Per creare un backend di archiviazione, è necessario creare un file di configurazione in formato JSON o YAML. Il file deve specificare il tipo di storage desiderato (NAS o SAN), il file system e l'SVM da cui ottenerlo e come autenticarsi. L'esempio seguente mostra come definire l'archiviazione basata su NAS e utilizzare un segreto AWS per archiviare le credenziali nell'SVM che si desidera utilizzare:

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"
    }
  }
}
```

Eseguire i seguenti comandi per creare e convalidare la configurazione del backend Trident (TBC):

- Crea la configurazione del backend Trident (TBC) dal file yaml ed esegui il seguente comando:

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

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

- Convalida che la configurazione del backend Trident (TBC) sia stata creata correttamente:

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

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

Dettagli del driver FSx per ONTAP

È possibile integrare Trident con Amazon FSx for NetApp ONTAP utilizzando i seguenti driver:

- **ontap-san**: Ogni PV fornito è una LUN all'interno del proprio volume Amazon FSx for NetApp ONTAP . Consigliato per l'archiviazione a blocchi.
- **ontap-nas**: Ogni PV fornito è un volume Amazon FSx for NetApp ONTAP completo. Consigliato per NFS e SMB.
- **ontap-san-economy**: Ogni PV fornito è una LUN con un numero configurabile di LUN per volume Amazon FSx for NetApp ONTAP .
- **ontap-nas-economy**: Ogni PV fornito è un qtree, con un numero configurabile di qtree per volume Amazon FSx for NetApp ONTAP .
- **ontap-nas-flexgroup**: Ogni PV fornito è un volume Amazon FSx for NetApp ONTAP FlexGroup completo.

Per i dettagli del driver, fare riferimento a "[Driver NAS](#)" E "[Driver SAN](#)".

Una volta creato il file di configurazione, esegui questo comando per crearlo all'interno del tuo EKS:

```
kubectl create -f configuration_file
```

Per verificare lo stato, eseguire questo comando:

```
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

Configurazione avanzata del backend ed esempi

Per le opzioni di configurazione del backend, consultare la seguente tabella:

Parametro	Descrizione	Esempio
version		Sempre 1
storageDriverName	Nome del driver di archiviazione	ontap-nas, ontap-nas-economy , ontap-nas-flexgroup , ontap-san , ontap-san-economy
backendName	Nome personalizzato o backend di archiviazione	Nome del driver + "_" + dataLIF
managementLIF	Indirizzo IP di un cluster o di un LIF di gestione SVM. È possibile specificare un nome di dominio completo (FQDN). Può essere impostato per utilizzare indirizzi IPv6 se Trident è stato installato utilizzando il flag IPv6. Gli indirizzi IPv6 devono essere definiti tra parentesi quadre, ad esempio [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Se fornisci il fsxFilesystemID sotto il aws campo, non è necessario fornire il managementLIF perché Trident recupera l'SVM managementLIF informazioni da AWS. Quindi, è necessario fornire le credenziali per un utente sotto l'SVM (ad esempio: vsadmin) e l'utente deve avere il vsadmin ruolo.	"10.0.0.1", "[2001:1234:abcd::fefe]"

Parametro	Descrizione	Esempio
dataLIF	Indirizzo IP del protocollo LIF. * Driver ONTAP NAS*: NetApp consiglia di specificare dataLIF. Se non specificato, Trident recupera i dataLIF dall'SVM. È possibile specificare un nome di dominio completo (FQDN) da utilizzare per le operazioni di montaggio NFS, consentendo di creare un DNS round-robin per bilanciare il carico su più dataLIF. Può essere modificato dopo l'impostazione iniziale. Fare riferimento a . * Driver ONTAP SAN*: Non specificare per iSCSI. Trident utilizza ONTAP Selective LUN Map per scoprire gli iSCI LIF necessari per stabilire una sessione multi-percorso. Se dataLIF è definito in modo esplicito, viene generato un avviso. Può essere impostato per utilizzare indirizzi IPv6 se Trident è stato installato utilizzando il flag IPv6. Gli indirizzi IPv6 devono essere definiti tra parentesi quadre, ad esempio [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].	
autoExportPolicy	Abilita la creazione e l'aggiornamento automatici dei criteri di esportazione [Booleano]. Utilizzando il autoExportPolicy E autoExportCIDRs opzioni, Trident può gestire automaticamente le policy di esportazione.	false
autoExportCIDRs	Elenco di CIDR per filtrare gli IP dei nodi di Kubernetes quando autoExportPolicy è abilitato. Utilizzando il autoExportPolicy E autoExportCIDRs opzioni, Trident può gestire automaticamente le policy di esportazione.	"["0.0.0.0/0", "::/0"]"
labels	Insieme di etichette arbitrarie formattate in JSON da applicare ai volumi	""
clientCertificate	Valore codificato in Base64 del certificato client. Utilizzato per l'autenticazione basata su certificato	""

Parametro	Descrizione	Esempio
clientPrivateKey	Valore codificato in Base64 della chiave privata del client. Utilizzato per l'autenticazione basata su certificato	""
trustedCACertificate	Valore codificato in Base64 del certificato CA attendibile. Opzionale. Utilizzato per l'autenticazione basata su certificato.	""
username	Nome utente per connettersi al cluster o alla SVM. Utilizzato per l'autenticazione basata sulle credenziali. Ad esempio, vsadmin.	
password	Password per connettersi al cluster o alla SVM. Utilizzato per l'autenticazione basata sulle credenziali.	
svm	Macchina virtuale di archiviazione da utilizzare	Derivato se è specificato un managementLIF SVM.
storagePrefix	Prefisso utilizzato durante il provisioning di nuovi volumi nell'SVM. Non può essere modificato dopo la creazione. Per aggiornare questo parametro, sarà necessario creare un nuovo backend.	trident
limitAggregateUsage	Non specificare per Amazon FSx for NetApp ONTAP. Il fornito fsxadmin E vsadmin non contengono le autorizzazioni richieste per recuperare l'utilizzo aggregato e limitarlo tramite Trident.	Non utilizzare.
limitVolumeSize	Il provisioning non riesce se la dimensione del volume richiesto è superiore a questo valore. Limita inoltre la dimensione massima dei volumi che gestisce per qtree e LUN e qtreesPerFlexvol l'opzione consente di personalizzare il numero massimo di qtree per FlexVol volume	"" (non applicato di default)
lunsPerFlexvol	Il numero massimo di LUN per volume Flexvol deve essere compreso nell'intervallo [50, 200]. Solo SAN.	"100"

Parametro	Descrizione	Esempio
debugTraceFlags	Flag di debug da utilizzare durante la risoluzione dei problemi. Esempio, {"api":false, "method":true} Non utilizzare debugTraceFlags a meno che non si stia risolvendo un problema e si necessiti di un dump di registro dettagliato.	null
nfsMountOptions	Elenco separato da virgole delle opzioni di montaggio NFS. Le opzioni di montaggio per i volumi persistenti di Kubernetes sono normalmente specificate nelle classi di archiviazione, ma se non vengono specificate opzioni di montaggio in una classe di archiviazione, Trident utilizzerà le opzioni di montaggio specificate nel file di configurazione del backend di archiviazione. Se non vengono specificate opzioni di montaggio nella classe di archiviazione o nel file di configurazione, Trident non imposta alcuna opzione di montaggio su un volume persistente associato.	""
nasType	Configurare la creazione di volumi NFS o SMB. Le opzioni sono nfs , smb , o nullo. Deve essere impostato su smb per volumi SMB. Impostando il valore su null, i volumi NFS vengono impostati di default.	nfs
qtreesPerFlexvol	Numero massimo di Qtree per FlexVol volume, deve essere compreso nell'intervallo [50, 300]	"200"
smbShare	È possibile specificare uno dei seguenti elementi: il nome di una condivisione SMB creata tramite Microsoft Management Console o ONTAP CLI oppure un nome che consente a Trident di creare la condivisione SMB. Questo parametro è obbligatorio per i backend Amazon FSx for ONTAP .	smb-share

Parametro	Descrizione	Esempio
useREST	Parametro booleano per utilizzare le API REST ONTAP . Quando impostato su true Trident utilizzerà le API REST ONTAP per comunicare con il backend. Questa funzionalità richiede ONTAP 9.11.1 e versioni successive. Inoltre, il ruolo di accesso ONTAP utilizzato deve avere accesso a ontap applicazione. Ciò è soddisfatto dal predefinito vsadmin E cluster-admin ruoli.	false
aws	È possibile specificare quanto segue nel file di configurazione per AWS FSx per ONTAP: - fsxFilesystemID : Specificare l'ID del file system AWS FSx. - apiRegion : Nome della regione API AWS. - apikey : Chiave API AWS. - secretKey : Chiave segreta AWS.	"" "" ""
credentials	Specificare le credenziali FSx SVM da archiviare in AWS Secrets Manager. - name : Amazon Resource Name (ARN) del segreto, che contiene le credenziali di SVM. - type : Impostato su awsarn . Fare riferimento a " Crea un segreto AWS Secrets Manager " per maggiori informazioni.	

Opzioni di configurazione del backend per il provisioning dei volumi

È possibile controllare il provisioning predefinito utilizzando queste opzioni in defaults sezione della configurazione. Per un esempio, vedere gli esempi di configurazione riportati di seguito.

Parametro	Descrizione	Predefinito
spaceAllocation	Assegnazione dello spazio per LUN	true
spaceReserve	Modalità di prenotazione dello spazio; "nessuno" (sottile) o "volume" (spesso)	none
snapshotPolicy	Criterio di snapshot da utilizzare	none

Parametro	Descrizione	Predefinito
qosPolicy	Gruppo di criteri QoS da assegnare ai volumi creati. Scegliere tra qosPolicy o adaptiveQosPolicy per ogni pool di archiviazione o backend. Per utilizzare i gruppi di policy QoS con Trident è necessario ONTAP 9.8 o versione successiva. È necessario utilizzare un gruppo di policy QoS non condiviso e assicurarsi che il gruppo di policy venga applicato individualmente a ciascun componente. Un gruppo di policy QoS condiviso impone il limite massimo per la produttività totale di tutti i carichi di lavoro.	""
adaptiveQosPolicy	Gruppo di policy QoS adattivo da assegnare ai volumi creati. Scegliere tra qosPolicy o adaptiveQosPolicy per ogni pool di archiviazione o backend. Non supportato da ontap-nas-economy.	""
snapshotReserve	Percentuale di volume riservata agli snapshot "0"	Se snapshotPolicy È none , else ""
splitOnClone	Dividere un clone dal suo genitore al momento della creazione	false
encryption	Abilita NetApp Volume Encryption (NVE) sul nuovo volume; l'impostazione predefinita è false . Per utilizzare questa opzione, NVE deve essere concesso in licenza e abilitato sul cluster. Se NAE è abilitato sul backend, qualsiasi volume fornito in Trident sarà abilitato per NAE. Per maggiori informazioni, fare riferimento a: "Come funziona Trident con NVE e NAE" .	false
luksEncryption	Abilita la crittografia LUKS. Fare riferimento a "Utilizzare Linux Unified Key Setup (LUKS)" . Solo SAN.	""
tieringPolicy	Criterio di tiering da utilizzare none	
unixPermissions	Modalità per nuovi volumi. Lasciare vuoto per i volumi SMB.	""

Parametro	Descrizione	Predefinito
securityStyle	Stile di sicurezza per i nuovi volumi. Supporti NFS mixed E unix stili di sicurezza. Supporti SMB mixed E ntfs stili di sicurezza.	L'impostazione predefinita di NFS è unix . L'impostazione predefinita di SMB è ntfs .

Prepararsi al provisioning dei volumi SMB

È possibile eseguire il provisioning dei volumi SMB utilizzando `ontap-nas` autista. Prima di completare [Integrazione dei driver ONTAP SAN e NAS](#) completare i seguenti passaggi.

Prima di iniziare

Prima di poter effettuare il provisioning dei volumi SMB utilizzando `ontap-nas` conducente, devi avere quanto segue.

- Un cluster Kubernetes con un nodo controller Linux e almeno un nodo worker Windows che esegue Windows Server 2019. Trident supporta volumi SMB montati su pod in esecuzione solo su nodi Windows.
- Almeno un segreto Trident contenente le credenziali di Active Directory. Per generare segreto `smbcreds` :

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

- Un proxy CSI configurato come servizio Windows. Per configurare un `csi-proxy`, fare riferimento a "[GitHub: Proxy CSI](#)" O "[GitHub: Proxy CSI per Windows](#)" per i nodi Kubernetes in esecuzione su Windows.

Passi

1. Crea condivisioni SMB. È possibile creare le condivisioni amministrative SMB in uno dei due modi seguenti: utilizzando "[Console di gestione Microsoft](#)" Snap-in Cartelle condivise o tramite ONTAP CLI. Per creare le condivisioni SMB utilizzando ONTAP CLI:

- a. Se necessario, creare la struttura del percorso della directory per la condivisione.

Il `vserver cifs share create` comando controlla il percorso specificato nell'opzione `-path` durante la creazione della condivisione. Se il percorso specificato non esiste, il comando fallisce.

- b. Crea una condivisione SMB associata all'SVM specificato:

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

- c. Verificare che la condivisione sia stata creata:

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



Fare riferimento a "[Crea una condivisione SMB](#)" per maggiori dettagli.

2. Durante la creazione del backend, è necessario configurare quanto segue per specificare i volumi SMB.
Per tutte le opzioni di configurazione del backend FSx for ONTAP , fare riferimento a "[Opzioni di configurazione ed esempi di FSx per ONTAP](#)" .

Parametro	Descrizione	Esempio
smbShare	È possibile specificare uno dei seguenti elementi: il nome di una condivisione SMB creata tramite Microsoft Management Console o ONTAP CLI oppure un nome che consenta a Trident di creare la condivisione SMB. Questo parametro è obbligatorio per i backend Amazon FSx for ONTAP .	smb-share
nasType	Deve essere impostato su smb . Se nullo, il valore predefinito è nfs .	smb
securityStyle	Stile di sicurezza per i nuovi volumi. Deve essere impostato su ntfs O mixed per volumi SMB .	ntfs`O `mixed per volumi SMB
unixPermissions	Modalità per nuovi volumi. Deve essere lasciato vuoto per i volumi SMB .	""

Configurare una classe di archiviazione e PVC

Configurare un oggetto StorageClass di Kubernetes e creare la classe di archiviazione per indicare a Trident come effettuare il provisioning dei volumi. Creare un PersistentVolumeClaim (PVC) che utilizzi la StorageClass Kubernetes configurata per richiedere l'accesso al PV. È quindi possibile montare il fotovoltaico su un pod.

Creare una classe di archiviazione

Configurare un oggetto StorageClass di Kubernetes

IL "[Oggetto StorageClass di Kubernetes](#)" L'oggetto identifica Trident come il provisioner utilizzato per quella classe e indica a Trident come effettuare il provisioning di un volume. Utilizzare questo esempio per configurare Storageclass per i volumi tramite NFS (fare riferimento alla sezione Attributi Trident di seguito per l'elenco completo degli attributi):

```

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

```

Utilizzare questo esempio per configurare Storageclass per i volumi che utilizzano iSCSI:

```

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

```

Per effettuare il provisioning dei volumi NFSv3 su AWS Bottlerocket, aggiungere i requisiti `mountOptions` alla classe di archiviazione:

```

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

```

Fare riferimento a "[Oggetti Kubernetes e Trident](#)" per i dettagli su come le classi di archiviazione interagiscono con `PersistentVolumeClaim` e parametri per controllare il modo in cui Trident approvvigiona i volumi.

Creare una classe di archiviazione

Passi

1. Questo è un oggetto Kubernetes, quindi usa `kubectl` per crearlo in Kubernetes.

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

2. Ora dovresti vedere una classe di archiviazione **basic-csi** sia in Kubernetes che in Trident e Trident dovrebbe aver rilevato i pool sul backend.

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

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

Creare il PVC

UN "[PersistentVolumeClaim](#)" (PVC) è una richiesta di accesso al PersistentVolume sul cluster.

Il PVC può essere configurato per richiedere una determinata dimensione di archiviazione o modalità di accesso. Utilizzando la StorageClass associata, l'amministratore del cluster può controllare molto più della dimensione e della modalità di accesso di PersistentVolume, ad esempio le prestazioni o il livello di servizio.

Dopo aver creato il PVC, è possibile montare il volume in un pod.

Esempi di manifesti

Manifesti di esempio PersistentVolumeClaim

Questi esempi mostrano le opzioni di configurazione di base del PVC.

PVC con accesso RWX

Questo esempio mostra un PVC di base con accesso RWX associato a una StorageClass denominata basic-csi .

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

PVC utilizzando l'esempio iSCSI

Questo esempio mostra un PVC di base per iSCSI con accesso RWO associato a una StorageClass denominata protection-gold .

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

Crea PVC

Passi

1. Creare il PVC.

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

2. Verificare lo stato del PVC.

```
kubectl get pvc
```

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

Fare riferimento a "[Oggetti Kubernetes e Trident](#)" per i dettagli su come le classi di archiviazione interagiscono con PersistentVolumeClaim e parametri per controllare il modo in cui Trident approvvigiona i volumi.

Attributi Trident

Questi parametri determinano quali pool di archiviazione gestiti da Trident devono essere utilizzati per fornire volumi di un determinato tipo.

Attributo	Tipo	Valori	Offerta	Richiesta	Supportato da
media ¹	corda	hdd, ibrido, ssd	Il pool contiene supporti di questo tipo; ibrido significa entrambi	Tipo di supporto specificato	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
provisioningType	corda	sottile, spesso	Il pool supporta questo metodo di provisioning	Metodo di provisioning specificato	spesso: tutto ontap; sottile: tutto ontap e solidfire-san
tipo backend	corda	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Pool appartiene a questo tipo di backend	Backend specificato	Tutti i conducenti
istantanee	bool	vero, falso	Il pool supporta volumi con snapshot	Volume con snapshot abilitati	ontap-nas, ontap-san, solidfire-san, gcp-cvs
cloni	bool	vero, falso	Il pool supporta la clonazione dei volumi	Volume con cloni abilitati	ontap-nas, ontap-san, solidfire-san, gcp-cvs

Attributo	Tipo	Valori	Offerta	Richiesta	Supportato da
crittografia	bool	vero, falso	Il pool supporta volumi crittografati	Volume con crittografia abilitata	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	interno	intero positivo	Pool è in grado di garantire IOPS in questo intervallo	Volume garantito per questi IOPS	solidfire-san

¹: Non supportato dai sistemi ONTAP Select

Distribuisci l'applicazione di esempio

Una volta creata la classe di accumulo e il PVC, è possibile montare il fotovoltaico su un pod. Questa sezione elenca il comando di esempio e la configurazione per collegare il PV a un pod.

Passi

1. Montare il volume in un pod.

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

Questi esempi mostrano le configurazioni di base per fissare il PVC a un pod: **Configurazione di base**:

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



Puoi monitorare i progressi utilizzando `kubectl get pod --watch`.

2. Verificare che il volume sia montato su `/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	

Ora puoi eliminare il Pod. L'applicazione Pod non esisterà più, ma il volume rimarrà.

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

Configurare il componente aggiuntivo Trident EKS su un cluster EKS

NetApp Trident semplifica la gestione dello storage Amazon FSx for NetApp ONTAP in Kubernetes, consentendo a sviluppatori e amministratori di concentrarsi sulla distribuzione delle applicazioni. Il componente aggiuntivo NetApp Trident EKS include le patch di sicurezza più recenti, le correzioni di bug ed è convalidato da AWS per funzionare con Amazon EKS. Il componente aggiuntivo EKS consente di garantire costantemente la sicurezza e la stabilità dei cluster Amazon EKS e di ridurre la quantità di lavoro necessaria per installare, configurare e aggiornare i componenti aggiuntivi.

Prerequisiti

Prima di configurare il componente aggiuntivo Trident per AWS EKS, assicurati di disporre di quanto segue:

- Un account cluster Amazon EKS con autorizzazioni per lavorare con i componenti aggiuntivi. Fare riferimento a "[Componenti aggiuntivi Amazon EKS](#)" .
- Autorizzazioni AWS per il marketplace AWS:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Tipo AMI: Amazon Linux 2 (AL2_x86_64) o Amazon Linux 2 Arm (AL2_ARM_64)
- Tipo di nodo: AMD o ARM
- Un file system Amazon FSx for NetApp ONTAP esistente

Passi

1. Assicurati di creare il ruolo IAM e il segreto AWS per consentire ai pod EKS di accedere alle risorse AWS. Per le istruzioni, vedere "[Crea un ruolo IAM e un segreto AWS](#)".
2. Nel cluster EKS Kubernetes, vai alla scheda **Componenti aggiuntivi**.

The screenshot shows the AWS EKS Cluster Overview page for a cluster named "tri-env-eks". At the top, there are buttons for "Delete cluster", "Upgrade version", and "View dashboard". A message at the top indicates that standard support for Kubernetes version 1.30 ends on July 28, 2025, with a link to the "pricing page". Below this, the "Cluster info" section shows the status as "Active", Kubernetes version 1.30, and a support period until July 28, 2025. The "Add-ons" tab is selected, showing a message about new versions available for one add-on. The "Add-ons (3)" section lists three items: "NetApp Trident", "AWS Lambda", and "AWS Fargate". Each item has "View details", "Edit", and "Remove" buttons, and a "Get more add-ons" button.

3. Vai su **Componenti aggiuntivi di AWS Marketplace** e scegli la categoria *archiviazione*.

The screenshot shows the AWS Marketplace add-ons search results for the category "storage". The search bar contains "Find add-on" and the filter "Any category" is set to "NetApp, Inc.". The results show one item: "NetApp Trident".

The screenshot shows the product details page for "NetApp Trident". The product is listed by "NetApp, Inc." and is categorized under "storage". It supports multiple Kubernetes versions (1.31, 1.30, 1.29, 1.28, 1.27, 1.26, 1.25, 1.24, 1.23) and starts at a certain price. There are "Standard Contract" and "View pricing details" buttons. Navigation buttons "Cancel" and "Next" are visible at the bottom.

4. Individua * NetApp Trident* e seleziona la casella di controllo per il componente aggiuntivo Trident , quindi fai clic su **Avanti**.
5. Scegli la versione desiderata del componente aggiuntivo.

Configure selected add-ons settings

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

The screenshot shows the configuration details for the NetApp Trident add-on. It includes the listed by (NetApp), category (storage), and status (Ready to install). A note indicates a subscription is active, and a link to view it is provided. The version dropdown is set to v25.6.0-eksbuild.1. There is also an optional configuration settings section. Navigation buttons at the bottom include Cancel, Previous, and Next.

Listed by	Category	Status
NetApp	storage	Ready to install

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

Version
Select the version for this add-on.
v25.6.0-eksbuild.1

Optional configuration settings

Cancel Previous Next

6. Configurare le impostazioni aggiuntive richieste.

Review and add

Step 1: Select add-ons

Edit

Selected add-ons (1)

Find add-on

< 1 >

Step 2: Configure selected add-ons settings

Edit

Selected add-ons version (1)

< 1 >

EKS Pod Identity (0)

< 1 >

Cancel Previous Create

7. Se si utilizza IRSA (ruoli IAM per l'account di servizio), fare riferimento ai passaggi di configurazione aggiuntivi "Qui".
8. Seleziona **Crea**.

9. Verificare che lo stato del componente aggiuntivo sia *Attivo*.

The screenshot shows the AWS Lambda console interface. At the top, there's a search bar with 'netapp' and several filter buttons: 'View details', 'Edit', 'Remove', 'Get more add-ons', 'Any category', 'Any status', and '1 match'. Below the search bar is a table with one row. The row details the 'NetApp Trident' add-on, which is listed under the 'NetApp' category. It has an 'Active' status, version 'v24.10.0-eksbuild.1', and no EKS Pod Identity assigned. The IAM role for service account is '(IRSA) Not set'. The 'Listed by' field shows 'NetApp, Inc.' with a link icon. A 'View subscription' button is located at the bottom right of the card.

10. Eseguire il seguente comando per verificare che Trident sia installato correttamente sul cluster:

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

11. Continuare l'installazione e configurare il backend di archiviazione. Per informazioni, vedere "[Configurare il backend di archiviazione](#)" .

Install/unistalla il componente aggiuntivo Trident EKS tramite CLI

Installare il componente aggiuntivo NetApp Trident EKS tramite CLI:

Il seguente comando di esempio installa il componente aggiuntivo Trident EKS:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.0-eksbuild.1 (con una versione dedicata)
```

Disinstallare il componente aggiuntivo NetApp Trident EKS tramite CLI:

Il seguente comando disinstalla il componente aggiuntivo Trident EKS:

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

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.