



Amazon FSx for NetApp ONTAP

Trident

NetApp
July 01, 2026

Sommario

Amazon FSx for NetApp ONTAP	1
Usa Trident con Amazon FSx for NetApp ONTAP	1
Requisiti	1
Considerazioni	1
Autenticazione	2
Amazon Machine Images (AMI) testate	2
Trova ulteriori informazioni	3
Crea un ruolo IAM e un AWS Secret	3
Crea un secret di AWS Secrets Manager	3
Crea policy IAM	4
Installare Trident	8
Installa Trident tramite helm	9
Installa Trident tramite il componente aggiuntivo EKS	11
Configurare una classe di storage	16
Crea un oggetto StorageClass	16
Effettuare il provisioning dei volumi SMB	25
Configurazione avanzata del backend ed esempi	25
Opzioni di configurazione del backend per il provisioning dei volumi	30
Configurare un PVC	32
Crea il PVC	32
Distribuisci un'applicazione	33
Distribuisci un'applicazione di esempio	33
Configura il componente aggiuntivo Trident EKS su un cluster EKS	34
Prerequisiti	35
Passaggi	35
Installa/disinstalla il componente aggiuntivo Trident EKS tramite CLI	38

Amazon FSx for NetApp ONTAP

Usa Trident con Amazon FSx for NetApp ONTAP

"Amazon FSx for NetApp ONTAP" è un servizio AWS completamente gestito che esegue file system basati sul sistema operativo per lo storage NetApp ONTAP. Fornisce funzionalità, prestazioni e amministrazione ONTAP con la scalabilità e la semplicità operativa di AWS. Un file system è la risorsa primaria in Amazon FSx ed è analogo a un cluster ONTAP on-premises. Ogni file system contiene una o più macchine virtuali di storage (SVM) e ogni SVM contiene uno o più volumi che archiviano file e directory. Questa integrazione consente ai cluster Kubernetes in esecuzione su Amazon Elastic Kubernetes Service (EKS) di eseguire il provisioning di volumi persistenti basati su ONTAP per carichi di lavoro a blocchi e file.

Requisiti

Oltre a ["Requisiti di Trident"](#), per integrare FSx for 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) che sia raggiungibile dai nodi worker del cluster.
- Nodi worker che sono preparati per ["NFS o iSCSI"](#).



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

Considerazioni

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



Se si specifica un ruolo IAM per Trident, è possibile omettere di specificare i campi `apiRegion`, `apiKey` e `secretKey` a Trident esplicitamente. Per ulteriori informazioni, fai riferimento a ["Opzioni ed esempi di configurazione di FSx per ONTAP"](#).

Utilizzo simultaneo di Trident SAN/iSCSI e del driver EBS-CSI

Se prevedi di utilizzare 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 utilizzare l' `fsxadmin` utente per il tuo file system o l' `vsadmin` utente configurato per la tua SVM.



Trident prevede di essere eseguito come `vsadmin` utente SVM o come utente con un nome diverso che abbia lo stesso ruolo. Amazon FSx for NetApp ONTAP ha un `fsxadmin` utente che è una sostituzione limitata dell'utente `admin cluster` di ONTAP. Si consiglia vivamente di utilizzare `vsadmin` con Trident.

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

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

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

Amazon Machine Images (AMI) testate

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

AMI	NAS	NAS-economy	iSCSI	iSCSI-economy
AL2023_x86_64_ST ANDARD	Sì	Sì	Sì	Sì
AL2_x86_64	Sì	Sì	Sì*	Sì*
BOTTLEROCKET_x 86_64	Sì**	Sì	N/A	N/A

AL2023_ARM_64_S TANDARD	Sì	Sì	Sì	Sì
AL2_ARM_64	Sì	Sì	Sì*	Sì*
BOTTLEROCKET_A RM_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 le AMI di cui è noto il funzionamento.

Test eseguiti con:

- EKS versione: 1.32
- Metodo di installazione: Helm 25.06 e come AWS add-On 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: Storage Class, pvc, pod
- Elimina: pod, pvc (normale, qtree/lun – economy, NAS con backup AWS)

Trova ulteriori informazioni

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

Crea un ruolo IAM e un AWS Secret

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



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

Crea un secret di AWS Secrets Manager

Poiché Trident emetterà API contro un FSx vserver per gestire lo storage per te, avrà bisogno di 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"\
  --secret-string
"{\"username\": \"vsadmin\", \"password\": \"<svmpassword>\"}"
```

Crea policy IAM

Anche Trident necessita delle autorizzazioni AWS per funzionare correttamente. Pertanto, è necessario creare una policy che dia a Trident le autorizzazioni di cui ha bisogno.

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

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

Esempio di policy JSON:

```

{
  "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 Pod Identity o ruolo IAM per l'associazione dell'account di servizio (IRSA)

È possibile configurare un account di servizio Kubernetes per assumere un ruolo AWS Identity and Access Management (IAM) con EKS Pod Identity o IAM role for Service account association (IRSA). Tutti i Pod configurati per utilizzare l'account di servizio possono quindi accedere a qualsiasi servizio AWS a cui il ruolo ha permessi di accesso.

Identità del pod

Le associazioni Amazon EKS Pod Identity consentono di gestire le credenziali per le tue applicazioni, in modo simile a come i profili delle istanze Amazon EC2 forniscono 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 ulteriori informazioni, fare riferimento a ["Configura l'agente di identità del pod Amazon EKS"](#).

Crea trust-relationship.json:

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

```
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 che è stato 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 il service account 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"  
        }  
      }  
    }  
  ]  
}
```

Aggiorna i seguenti valori nel file `trust-relationship.json`:

- **<account_id>** - ID del tuo account AWS
- **<oidc_provider>** - L'OIDC del tuo cluster EKS. Puoi ottenere l'`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 (che è stato creato nel passaggio sopra) al ruolo utilizzando questo comando:

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

Verifica che il provider OICD sia associato:

Verifica che il tuo provider OIDC sia associato al tuo cluster. Puoi verificarlo utilizzando 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 il seguente esempio per creare un ruolo IAM per 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
```

Installare 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:

- Helm
- Componente aggiuntivo EKS

Se desideri utilizzare la funzionalità di snapshot, installa il componente aggiuntivo CSI snapshot controller. Consulta ["Abilita la funzionalità snapshot per i volumi CSI"](#) per maggiori informazioni.

Installa Trident tramite helm

Identità del pod

1. Aggiungi 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 utilizzare il comando `helm list` per rivedere i dettagli dell'installazione come nome, namespace, chart, 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	deployed	trident-operator-
100.2502.0	25.02.0		

Associazione account di servizio (IRSA)

1. Aggiungi 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 utilizzare il comando `helm list` per rivedere i dettagli dell'installazione come nome, namespace, chart, 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	deployed	trident-operator-
100.2510.0	25.10.0		

Se si prevede di utilizzare iSCSI, assicurarsi che iSCSI sia abilitato sul 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 che i cluster Amazon EKS siano sicuri e stabili e di ridurre la quantità di lavoro necessaria per installare, configurare e aggiornare i componenti aggiuntivi.

Prerequisiti

Assicurati di avere quanto segue prima di configurare il componente aggiuntivo Trident per AWS EKS:

- Un account cluster Amazon EKS con abbonamento aggiuntivo
- Autorizzazioni AWS per l'AWS marketplace:
"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 per NetApp ONTAP esistente

Abilita il componente aggiuntivo Trident per AWS

Console di gestione

1. Apri la console Amazon EKS su <https://console.aws.amazon.com/eks/home#/clusters>.
2. Nel riquadro di navigazione a sinistra, seleziona **Clusters**.
3. Seleziona il nome del cluster per cui desideri configurare il componente aggiuntivo NetApp Trident CSI.
4. Seleziona **Componenti aggiuntivi** e poi seleziona **Ottieni altri componenti aggiuntivi**.
5. Seguire questi passaggi per selezionare il software add-on:
 - a. Scorri verso il basso fino alla sezione **AWS Marketplace add-ons** e digita **"Trident"** nella casella di ricerca.
 - b. Selezionare la check box nell'angolo in alto a destra della casella Trident by NetApp.
 - c. Seleziona **Next**.
6. Nella pagina delle impostazioni **Configura i componenti aggiuntivi selezionati**, eseguire le seguenti operazioni:



Salta questi passaggi se utilizzi l'associazione Pod Identity.

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

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

+

Se si seleziona **Override** per il metodo di risoluzione dei conflitti, una o più impostazioni del componente aggiuntivo esistente possono essere sovrascritte con le impostazioni dell'add-on Amazon EKS. Se non si abilita questa opzione e si verifica un conflitto con le impostazioni esistenti, l'operazione non riesce. È possibile utilizzare il messaggio di errore risultante per risolvere il conflitto. Prima di selezionare questa opzione, assicurarsi che l'add-on Amazon EKS non gestisca impostazioni che è necessario autogestire.

7. Scegli **Next**.
8. Nella pagina **Revisione e aggiunta**, scegliere **Crea**.

Al termine dell'installazione del software add-on, viene visualizzato il software add-on installato.

AWS CLI

1. Crea il add-on.json file:

Per Pod Identity, utilizzare il seguente formato:



Utilizzare il

```
{
  "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"
  }
}
```



Sostituisci <role ARN> con l'ARN del ruolo che è stato creato nel passaggio precedente.

2. Installare il Trident EKS add-on.

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

eksctl

Il seguente esempio di comando installa il Trident EKS add-on:

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

Aggiornare il software add-on 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 **Clusters**.
3. Selezionare il nome del cluster per cui si desidera aggiornare il software add-on NetApp Trident CSI.
4. Selezionare la scheda **Add-ons**.
5. Seleziona **Trident by NetApp** e poi seleziona **Modifica**.
6. Nella pagina **Configura Trident by NetApp**, procedere come segue:
 - a. Seleziona la **Version** che desideri utilizzare.
 - b. Espandi le **Impostazioni di configurazione opzionali** e modificalo secondo necessità.
 - c. Seleziona **Salva modifiche**.

AWS CLI

Il seguente esempio aggiorna l'add-on EKS:

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

eksctl

- Controlla la versione corrente del tuo software add-on FSxN Trident CSI. Sostituisci `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 software add-on alla versione riportata sotto UPDATE AVAILABLE 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 l' `--force` opzione e una qualsiasi delle impostazioni Amazon EKS add-on è in conflitto con le impostazioni esistenti, l'aggiornamento dell'Amazon EKS add-on non riesce; viene visualizzato un messaggio di errore per aiutarti a risolvere il conflitto. Prima di specificare questa opzione, assicurati che l'Amazon EKS add-on non gestisca impostazioni che devi gestire, perché tali impostazioni vengono sovrascritte con questa opzione. Per ulteriori informazioni su altre opzioni per questa impostazione, vedi ["Componenti aggiuntivi"](#). Per ulteriori informazioni sulla gestione dei campi Amazon EKS Kubernetes, vedi ["Gestione dei campi Kubernetes"](#).

Disinstallare/rimuovere il Trident EKS add-on

Hai due opzioni per rimuovere un add-on di Amazon EKS:

- **Conserva il software add-on sul tuo cluster** – Questa opzione rimuove la gestione di qualsiasi impostazione da parte di Amazon EKS. Rimuove anche la possibilità per Amazon EKS di notificarti gli aggiornamenti e di aggiornare automaticamente l'add-on Amazon EKS dopo che hai avviato un aggiornamento. Tuttavia, conserva il software add-on sul tuo cluster. Questa opzione rende l'add-on un'installazione autogestita, invece che un add-on Amazon EKS. Con questa opzione, non c'è alcun downtime per l'add-on. Mantieni l' `--preserve` opzione nel comando per conservare l'add-on.
- **Rimuovere il software add-on interamente dal cluster** – NetApp consiglia di rimuovere l'add-on Amazon EKS dal cluster solo se non ci sono risorse sul cluster che dipendono da esso. Rimuovere l'opzione `--preserve` dal comando `delete` per rimuovere l'add-on.



Se al software add-on è associato un account IAM, l'account IAM non viene rimosso.

Console di gestione

1. Apri la console Amazon EKS su <https://console.aws.amazon.com/eks/home#/clusters>.
2. Nel riquadro di navigazione sinistro, selezionare **Clusters**.
3. Selezionare il nome del cluster dal quale si desidera rimuovere il software add-on NetApp Trident CSI.
4. Selezionare la scheda **Add-ons** e poi scegliere **Trident by NetApp**.*
5. Seleziona **Rimuovi**.
6. Nella finestra di dialogo **Remove netapp_trident-operator confirmation**, procedere come segue:
 - a. Se si desidera che Amazon EKS smetta di gestire le impostazioni del software add-on, selezionare **Preserva sul cluster**. Eseguire questa operazione se si desidera conservare il software add-on sul cluster in modo da poter gestire autonomamente tutte le impostazioni del software add-on.
 - b. Immettere **netapp_trident-operator**.
 - c. Seleziona **Rimuovi**.

AWS CLI

Sostituire `my-cluster` con il nome del cluster, quindi eseguire 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 una classe di storage

Il "[Oggetto Kubernetes StorageClass](#)" identifica un provisioner e istruisce il provisioner su come effettuare il provisioning dei volumi. Questa sezione mostra come configurare un oggetto Kubernetes StorageClass che specifica Trident come provisioner.

Crea un oggetto StorageClass

Quando si crea una StorageClass per FSx for ONTAP, Trident creerà automaticamente la configurazione del backend.



Se desideri configurare manualmente il backend di storage, consulta la [\[create-a-kubernetes-storageclass-without-automatic-backend-configuration\]](#) sezione per sapere come creare separatamente il backend Trident e la storage class.

Specificare i parametri richiesti StorageClass

I seguenti tre parametri devono essere definiti durante la creazione di un StorageClass:

Parametro	Richiesto	Tipo	Descrizione
fsxFilesystemID	Sì	stringa	ID del file system FSx for NetApp ONTAP
storageDriverName	Sì	stringa	Driver di storage Trident (ad esempio, <code>ontap-nas</code> o <code>ontap-san</code>)
credentialsName	Sì	stringa	Nome del segreto Kubernetes che contiene le credenziali FSx for ONTAP

Specificare parametri facoltativi

È possibile passare parametri backend opzionali tramite la StorageClass. Definire tutti i valori opzionali come stringhe nella sezione StorageClass `parameters`. Per un elenco completo dei parametri backend, vedere: ["Configurazione del backend FSx for NetApp ONTAP"](#).

Esempi di file di configurazione StorageClass.

L'esempio seguente mostra un StorageClass che attiva la configurazione automatica del backend.

YAML

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

JSON

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

Crea il StorageClass

Una volta creato il file di configurazione, esegui il seguente comando per creare la storage class.

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

Ora dovresti vedere una classe di storage **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

Dopo aver applicato il StorageClass, Trident crea automaticamente il backend. Puoi quindi creare PersistentVolumeClaims che fanno riferimento a questo StorageClass.

Verifica lo stato della configurazione del backend

Trident registra il risultato della creazione del backend nelle annotazioni di StorageClass.

Annotazione	Descrizione
trident.netapp.io/configuratorStatus	Risultato della configurazione (Success o Failure)
trident.netapp.io/configuratorMessage	Messaggio di stato o errore dettagliato
trident.netapp.io/configuratorName	Nome della risorsa del configuratore interno
trident.netapp.io/managed	Indica che la StorageClass è gestita da Trident
trident.netapp.io/additionalStoragePools	Pool di storage creati per questo backend

Per verificare lo stato, eseguire:

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

Confermare che `trident.netapp.io/configuratorStatus` è impostato su `Success`. Se il valore è `Failure`, esaminare `trident.netapp.io/configuratorMessage` per l'errore.

Aggiungi file system FSxN aggiuntivi

Se hai bisogno di ulteriore capacità di archiviazione continuando a utilizzare lo stesso StorageClass, aggiungi ulteriori ID del file system FSxN.

Modifica la StorageClass e aggiungi la seguente annotazione:

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

Dopo aver applicato la modifica, Trident aggiorna la configurazione del backend e aggiorna le annotazioni StorageClass.

Considerazioni operative e limitazioni

- L'eliminazione di un StorageClass che ha la configurazione automatica del backend solitamente elimina il backend Trident associato. Ciò può interrompere la connettività di storage e interrompere i carichi di lavoro in esecuzione. Verifica l'impatto prima di eliminare un StorageClass gestito.
- La configurazione automatica del backend è supportata solo per AWS FSx per NetApp ONTAP.

Crea un Kubernetes StorageClass senza configurazione automatica del backend

Se desideri creare il backend Trident e la StorageClass separatamente, segui questi passaggi.

Scopri come funziona la configurazione automatica del backend

Trident deriva la configurazione del backend dalla definizione di StorageClass. Quando si applica la StorageClass, Trident convalida i parametri richiesti, crea il backend e annota la StorageClass con lo stato.

Trident crea il VolumeSnapshotClass solo una volta. Trident riutilizza lo stesso VolumeSnapshotClass per i successivi StorageClasses.

Crea il backend Trident

Per creare un backend Trident, 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, la SVM da cui ottenerlo e come autenticarsi con essa. L'esempio seguente mostra come definire uno storage basato su NAS e utilizzare un segreto AWS per memorizzare le credenziali per la 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: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"
    }
  }
}
```

Dettagli del driver FSx per ONTAP

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

Nome driver	Descrizione
ontap-san	Ogni PV di cui viene effettuato il provisioning è una LUN all'interno del proprio volume Amazon FSx for NetApp ONTAP. Consigliato per storage 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 di cui viene effettuato il provisioning è un LUN con un numero configurabile di LUN per Amazon FSx for NetApp ONTAP volume.
ontap-nas-economy	Ogni PV di cui viene effettuato il provisioning è un qtree, con un numero configurabile di qtree per Amazon FSx for NetApp ONTAP volume.
ontap-nas-flexgroup	Ogni PV fornito è un volume Amazon FSx for NetApp ONTAP FlexGroup completo.

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

Crea il backend

Dopo aver creato il file di configurazione, eseguire i seguenti comandi per creare e convalidare la Trident Backend Configuration (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
```

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

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

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

Per ulteriori informazioni su altre opzioni di configurazione, consultare la [\[Backend-advanced-configuration-and-examples\]](#) sezione seguente.

Configura una Storage Class senza configurazione automatica del backend

Di seguito sono riportati alcuni esempi di configurazioni di Storage Class da utilizzare con Trident e FSx for ONTAP.

Classe di archiviazione per NFS

È possibile utilizzare questo esempio per configurare StorageClass per 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"
```

Classe di storage per iSCSI

Utilizza questo esempio per configurare StorageClass per volumi tramite iSCSI:

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

Classe di archiviazione che utilizza NFSv3 e AWS Bottlerocket

Per eseguire il provisioning di volumi NFSv3 su AWS Bottlerocket, aggiungete il necessario `mountOptions` alla storage class:

```

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

```

Attributi di Trident StorageClass

Questi parametri determinano quali pool di storage gestiti da Trident devono essere utilizzati per effettuare il provisioning dei volumi di un determinato tipo.

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

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

¹: Non supportato da ONTAP Select o FSx for ONTAP

Fate riferimento a "[Oggetti Kubernetes e Trident](#)" per i dettagli su come le classi di storage interagiscono con PersistentVolumeClaim e sui parametri per controllare come Trident effettua il provisioning dei volumi.

Crea la classe di archiviazione

Una volta configurato il StorageClass, puoi crearlo in Kubernetes.

Passaggi

1. Si tratta di un oggetto Kubernetes, quindi usa `kubectl` per crearlo in Kubernetes.

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

2. Ora dovresti vedere una classe di storage **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
```

Effettuare il provisioning dei volumi SMB

È possibile eseguire il provisioning dei volumi SMB utilizzando il `ontap-nas` driver. Tuttavia, per farlo è necessario completare questi passaggi: "[Prepararsi al provisioning dei volumi SMB](#)".

Configurazione avanzata del backend ed esempi

Consulta la tabella seguente per le opzioni di configurazione del backend:

Parametro	Descrizione	Esempio
version		Sempre 1

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

Parametro	Descrizione	Esempio
dataLIF	<p>Indirizzo IP del protocollo LIF.</p> <p>ONTAP NAS drivers: NetApp consiglia di specificare dataLIF. Se non fornito, Trident recupera i dataLIF dall'SVM. Puoi specificare un fully-qualified domain name (FQDN) da usare per le operazioni di mount NFS, permettendoti di creare un DNS round-robin per bilanciare il carico tra più dataLIF. Può essere modificato dopo l'impostazione iniziale. ONTAP SAN drivers: non specificare per iSCSI. Trident usa ONTAP Selective LUN Map per individuare i LIF iSCSI necessari a stabilire una sessione multipath. Viene generato un avviso se dataLIF è definito esplicitamente. Può essere impostato per usare indirizzi IPv6 se hai installato Trident usando il flag IPv6. Gli indirizzi IPv6 devono essere definiti tra parentesi quadre, ad esempio [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p>	
autoExportPolicy	<p>Abilita la creazione e l'aggiornamento automatici delle policy di esportazione [Boolean]. Utilizzando le autoExportPolicy e autoExportCIDRs opzioni, Trident può gestire automaticamente le policy di esportazione.</p>	false
autoExportCIDRs	<p>Elenco di CIDR in base ai quali filtrare gli IP dei nodi Kubernetes quando autoExportPolicy è abilitato. Utilizzando le autoExportPolicy e autoExportCIDRs opzioni, Trident può gestire automaticamente le policy di esportazione.</p>	"["0.0.0.0/0", "::/0"]"
labels	<p>Set di etichette arbitrarie in formato JSON da applicare ai volumi</p>	""
clientCertificate	<p>Valore codificato in Base64 del certificato client. Utilizzato per l'autenticazione basata su certificato</p>	""

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. Facoltativo. Utilizzato per l'autenticazione basata su certificato.	""
username	Nome utente per connettersi al cluster o alla SVM. Utilizzata per l'autenticazione basata sulle credenziali. Ad esempio, vsadmin.	
password	Password per connettersi al cluster o alla SVM. Utilizzata per l'autenticazione basata sulle credenziali.	
svm	Macchina virtuale di storage da utilizzare	Derivato se viene specificato un SVM managementLIF.
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 per NetApp ONTAP. I <code>fsxadmin</code> e <code>vsadmin</code> forniti non contengono le autorizzazioni necessarie per recuperare l'utilizzo aggregato e limitarlo tramite Trident.	Non utilizzare.
limitVolumeSize	Il provisioning fallisce se la dimensione del volume richiesto supera questo valore. Limita inoltre la dimensione massima dei volumi che gestisce per qtree e LUN, e l'`qtreesPerFlexvol` opzione consente di personalizzare il numero massimo di qtree per FlexVol volume	"" (non applicato per impostazione predefinita)
lunsPerFlexvol	Numero massimo di LUN per FlexVol volume, deve essere compreso nell'intervallo [50, 200]. Solo SAN.	"100"

Parametro	Descrizione	Esempio
debugTraceFlags	Flag di debug da usare per la risoluzione dei problemi. Ad esempio, {"api":false, "method":true} non utilizzare debugTraceFlags a meno che non si stia risolvendo un problema e si richieda un dump dettagliato del log.	null
nfsMountOptions	Elenco separato da virgole delle opzioni di montaggio NFS. Le opzioni di montaggio per i volumi persistenti Kubernetes sono normalmente specificate nelle classi di storage, ma se non vengono specificate opzioni di montaggio in una classe di storage, Trident utilizzerà le opzioni di montaggio specificate nel file di configurazione del backend di storage. Se non vengono specificate opzioni di montaggio nella classe di storage o nel file di configurazione, Trident non imposterà alcuna opzione di montaggio su un volume persistente associato.	""
nasType	Configura la creazione di volumi NFS o SMB. Le opzioni sono <code>nfs</code> , <code>smb</code> o <code>null</code> . Deve essere impostato su <code>smb</code> per i volumi SMB. Impostando su <code>null</code> , vengono creati di default volumi NFS.	<code>nfs</code>
qtreesPerFlexvol	Numero massimo di <code>qtree</code> per volume FlexVol, deve essere compreso nell'intervallo [50, 300]	"200"
smbShare	È possibile specificare uno dei seguenti parametri: 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 Amazon FSx for ONTAP backends.	<code>smb-share</code>

Parametro	Descrizione	Esempio
useREST	Parametro booleano per utilizzare le API REST di ONTAP. Se impostato su <code>true</code> , Trident utilizzerà le API REST di ONTAP per comunicare con il backend. Questa funzione richiede ONTAP 9.11.1 e versioni successive. Inoltre, il ruolo di login ONTAP utilizzato deve avere accesso all'applicazione <code>ontap</code> . Questo è soddisfatto dai ruoli predefiniti <code>vsadmin</code> e <code>cluster-admin</code> .	<code>false</code>
aws	È possibile specificare quanto segue nel file di configurazione per AWS FSx for ONTAP: - <code>fsxFilesystemID</code> : Specificare l'ID del file system AWS FSx. - <code>apiRegion</code> : Nome della regione API AWS. - <code>apikey</code> : Chiave API AWS. - <code>secretKey</code> : Chiave segreta AWS.	"" "" ""
credentials	Specificare le credenziali FSx SVM da archiviare in AWS Secrets Manager. - <code>name</code> : Amazon Resource Name (ARN) del segreto, che contiene le credenziali di SVM. - <code>type</code> : Impostare su <code>awsarn</code> . Consulta "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 nella `defaults` sezione della configurazione. Per un esempio, vedere gli esempi di configurazione riportati di seguito.

Parametro	Descrizione	Predefinito
<code>spaceAllocation</code>	Allocazione dello spazio per le LUN	<code>true</code>
<code>spaceReserve</code>	Modalità di prenotazione dello spazio; "none" (thin) o "volume" (thick)	<code>none</code>
<code>snapshotPolicy</code>	policy di Snapshot da utilizzare	<code>none</code>

Parametro	Descrizione	Predefinito
qosPolicy	Gruppo di policy QoS da assegnare ai volumi creati. Scegli uno tra qosPolicy o adaptiveQosPolicy per ogni pool di storage o backend. L'utilizzo di gruppi di policy QoS con Trident richiede ONTAP 9.8 o versioni successive. È consigliabile utilizzare un gruppo di policy QoS non condiviso e assicurarsi che il gruppo di policy venga applicato a ciascun componente singolarmente. Un gruppo di policy QoS condiviso impone il limite massimo per il throughput di tutti i carichi di lavoro.	""
adaptiveQosPolicy	Gruppo di policy QoS adattivo da assegnare ai volumi creati. Scegli uno tra qosPolicy o adaptiveQosPolicy per ogni pool di storage o backend. Non supportato da ontap-nas-economy.	""
snapshotReserve	Percentuale di volume riservata per gli 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. NVE deve essere concesso in licenza e abilitato sul cluster per utilizzare questa opzione. Se NAE è abilitato sul backend, qualsiasi volume fornito in Trident sarà abilitato per NAE. Per ulteriori informazioni, fare riferimento a: "Come funziona Trident con NVE e NAE" .	false
luksEncryption	Abilita la crittografia LUKS. Consulta "Usa Linux Unified Key Setup (LUKS)" . Solo SAN.	""
tieringPolicy	Criterio di tiering da utilizzare none	
unixPermissions	Modalità per nuovi volumi. Lasciare vuoto per volumi SMB.	""
securityStyle	Stile di sicurezza per i nuovi volumi. NFS supporta mixed e unix stili di sicurezza. SMB supporta mixed e ntfs stili di sicurezza.	L'impostazione predefinita di NFS è unix. L'impostazione predefinita di SMB è ntfs.

Configurare un PVC

Questa sezione include istruzioni su come creare un PersistentVolumeClaim (PVC) che utilizza la StorageClass di Kubernetes configurata per richiedere un PV. In caso di successo, è possibile montare il PV su un pod.

Crea il PVC

Un "*PersistentVolumeClaim*" (PVC) è una richiesta di accesso al PersistentVolume sul cluster. Il PVC può essere configurato per richiedere storage di una certa dimensione o modalità di accesso. Utilizzando il StorageClass associato, l'amministratore del cluster può controllare più della sola dimensione e modalità di accesso della PersistentVolume, come ad esempio le prestazioni o il livello di servizio.

Dopo aver creato il backend Trident e la StorageClass, è possibile creare un PVC. Una volta creato il PVC, è possibile montare il volume in un pod.

Esempi di manifest

I seguenti 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 un StorageClass denominato `basic-csi`.

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

Esempio di PVC utilizzando iSCSI

Questo esempio mostra un PVC di base per iSCSI con accesso RWO che è associato a un StorageClass denominato `protection-gold`.

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

Crea PVC

Passaggi

1. Crea 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

Fate riferimento a "[Oggetti Kubernetes e Trident](#)" per i dettagli su come le classi di storage interagiscono con PersistentVolumeClaim e sui parametri per controllare come Trident effettua il provisioning dei volumi.

Distribuisce un'applicazione

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

Distribuisce un'applicazione di esempio

Passaggi

1. Monta il volume in un pod.

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

Questi esempi mostrano configurazioni di base per collegare 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 l'avanzamento usando `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
```

Configura 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 che i cluster Amazon EKS siano sicuri e stabili e di ridurre la quantità di lavoro necessaria per installare, configurare e aggiornare i componenti aggiuntivi.

Prerequisiti

Assicurati di avere quanto segue prima di configurare il componente aggiuntivo Trident per AWS EKS:

- Un account cluster Amazon EKS con autorizzazioni per utilizzare i componenti aggiuntivi. Consulta ["Componenti aggiuntivi Amazon EKS"](#).
- Autorizzazioni AWS per l'AWS marketplace:
"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 per NetApp ONTAP esistente

Passaggi

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

The screenshot shows the AWS EKS console interface for a cluster named 'tri-env-eks'. At the top right, there are buttons for 'Delete cluster', 'Upgrade version', and 'View dashboard'. Below this, a notification banner states: '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 [2].' with an 'Upgrade now' button. The main content area is titled 'Cluster info' and includes a table with the following data:

Status	Kubernetes version	Support period	Provider
Active	1.30	Standard support until July 28, 2025	EKS

Below the table, there are sections for 'Cluster health issues' and 'Upgrade insights', both showing 0 issues/insights. A navigation bar at the bottom of the cluster info section includes tabs for Overview, Resources, Compute, Networking, Add-ons (1), Access, Observability, Update history, and Tags. Below this, another notification banner says: 'New versions are available for 1 add-on.' The 'Add-ons (3)' section is active, showing a search bar with 'Find add-on', filters for 'Any category' and 'Any status', and a 'Get more add-ons' button. It indicates there are 3 matches and a page number '1'.

3. Vai su **AWS Marketplace add-ons** e scegli la categoria *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 **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. Individua **NetApp Trident** e seleziona la casella di controllo per il componente aggiuntivo Trident, quindi fai clic su **Avanti**.
5. Scegli la versione desiderata dell'add-on.

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

NetApp Trident [Remove add-on](#)

Listed by NetApp	Category storage	Status ✔ 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.

► **Optional configuration settings**

[Cancel](#) [Previous](#) [Next](#)

6. Configura le impostazioni aggiuntive richieste.

Review and add

Step 1: Select add-ons

Edit

Selected add-ons (1)

Find add-on

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

Step 2: Configure selected add-ons settings

Edit

Selected add-ons version (1)

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

EKS Pod Identity (0)

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

Cancel

Previous

Create

- Se si utilizza IRSA (IAM roles for service account), fare riferimento ai passaggi di configurazione aggiuntivi "qui".
- Seleziona **Create**.
- Verificare che lo stato del componente aggiuntivo sia *Active*.

Add-ons (1) Info

View details Edit Remove Get more add-ons

netapp

Any categ... Any status 1 match

NetApp **NetApp Trident**

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

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

Listed by [NetApp, Inc.](#)

View subscription

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

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

11. Continua la configurazione e configura il backend di storage. Per informazioni, vedi ["Configura il backend di storage"](#).

Installa/disinstalla il componente aggiuntivo Trident EKS tramite CLI

Installa il componente aggiuntivo Trident EKS di NetApp utilizzando la 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)
```

Il seguente comando di esempio installa il componente aggiuntivo Trident EKS versione 25.6.1:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.1-eksbuild.1 (con una versione dedicata)
```

Il seguente comando di esempio installa il componente aggiuntivo Trident EKS versione 25.6.2:

```
eksctl create addon --cluster clusterName --name netapp_trident-operator  
--version v25.6.2-eksbuild.1 (con una versione dedicata)
```

Disinstalla il componente aggiuntivo NetApp Trident EKS utilizzando la 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 COMMERCIALIZZABILITÀ 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.