



Amazon FSx for NetApp ONTAP

Trident

NetApp

January 15, 2026

This PDF was generated from <https://docs.netapp.com/es-es/trident-2506/trident-use/trident-fsx.html> on January 15, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Amazon FSx for NetApp ONTAP	1
Utilice Trident con Amazon FSx for NetApp ONTAP	1
Requisitos	1
Consideraciones	1
Autenticación	2
Imágenes de máquina de Amazon (AMI) probadas	3
Encuentra más información	3
Crea un rol de IAM y un secreto de AWS	3
Crear secreto de AWS Secrets Manager	4
Crear política de IAM	4
Instalar Trident	9
Instala Trident mediante Helm	9
Instala Trident mediante el complemento EKS	11
Configurar el backend de almacenamiento	16
Integración de controladores SAN y NAS de ONTAP	16
Detalles del controlador FSx para ONTAP	18
Configuración avanzada del backend y ejemplos	19
Opciones de configuración de backend para el aprovisionamiento de volúmenes	23
Preparar el aprovisionamiento de volúmenes SMB	25
Configure una clase de almacenamiento y un PVC	26
Crear una clase de almacenamiento	26
Crea el PVC	28
Atributos del Trident	30
Implementar aplicación de muestra	31
Configure el complemento Trident EKS en un clúster EKS	32
Prerrequisitos	32
Pasos	33
Instalar/desinstalar el complemento Trident EKS mediante la CLI	35

Amazon FSx for NetApp ONTAP

Utilice Trident con Amazon FSx for NetApp ONTAP

"Amazon FSx for NetApp ONTAP" Es un servicio de AWS totalmente administrado que permite a los clientes lanzar y ejecutar sistemas de archivos basados en el sistema operativo de almacenamiento NetApp ONTAP . FSx para ONTAP le permite aprovechar las características, el rendimiento y las capacidades administrativas de NetApp con las que ya está familiarizado, al tiempo que se beneficia de la simplicidad, la agilidad, la seguridad y la escalabilidad del almacenamiento de datos en AWS. FSx para ONTAP admite las funciones del sistema de archivos y las API de administración de ONTAP .

Puede integrar su sistema de archivos Amazon FSx for NetApp ONTAP con Trident para garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) puedan aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

En Amazon FSx, el sistema de archivos es el recurso principal, análogo a un clúster ONTAP local. Dentro de cada SVM puedes crear uno o varios volúmenes, que son contenedores de datos que almacenan los archivos y carpetas de tu sistema de archivos. Con Amazon FSx for NetApp ONTAP se proporcionará como un sistema de archivos administrado en la nube. El nuevo tipo de sistema de archivos se llama * NetApp ONTAP*.

Al usar Trident con Amazon FSx for NetApp ONTAP, puede garantizar que los clústeres de Kubernetes que se ejecutan en Amazon Elastic Kubernetes Service (EKS) puedan aprovisionar volúmenes persistentes de bloques y archivos respaldados por ONTAP.

Requisitos

Además de "[Requisitos de Trident](#)" Para integrar FSx para ONTAP con Trident, necesitas:

- Un clúster de Amazon EKS existente o un clúster de Kubernetes autogestionado con `kubectl` instalado.
- Una máquina virtual de almacenamiento y sistema de archivos (SVM) Amazon FSx for NetApp ONTAP existente a la que se pueda acceder desde los nodos de trabajo de su clúster.
- Nodos de trabajo que están preparados para "[NFS o iSCSI](#)" .



Asegúrese de seguir los pasos de preparación de nodos necesarios para Amazon Linux y Ubuntu. "["Imágenes de máquinas de Amazon"](#) (AMI) dependiendo de su tipo de AMI EKS.

Consideraciones

- Volúmenes SMB:
 - Los volúmenes SMB son compatibles mediante el uso de `ontap-nas` Solo el conductor.
 - Los volúmenes SMB no son compatibles con el complemento Trident EKS.
 - Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows. Referirse a "["Preparar el aprovisionamiento de volúmenes SMB"](#) Para más detalles.
- Antes de Trident 24.02, los volúmenes creados en sistemas de archivos Amazon FSx que tenían habilitadas las copias de seguridad automáticas no podían ser eliminados por Trident. Para evitar este problema en Trident 24.02 o posterior, especifique el `fsxFilesystemID` AWS `apiRegion` AWS `apiKey`

y AWS secretKey en el archivo de configuración de backend para AWS FSx para ONTAP.



Si especificas un rol de IAM para Trident, puedes omitir la especificación del apiRegion , apiKey , y secretKey campos a Trident explícitamente. Para obtener más información, consulte "[Opciones de configuración y ejemplos de FSx para ONTAP](#)" .

Uso simultáneo del controlador Trident SAN/iSCSI y EBS-CSI

Si planea usar controladores ontap-san (por ejemplo, iSCSI) con AWS (EKS, ROSA, EC2 o cualquier otra instancia), la configuración de múltiples rutas requerida en los nodos podría entrar en conflicto con el controlador CSI de Amazon Elastic Block Store (EBS). Para garantizar que las funciones de rutas múltiples funcionen sin interferir con los discos EBS en el mismo nodo, debe excluir EBS en su configuración de rutas múltiples. Este ejemplo muestra un multipath.conf Archivo que incluye la configuración necesaria de Trident excluyendo los discos EBS del multipathing:

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

Autenticación

Trident ofrece dos modos de autenticación.

- Basado en credenciales (recomendado): Almacena las credenciales de forma segura en AWS Secrets Manager. Puedes utilizar el fsxadmin usuario para su sistema de archivos o el vsadmin Usuario configurado para su SVM.



Trident espera ser gestionado como un vsadmin Usuario de SVM o como usuario con un nombre diferente que tenga el mismo rol. Amazon FSx for NetApp ONTAP tiene un fsxadmin usuario que es un reemplazo limitado del ONTAP admin Usuario del clúster. Recomendamos encarecidamente utilizar vsadmin con Trident.

- Basado en certificados: Trident se comunicará con la SVM en su sistema de archivos FSx utilizando un certificado instalado en su SVM.

Para obtener detalles sobre cómo habilitar la autenticación, consulte la autenticación correspondiente a su tipo de controlador:

- "[Autenticación NAS de ONTAP](#)"
- "[Autenticación SAN de ONTAP](#)"

Imágenes de máquina de Amazon (AMI) probadas

El clúster EKS admite varios sistemas operativos, pero AWS ha optimizado ciertas imágenes de máquina de Amazon (AMI) para contenedores y EKS. Las siguientes AMI se han probado con NetApp Trident 25.02.

IAM	NAS	Economía NAS	iSCSI	Economía iSCSI
AL2023_x86_64_ST ANDARD	Sí	Sí	Sí	Sí
AL2_x86_64	Sí	Sí	Sí*	Sí*
BOTTLEROCKET_x 86_64	Sí**	Sí	N/A	N/A
AL2023_ARM_64_S TANDARD	Sí	Sí	Sí	Sí
AL2_ARM_64	Sí	Sí	Sí*	Sí*
BOTTLEROCKET_A RM_64	Sí**	Sí	N/A	N/A

- * No se puede eliminar el PV sin reiniciar el nodo
- ** No funciona con NFSv3 con Trident versión 25.02.



Si la AMI que desea no aparece en esta lista, no significa que no sea compatible; simplemente significa que no se ha probado. Esta lista sirve de guía para las AMI que se sabe que funcionan.

Pruebas realizadas con:

- Versión de EKS: 1.32
- Método de instalación: Helm 25.06 y como complemento de AWS 25.06
- Para NAS se probaron tanto NFSv3 como NFSv4.1.
- Para SAN solo se probó iSCSI, no NVMe-oF.

Pruebas realizadas:

- Crear: Clase de almacenamiento, PVC, cápsula
- Eliminar: pod, pvc (normal, qtree/lun – económico, NAS con copia de seguridad de AWS)

Encuentra más información

- ["Documentación de Amazon FSx for NetApp ONTAP"](#)
- ["Artículo de blog sobre Amazon FSx for NetApp ONTAP"](#)

Crea un rol de IAM y un secreto de AWS

Puedes configurar los pods de Kubernetes para que accedan a los recursos de AWS autenticándose como un rol de AWS IAM en lugar de proporcionar credenciales explícitas de AWS.



Para autenticarse utilizando un rol de AWS IAM, debe tener un clúster de Kubernetes implementado utilizando EKS.

Crear secreto de AWS Secrets Manager

Dado que Trident emitirá API contra un servidor virtual FSx para administrar el almacenamiento por usted, necesitará credenciales para hacerlo. La forma segura de transmitir esas credenciales es mediante un secreto de AWS Secrets Manager. Por lo tanto, si aún no tiene uno, deberá crear un secreto de AWS Secrets Manager que contenga las credenciales de la cuenta vsadmin.

Este ejemplo crea un secreto de AWS Secrets Manager para almacenar las credenciales de Trident CSI:

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

Crear política de IAM

Trident también necesita permisos de AWS para funcionar correctamente. Por lo tanto, debe crear una política que otorgue a Trident los permisos que necesita.

Los siguientes ejemplos crean una política de IAM utilizando la CLI de AWS:

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

Ejemplo de JSON de política:

```

{
  "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"
}

```

Crear identidad de pod o rol de IAM para la asociación de cuenta de servicio (IRSA)

Puede configurar una cuenta de servicio de Kubernetes para que asuma un rol de AWS Identity and Access Management (IAM) con EKS Pod Identity o IAM role for Service account association (IRSA). Cualquier Pod que esté configurado para usar la cuenta de servicio podrá acceder a cualquier servicio de AWS al que el rol tenga permisos de acceso.

Identidad de pod

Las asociaciones de identidad de pods de Amazon EKS ofrecen la capacidad de administrar las credenciales de sus aplicaciones, de forma similar a como los perfiles de instancias de Amazon EC2 proporcionan credenciales a las instancias de Amazon EC2.

Instale Pod Identity en su clúster EKS:

Puede crear la identidad del Pod a través de la consola de AWS o utilizando el siguiente comando de la CLI de AWS:

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

Para obtener más información, consulte "[Configurar el agente de identidad de pod de Amazon EKS](#)" .

Crear trust-relationship.json:

Cree el archivo trust-relationship.json para permitir que la entidad de servicio de EKS asuma este rol para la identidad del pod. A continuación, cree un rol con esta política de confianza:

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

archivo trust-relationship.json:

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

Adjunte la política de rol al rol de IAM:

Asocie la política de rol del paso anterior al rol de IAM que se creó:

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

Crear una asociación de identidad de pod:

Cree una asociación de identidad de pod entre el rol de IAM y la cuenta de servicio de 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
```

Rol de IAM para la asociación de cuentas de servicio (IRSA)

Utilizando la CLI de AWS:

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

Archivo 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"
        }
      }
    }
  ]
}

```

Actualiza los siguientes valores en el `trust-relationship.json` archivo:

- **<account_id>** - Tu ID de cuenta de AWS
- **<oidc_provider>** - El OIDC de su clúster EKS. Puede obtener el proveedor oidc ejecutando:

```

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

```

Asocia el rol de IAM con la política de IAM:

Una vez creado el rol, adjúntele la política (creada en el paso anterior) mediante este comando:

```

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

```

Verificar que el proveedor de OICD esté asociado:

Verifique que su proveedor OIDC esté asociado con su clúster. Puedes verificarlo usando este comando:

```

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

```

Si la salida está vacía, utilice el siguiente comando para asociar IAM OIDC a su clúster:

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

Si utiliza **eksctl**, siga el siguiente ejemplo para crear un rol de IAM para la cuenta de servicio en 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
```

Instalar Trident

Trident simplifica la gestión del almacenamiento de Amazon FSx for NetApp ONTAP en Kubernetes para que sus desarrolladores y administradores puedan centrarse en el despliegue de aplicaciones.

Puedes instalar Trident utilizando uno de los siguientes métodos:

- Timón
- Complemento EKS

Si desea utilizar la funcionalidad de instantáneas, instale el complemento CSI snapshot controller. Referirse a "[Habilitar la funcionalidad de instantáneas para volúmenes CSI](#)" Para más información.

Instala Trident mediante Helm.

Identidad de pod

1. Añadir el repositorio Trident Helm:

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

2. Instala Trident siguiendo el siguiente ejemplo:

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

Puedes utilizar el `helm list` comando para revisar los detalles de la instalación, como nombre, espacio de nombres, gráfico, estado, versión de la aplicación y número de revisión.

```
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

Asociación de cuentas de servicio (IRSA)

1. Añadir el repositorio Trident Helm:

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

2. Establezca los valores para **proveedor de nube e identidad de nube**:

```
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
```

Puedes utilizar el `helm list` comando para revisar los detalles de la instalación, como nombre, espacio de nombres, gráfico, estado, versión de la aplicación y número de revisión.

```
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-100.2506.0
		25.06.0	

Si planea utilizar iSCSI, asegúrese de que iSCSI esté habilitado en su máquina cliente. Si utiliza el sistema operativo del nodo de trabajo AL2023, puede automatizar la instalación del cliente iSCSI agregando el parámetro `node prep` en la instalación de helm:

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

Instala Trident mediante el complemento EKS.

El complemento Trident EKS incluye los últimos parches de seguridad, correcciones de errores y está validado por AWS para funcionar con Amazon EKS. El complemento EKS le permite garantizar de forma consistente que sus clústeres de Amazon EKS sean seguros y estables, y reduce la cantidad de trabajo que necesita realizar para instalar, configurar y actualizar complementos.

Prerrequisitos

Asegúrese de tener lo siguiente antes de configurar el complemento Trident para AWS EKS:

- Una cuenta de clúster de Amazon EKS con suscripción adicional
- Permisos de AWS para el mercado de AWS:
`"aws-marketplace:ViewSubscriptions",`
`"aws-marketplace:Subscribe",`
`"aws-marketplace:Unsubscribe"`
- Tipo de AMI: Amazon Linux 2 (AL2_x86_64) o Amazon Linux 2 Arm (AL2_ARM_64)
- Tipo de nodo: AMD o ARM
- Un sistema de archivos Amazon FSx for NetApp ONTAP existente

Habilita el complemento Trident para AWS

Consola de administración

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters> .
2. En el panel de navegación izquierdo, seleccione **Clústeres**.
3. Seleccione el nombre del clúster para el que desea configurar el complemento NetApp Trident CSI.
4. Seleccione **Complementos** y luego seleccione **Obtener más complementos**.
5. Siga estos pasos para seleccionar el complemento:
 - a. Desplácese hacia abajo hasta la sección **Complementos de AWS Marketplace** y escriba **"Trident"** en el cuadro de búsqueda.
 - b. Seleccione la casilla de verificación en la esquina superior derecha del cuadro Trident by NetApp
 - c. Seleccione **Siguiente**.
6. En la página de configuración **Configurar complementos seleccionados**, haga lo siguiente:



Omite estos pasos si estás usando la asociación de identidad de pod.

- a. Seleccione la **Versión** que desea utilizar.
- b. Si utiliza la autenticación IRSA, asegúrese de configurar los valores disponibles en la configuración opcional:
 - Seleccione la **Versión** que desea utilizar.
 - Siga el **Esquema de configuración del complemento** y configure el parámetro **configurationValues** en la sección **Valores de configuración** con el ARN del rol que creó en el paso anterior (el valor debe tener el siguiente formato):

```
{
```

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

```
}
```

+

Si selecciona Anular como método de resolución de conflictos, una o más de las configuraciones del complemento existente pueden sobrescribirse con la configuración del complemento de Amazon EKS. Si no habilita esta opción y hay un conflicto con su configuración existente, la operación fallará. Puede utilizar el mensaje de error resultante para solucionar el conflicto. Antes de seleccionar esta opción, asegúrese de que el complemento Amazon EKS no gestione configuraciones que usted deba administrar manualmente.

7. Seleccione **Siguiente**.
8. En la página **Revisar y agregar**, seleccione **Crear**.

Una vez finalizada la instalación del complemento, verá el complemento instalado.

CLI de AWS

1. Crea el add-on.json archivo:

Para la identidad del pod, utilice el siguiente formato:

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

Para la autenticación IRSA, utilice el siguiente 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"  
  }  
}
```



Reemplazar <role ARN> con el ARN del rol que se creó en el paso anterior.

2. Instala el complemento Trident EKS.

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

eksctl

El siguiente comando de ejemplo instala el complemento Trident EKS:

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

Actualizar el complemento Trident EKS

Consola de administración

1. Abra la consola de Amazon EKS <https://console.aws.amazon.com/eks/home#/clusters> .
2. En el panel de navegación izquierdo, seleccione **Clústeres**.
3. Seleccione el nombre del clúster para el que desea actualizar el complemento NetApp Trident CSI.
4. Seleccione la pestaña **Complementos**.
5. Seleccione * Trident by NetApp* y luego seleccione **Editar**.
6. En la página **Configurar Trident de NetApp**, haga lo siguiente:
 - a. Seleccione la **Versión** que desea utilizar.
 - b. Amplíe la sección **Ajustes de configuración opcionales** y modifíquela según sea necesario.
 - c. Seleccione **Guardar cambios**.

CLI de AWS

El siguiente ejemplo actualiza el complemento 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

- Comprueba la versión actual de tu complemento FSxN Trident CSI. Reemplazar `my-cluster` con el nombre de su clúster.

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

Ejemplo de salida:

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'"}		

- Actualiza el complemento a la versión que se muestra en **ACTUALIZACIÓN DISPONIBLE** en el resultado del paso anterior.

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

Si eliminas el `--force` Si alguna de las opciones y alguna de las configuraciones del complemento de Amazon EKS entra en conflicto con su configuración existente, la actualización del complemento de Amazon EKS fallará; recibirá un mensaje de error para ayudarle a resolver el conflicto. Antes de especificar esta opción, asegúrese de que el complemento Amazon EKS no gestione configuraciones que usted necesite administrar, ya que estas configuraciones se sobrescriben con esta opción. Para obtener más información sobre otras opciones para esta configuración, consulte "[Complementos](#)" . Para obtener más información sobre la administración de campos de Amazon EKS Kubernetes, consulte "[Gestión de campos de Kubernetes](#)" .

Desinstala/elimina el complemento Trident EKS.

Tienes dos opciones para eliminar un complemento de Amazon EKS:

- **Conservar el software complementario en su clúster** – Esta opción elimina la administración de Amazon EKS de cualquier configuración. También elimina la capacidad de Amazon EKS para notificarte sobre actualizaciones y actualizar automáticamente el complemento de Amazon EKS después de que usted inicie una actualización. Sin embargo, conserva el software adicional en su clúster. Esta opción convierte el complemento en una instalación autogestionada, en lugar de un complemento de Amazon EKS. Con esta opción, no hay tiempo de inactividad para el complemento. Conservar el `--preserve` opción en el comando para conservar el complemento.
- **Elimine por completo el software complementario de su clúster** – NetApp recomienda que elimine el complemento Amazon EKS de su clúster solo si no hay recursos en su clúster que dependan de él. Quitar el `--preserve` opción de la `delete` comando para eliminar el complemento.



Si el complemento tiene una cuenta IAM asociada, dicha cuenta no se eliminará.

Consola de administración

1. Abra la consola de Amazon EKS en <https://console.aws.amazon.com/eks/home#/clusters> .
2. En el panel de navegación izquierdo, seleccione **Clústeres**.
3. Seleccione el nombre del clúster para el que desea eliminar el complemento NetApp Trident CSI.
4. Seleccione la pestaña **Complementos** y luego seleccione * Trident de NetApp*.
5. Seleccione **Eliminar**.
6. En el cuadro de diálogo **Eliminar confirmación de netapp_trident-operator**, haga lo siguiente:
 - a. Si desea que Amazon EKS deje de administrar la configuración del complemento, seleccione **Conservar en el clúster**. Haz esto si quieras conservar el software adicional en tu clúster para poder gestionar tú mismo todas las configuraciones del complemento.
 - b. Introduzca **netapp_trident-operator**.
 - c. Seleccione **Eliminar**.

CLI de AWS

Reemplazar `my-cluster` con el nombre de su clúster y, a continuación, ejecute el siguiente comando.

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

eksctl

El siguiente comando desinstala el complemento Trident EKS:

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

Configurar el backend de almacenamiento

Integración de controladores SAN y NAS de ONTAP

Para crear un backend de almacenamiento, necesitas crear un archivo de configuración en formato JSON o YAML. El archivo debe especificar el tipo de almacenamiento que desea (NAS o SAN), el sistema de archivos, la SVM de la que se obtendrá y cómo autenticarse con ella. El siguiente ejemplo muestra cómo definir el almacenamiento basado en NAS y cómo usar un secreto de AWS para almacenar las credenciales de la SVM que desea usar:

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"
    }
  }
}
```

Ejecute los siguientes comandos para crear y validar la configuración del backend de Trident (TBC):

- Crea la configuración del backend de Trident (TBC) a partir del archivo YAML y ejecuta el siguiente comando:

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

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

- Validar que la configuración del backend de Trident (TBC) se creó correctamente:

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

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

Detalles del controlador FSx para ONTAP

Puede integrar Trident con Amazon FSx for NetApp ONTAP utilizando los siguientes controladores:

- `ontap-san` Cada PV aprovisionado es un LUN dentro de su propio volumen Amazon FSx for NetApp ONTAP . Recomendado para almacenamiento en bloque.
- `ontap-nas` Cada PV aprovisionado es un volumen completo de Amazon FSx for NetApp ONTAP . Recomendado para NFS y SMB.
- `ontap-san-economy` Cada PV aprovisionado es un LUN con un número configurable de LUN por volumen de Amazon FSx for NetApp ONTAP .
- `ontap-nas-economy` Cada PV aprovisionado es un qtree, con un número configurable de qtrees por volumen de Amazon FSx for NetApp ONTAP .
- `ontap-nas-flexgroup` Cada PV aprovisionado es un volumen completo de Amazon FSx for NetApp ONTAP FlexGroup .

Para obtener detalles sobre el conductor, consulte "[Controladores NAS](#)" y "[Controladores SAN](#)" .

Una vez creado el archivo de configuración, ejecute este comando para crearlo en su EKS:

```
kubectl create -f configuration_file
```

Para verificar el estado, ejecute este 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

Configuración avanzada del backend y ejemplos

Consulte la siguiente tabla para ver las opciones de configuración del backend:

Parámetro	Descripción	Ejemplo
version		Siempre 1
storageDriverName	Nombre del controlador de almacenamiento	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, ontap-san-economy
backendName	Nombre personalizado o el backend de almacenamiento	Nombre del controlador + "_" + dataLIF
managementLIF	Dirección IP de un clúster o LIF de administración de SVM. Se puede especificar un nombre de dominio completo (FQDN). Se puede configurar para usar direcciones IPv6 si Trident se instaló usando la bandera IPv6. Las direcciones IPv6 deben definirse entre corchetes, como por ejemplo [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. Si usted proporciona el fsxFilesystemID bajo el aws campo, no es necesario que proporcione el managementLIF porque Trident recupera la SVM managementLIF información de AWS. Por lo tanto, debe proporcionar las credenciales de un usuario en la SVM (por ejemplo: vsadmin) y el usuario debe tener vsadmin role.	"10.0.0.1", "[2001:1234:abcd::fefe]"

Parámetro	Descripción	Ejemplo
dataLIF	<p>Dirección IP del protocolo LIF. *</p> <p>Controladores NAS ONTAP : NetApp recomienda especificar dataLIF. Si no se proporcionan, Trident obtiene los dataLIF del SVM. Puede especificar un nombre de dominio completo (FQDN) para usarlo en las operaciones de montaje NFS, lo que le permite crear un DNS round-robin para equilibrar la carga en múltiples dataLIF.</p> <p>Puede modificarse después de la configuración inicial. Referirse a . * Controladores ONTAP SAN:</p> <p>No especificar para iSCSI. Trident utiliza ONTAP Selective LUN Map para descubrir los LIF iSCI necesarios para establecer una sesión de múltiples rutas. Se genera una advertencia si dataLIF se define explícitamente. Se puede configurar para usar direcciones IPv6 si Trident se instaló usando la bandera IPv6. Las direcciones IPv6 deben definirse entre corchetes, como por ejemplo [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p>	
autoExportPolicy	Habilitar la creación y actualización automática de políticas de exportación [Booleano]. Utilizando el autoExportPolicy y autoExportCIDRs Con algunas opciones, Trident puede gestionar las políticas de exportación automáticamente.	false
autoExportCIDRs	<p>Lista de CIDR para filtrar las direcciones IP de los nodos de Kubernetes cuando autoExportPolicy está habilitado. Utilizando el autoExportPolicy y autoExportCIDRs Con algunas opciones, Trident puede gestionar las políticas de exportación automáticamente.</p>	["0.0.0.0/0", "::/0"]
labels	Conjunto de etiquetas arbitrarias con formato JSON para aplicar a los volúmenes	""

Parámetro	Descripción	Ejemplo
clientCertificate	Valor codificado en Base64 del certificado del cliente. Se utiliza para la autenticación basada en certificados.	""
clientPrivateKey	Valor codificado en Base64 de la clave privada del cliente. Se utiliza para la autenticación basada en certificados.	""
trustedCACertificate	Valor codificado en Base64 del certificado de CA de confianza. Opcional. Se utiliza para la autenticación basada en certificados.	""
username	Nombre de usuario para conectarse al clúster o SVM. Se utiliza para la autenticación basada en credenciales. Por ejemplo, vsadmin.	
password	Contraseña para conectarse al clúster o SVM. Se utiliza para la autenticación basada en credenciales.	
svm	máquina virtual de almacenamiento a utilizar	Se deriva si se especifica un SVM managementLIF.
storagePrefix	Prefijo utilizado al aprovisionar nuevos volúmenes en la SVM. No se puede modificar después de su creación. Para actualizar este parámetro, deberá crear un nuevo backend.	trident
limitAggregateUsage	No especificar para Amazon FSx for NetApp ONTAP. El proporcionado fsxadmin y vsadmin No contienen los permisos necesarios para recuperar el uso agregado y limitarlo mediante Trident.	No utilizar.
limitVolumeSize	Fallará el aprovisionamiento si el tamaño de volumen solicitado supera este valor. También restringe el tamaño máximo de los volúmenes que administra para qtrees y LUN, y el qtreesPerFlexvol Esta opción permite personalizar el número máximo de qtrees por FlexVol volume.	" (no se aplica por defecto)

Parámetro	Descripción	Ejemplo
lunsPerFlexvol	El número máximo de LUN por volumen de Flexvol debe estar en el rango [50, 200]. Solo SAN.	"100"
debugTraceFlags	Indicadores de depuración para usar al solucionar problemas. Ejemplo: {"api":false, "method":true} No usar debugTraceFlags a menos que esté solucionando problemas y necesite un registro detallado.	nulo
nfsMountOptions	Lista de opciones de montaje NFS separadas por comas. Las opciones de montaje para volúmenes persistentes de Kubernetes normalmente se especifican en las clases de almacenamiento, pero si no se especifican opciones de montaje en una clase de almacenamiento, Trident recurrirá a las opciones de montaje especificadas en el archivo de configuración del backend de almacenamiento. Si no se especifican opciones de montaje en la clase de almacenamiento o en el archivo de configuración, Trident no establecerá ninguna opción de montaje en un volumen persistente asociado.	""
nasType	Configure la creación de volúmenes NFS o SMB. Las opciones son nfs , smb , o nulo. Debe configurarse en smb para volúmenes SMB. Si se establece en nulo, se utilizarán volúmenes NFS por defecto.	nfs
qtreesPerFlexvol	Número máximo de Qtrees por FlexVol volume, debe estar en el rango [50, 300]	"200"
smbShare	Puede especificar una de las siguientes opciones: el nombre de un recurso compartido SMB creado mediante la Consola de administración de Microsoft o la CLI de ONTAP , o un nombre para permitir que Trident cree el recurso compartido SMB. Este parámetro es necesario para los backends de Amazon FSx para ONTAP .	smb-share

Parámetro	Descripción	Ejemplo
useREST	Parámetro booleano para utilizar las API REST de ONTAP. Cuando se configura para true Trident utilizará las API REST de ONTAP para comunicarse con el backend. Esta función requiere ONTAP 9.11.1 y versiones posteriores. Además, el rol de inicio de sesión de ONTAP utilizado debe tener acceso a <code>ontap</code> solicitud. Esto se satisface mediante lo predefinido. <code>vsadmin</code> y <code>cluster-admin</code> roles.	false
aws	En el archivo de configuración de AWS FSx para ONTAP puede especificar lo siguiente: <code>fsxFilesystemID</code> : Especifique el ID del sistema de archivos AWS FSx. - <code>apiRegion</code> Nombre de la región de la API de AWS. - <code>apikey</code> Clave de API de AWS. - <code>secretKey</code> Clave secreta de AWS.	"" "" ""
credentials	Especifique las credenciales de FSx SVM que se almacenarán en AWS Secrets Manager. - <code>name</code> : Nombre de recurso de Amazon (ARN) del secreto, que contiene las credenciales de SVM. - <code>type</code> : Configurado a <code>awsarn</code> . Referirse a " Crea un secreto de AWS Secrets Manager " Para más información.	

Opciones de configuración de backend para el aprovisionamiento de volúmenes

Puedes controlar el aprovisionamiento predeterminado utilizando estas opciones en el `defaults` sección de la configuración. Para ver un ejemplo, consulte los ejemplos de configuración a continuación.

Parámetro	Descripción	Por defecto
<code>spaceAllocation</code>	Asignación de espacio para LUN	true
<code>spaceReserve</code>	Modo de reserva de espacio: "ninguno" (delgado) o "volumen" (grueso).	none
<code>snapshotPolicy</code>	Política de instantáneas a utilizar	none

Parámetro	Descripción	Por defecto
qosPolicy	Grupo de políticas QoS que se asignará a los volúmenes creados. Elija una de las opciones qosPolicy o adaptiveQosPolicy por grupo de almacenamiento o backend. El uso de grupos de políticas QoS con Trident requiere ONTAP 9.8 o posterior. Debe utilizar un grupo de políticas QoS no compartido y asegurarse de que el grupo de políticas se aplique a cada componente individualmente. Un grupo de políticas QoS compartidas impone un límite máximo al rendimiento total de todas las cargas de trabajo.	""
adaptiveQosPolicy	Grupo de políticas QoS adaptativas para asignar a los volúmenes creados. Elija una de las opciones qosPolicy o adaptiveQosPolicy por grupo de almacenamiento o backend. No compatible con ontap-nas-economy.	""
snapshotReserve	Porcentaje de volumen reservado para instantáneas "0"	Si snapshotPolicy es none , else ""
splitOnClone	Separar un clon de su progenitor al crearlo	false
encryption	Habilite el cifrado de volumen de NetApp (NVE) en el nuevo volumen; el valor predeterminado es false . Para utilizar esta opción, NVE debe estar licenciado y habilitado en el clúster. Si NAE está habilitado en el backend, cualquier volumen aprovisionado en Trident tendrá NAE habilitado. Para obtener más información, consulte: " Cómo funciona Trident con NVE y NAE " .	false
luksEncryption	Habilitar el cifrado LUKS. Referirse a " Utilice la configuración de clave unificada de Linux (LUKS) ." . Solo SAN.	""
tieringPolicy	Política de niveles a utilizar none	
unixPermissions	Modo para nuevos volúmenes. Dejar en blanco para volúmenes SMB.	""

Parámetro	Descripción	Por defecto
securityStyle	Estilo de seguridad para nuevos volúmenes. NFS admite mixed y unix Estilos de seguridad. Las PYMES son compatibles con el soporte. mixed y ntfs Estilos de seguridad.	El valor predeterminado de NFS es unix . El valor predeterminado de SMB es ntfs .

Preparar el aprovisionamiento de volúmenes SMB

Puede aprovisionar volúmenes SMB utilizando `ontap-nas` conductor. Antes de completar [Integración de controladores SAN y NAS de ONTAP](#) Complete los siguientes pasos.

Antes de empezar

Antes de poder aprovisionar volúmenes SMB utilizando el `ontap-nas` Conductor, usted debe tener lo siguiente.

- Un clúster de Kubernetes con un nodo controlador Linux y al menos un nodo de trabajo Windows que ejecuta Windows Server 2019. Trident solo admite volúmenes SMB montados en pods que se ejecutan en nodos Windows.
- Al menos un secreto de Trident que contenga sus credenciales de Active Directory. Para generar secretos `smbcreds` :

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

- Un proxy CSI configurado como servicio de Windows. Para configurar un `csi-proxy` , consulte a ["GitHub: Proxy CSI"](#) o ["GitHub: Proxy CSI para Windows"](#) para nodos de Kubernetes que se ejecutan en Windows.

Pasos

1. Crear recursos compartidos SMB. Puedes crear los recursos compartidos de administración SMB de dos maneras: utilizando... ["Consola de administración de Microsoft"](#) Complemento de carpetas compartidas o mediante la CLI de ONTAP . Para crear los recursos compartidos SMB mediante la CLI de ONTAP :

- a. Si es necesario, cree la estructura de rutas de directorio para el recurso compartido.

El `vserver cifs share create` El comando verifica la ruta especificada en la opción `-path` durante la creación del recurso compartido. Si la ruta especificada no existe, el comando falla.

- b. Cree un recurso compartido SMB asociado con la SVM especificada:

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

- c. Verifique que se haya creado el recurso compartido:

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



Referirse a "[Crear un recurso compartido SMB](#)" Para más detalles.

2. Al crear el backend, debe configurar lo siguiente para especificar los volúmenes SMB. Para conocer todas las opciones de configuración del backend de FSx para ONTAP , consulte "["Opciones de configuración y ejemplos de FSx para ONTAP"](#)" .

Parámetro	Descripción	Ejemplo
smbShare	Puede especificar una de las siguientes opciones: el nombre de un recurso compartido SMB creado mediante la Consola de administración de Microsoft o la CLI de ONTAP , o un nombre para permitir que Trident cree el recurso compartido SMB. Este parámetro es necesario para los backends de Amazon FSx para ONTAP .	smb-share
nasType	Debe configurarse en smb . Si es nulo, el valor predeterminado es nfs .	smb
securityStyle	Estilo de seguridad para nuevos volúmenes. Debe configurarse en ntfs o mixed para volúmenes SMB.	ntfs`o `mixed para volúmenes SMB
unixPermissions	Modo para nuevos volúmenes. Debe dejarse vacío para volúmenes SMB.	""

Configure una clase de almacenamiento y un PVC

Configure un objeto StorageClass de Kubernetes y cree la clase de almacenamiento para indicar a Trident cómo aprovisionar volúmenes. Cree un PersistentVolumeClaim (PVC) que utilice la StorageClass de Kubernetes configurada para solicitar acceso al PV. Luego puedes montar el panel fotovoltaico en un soporte.

Crear una clase de almacenamiento

Configurar un objeto StorageClass de Kubernetes

El "["Objeto StorageClass de Kubernetes"](#)" El objeto identifica a Trident como el proveedor que se utiliza para esa clase e indica a Trident cómo aprovisionar un volumen. Utilice este ejemplo para configurar Storageclass para volúmenes que utilizan NFS (consulte la sección Atributos de Trident a continuación para obtener la lista completa de atributos):

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

Utilice este ejemplo para configurar Storageclass para volúmenes que utilizan 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"
```

Para aprovisionar volúmenes NFSv3 en AWS Bottlerocket, agregue los necesarios. `mountOptions` a la clase de almacenamiento:

```
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
```

Referirse a "[Objetos de Kubernetes y Trident](#)" Para obtener detalles sobre cómo interactúan las clases de almacenamiento con `PersistentVolumeClaim` y parámetros para controlar cómo Trident gestiona los volúmenes.

Crear una clase de almacenamiento

Pasos

- Este es un objeto de Kubernetes, así que use `kubectl` para crearlo en Kubernetes.

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

- Ahora debería ver una clase de almacenamiento **basic-csi** tanto en Kubernetes como en Trident, y Trident debería haber detectado los pools en el backend.

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

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

Crea el PVC

A "[Reclamación de volumen persistente](#)" (PVC) es una solicitud de acceso al PersistentVolume en el clúster.

El PVC se puede configurar para solicitar el almacenamiento de un tamaño o modo de acceso determinado. Mediante la StorageClass asociada, el administrador del clúster puede controlar más que el tamaño del PersistentVolume y el modo de acceso, como el rendimiento o el nivel de servicio.

Una vez creado el PVC, puede montar el volumen en un soporte.

Ejemplos de manifiestos

Muestra de PersistentVolumeClaim

Estos ejemplos muestran opciones básicas de configuración de PVC.

PVC con acceso RWX

Este ejemplo muestra un PVC básico con acceso RWX que está asociado a una StorageClass llamada basic-csi .

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

Ejemplo de PVC usando iSCSI

Este ejemplo muestra un PVC básico para iSCSI con acceso RWO que está asociado con una StorageClass llamada protection-gold .

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

Crear PVC

Pasos

1. Crear el PVC.

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

2. Verifique el estado del PVC.

```
kubectl get pvc
```

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

Referirse a "["Objetos de Kubernetes y Trident"](#)" Para obtener detalles sobre cómo interactúan las clases de almacenamiento con PersistentVolumeClaim y parámetros para controlar cómo Trident gestiona los volúmenes.

Atributos del Trident

Estos parámetros determinan qué pools de almacenamiento gestionados por Trident deben utilizarse para aprovisionar volúmenes de un tipo determinado.

Atributo	Tipo	Valores	Oferta	Pedido	Con el apoyo de
medios ¹	cadena	disco duro, híbrido, SSD	La piscina contiene medios de este tipo; híbrido significa ambos	Tipo de medio especificado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san
tipo de aprovisionamiento	cadena	delgado, grueso	Pool admite este método de aprovisionamiento.	Método de aprovisionamiento especificado	Espeso: todo Ontap; fino: todo Ontap y Solidfire-san
Tipo de backend	cadena	ontap-nas, ontap-nas-economy, ontap-nas-flexgroup, ontap-san, solidfire-san, gcp-cvs, azure-netapp-files, ontap-san-economy	Pool pertenece a este tipo de backend.	Backend especificado	Todos los conductores
instantáneas	bool	verdadero, falso	El pool admite volúmenes con instantáneas.	Volumen con instantáneas habilitadas	ontap-nas, ontap-san, solidfire-san, gcp-cvs
clones	bool	verdadero, falso	Pool admite la clonación de volúmenes.	Volumen con clones habilitado	ontap-nas, ontap-san, solidfire-san, gcp-cvs

Atributo	Tipo	Valores	Oferta	Pedido	Con el apoyo de
cifrado	bool	verdadero, falso	Pool admite volúmenes cifrados	Volumen con cifrado habilitado	ontap-nas, ontap-nas-economy, ontap-nas-flexgroups, ontap-san
IOPS	int	entero positivo	Pool es capaz de garantizar IOPS en este rango.	El volumen garantizaba estas IOPS	solidfire-san

¹: No compatible con los sistemas ONTAP Select

Implementar aplicación de muestra

Una vez creadas la clase de almacenamiento y el PVC, puede montar el PV en un pod. Esta sección enumera el comando de ejemplo y la configuración para adjuntar el PV a un pod.

Pasos

1. Monte el volumen en una cápsula.

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

Estos ejemplos muestran configuraciones básicas para conectar el PVC a un pod: **Configuración básica**:

```
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
```



Puedes supervisar el progreso usando `kubectl get pod --watch`.

2. Verifique que el volumen esté montado en `/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	

Ahora puedes eliminar el Pod. La aplicación Pod dejará de existir, pero el volumen se mantendrá.

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

Configure el complemento Trident EKS en un clúster EKS.

NetApp Trident simplifica la gestión del almacenamiento de Amazon FSx for NetApp ONTAP en Kubernetes para que sus desarrolladores y administradores puedan centrarse en el despliegue de aplicaciones. El complemento NetApp Trident EKS incluye los últimos parches de seguridad, correcciones de errores y está validado por AWS para funcionar con Amazon EKS. El complemento EKS le permite garantizar de forma consistente que sus clústeres de Amazon EKS sean seguros y estables, y reduce la cantidad de trabajo que necesita realizar para instalar, configurar y actualizar complementos.

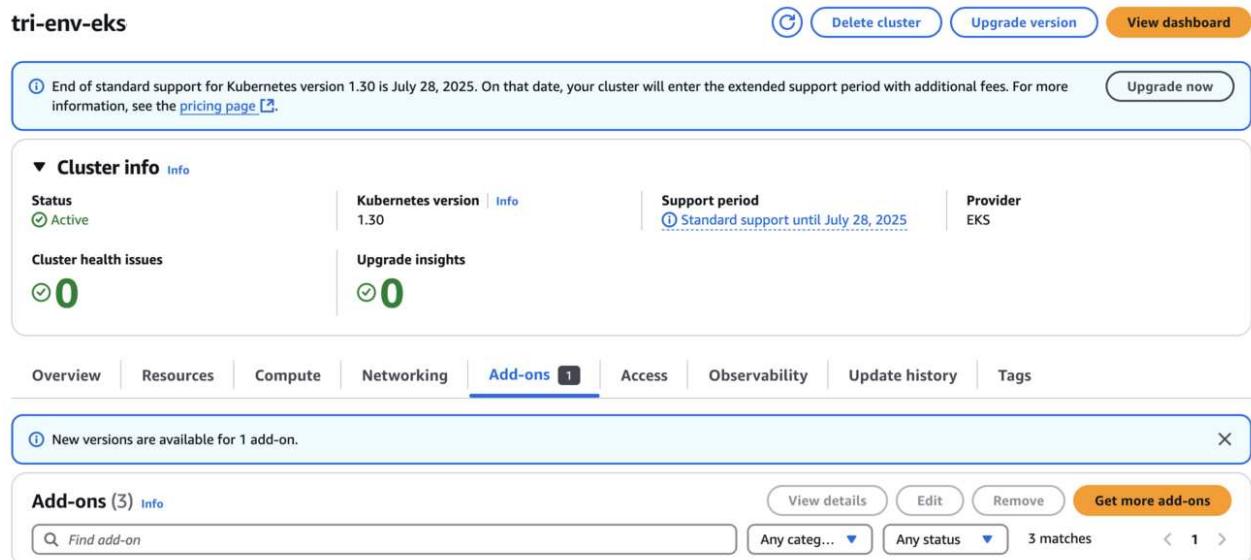
Prerrequisitos

Asegúrese de tener lo siguiente antes de configurar el complemento Trident para AWS EKS:

- Una cuenta de clúster de Amazon EKS con permisos para trabajar con complementos. Referirse a ["Complementos de Amazon EKS"](#) .
- Permisos de AWS para el mercado de AWS:
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe"
- Tipo de AMI: Amazon Linux 2 (AL2_x86_64) o Amazon Linux 2 Arm (AL2_ARM_64)
- Tipo de nodo: AMD o ARM
- Un sistema de archivos Amazon FSx for NetApp ONTAP existente

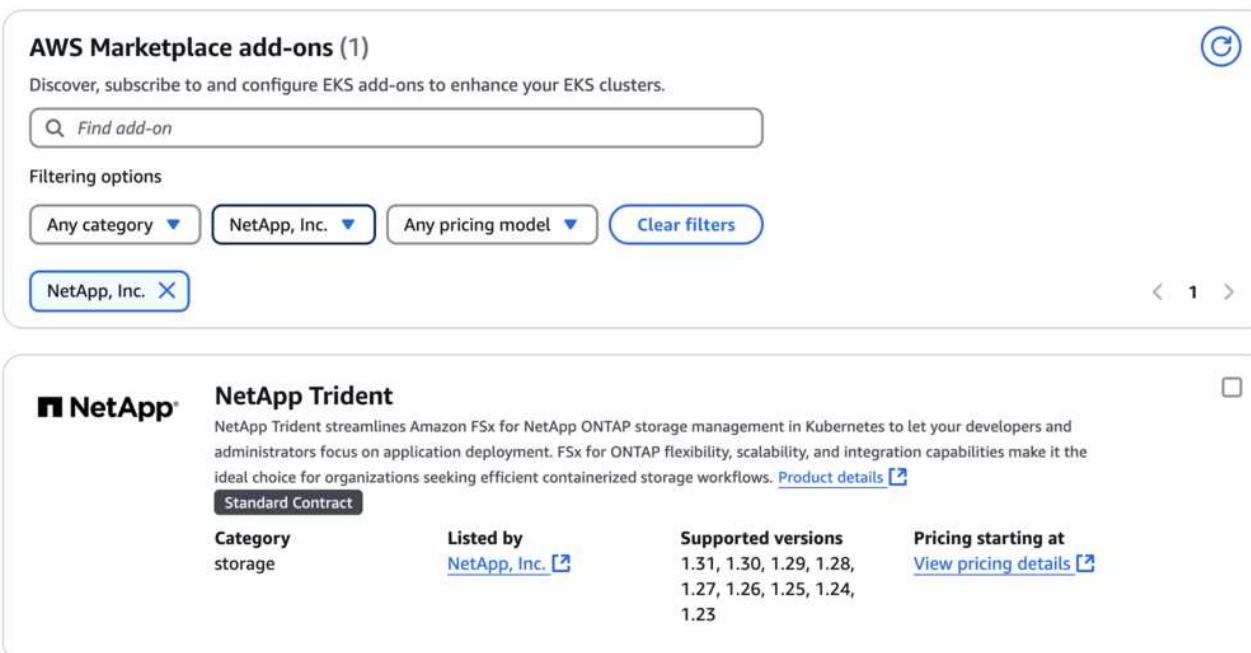
Pasos

1. Asegúrese de crear un rol de IAM y un secreto de AWS para permitir que los pods de EKS accedan a los recursos de AWS. Para obtener instrucciones, consulte "[Crea un rol de IAM y un secreto de AWS](#)".
2. En su clúster de Kubernetes EKS, vaya a la pestaña **Complementos**.



The screenshot shows the AWS EKS Cluster Overview page for a cluster named "tri-env-eks". The "Add-ons" tab is selected. A message at the top indicates "New versions are available for 1 add-on." The "Add-ons (3)" section shows three available add-ons: "NetApp Trident", "AWS EBS Provisioner", and "AWS EFS Provisioner". Each item has "View details", "Edit", and "Remove" buttons. A "Get more add-ons" button is also present. The "Add-ons" tab has a count of 1, and there are 3 matches.

3. Vaya a **Complementos de AWS Marketplace** y elija la categoría *almacenamiento*.



The screenshot shows the AWS Marketplace add-ons search results for the "storage" category. The search term "NetApp, Inc." is entered. The results list "NetApp Trident" by NetApp, Inc. The product description states: "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." The "Product details" button is highlighted. The "Standard Contract" button is also visible. The "Next" button is located at the bottom right of the page.

4. Localice * NetApp Trident* y seleccione la casilla de verificación del complemento Trident , y haga clic en **Siguiente**.
5. Elige la versión deseada del complemento.

Configure selected add-ons settings

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

NetApp Trident

Listed by **NetApp**

Category storage

Status Ready to install

You're subscribed to this software

View subscription

Version

Select the version for this add-on.

v25.6.0-eksbuild.1

Optional configuration settings

Cancel Previous Next

6. Configure los ajustes complementarios necesarios.

Review and add

Step 1: Select add-ons

Edit

Selected add-ons (1)

Find add-on

< 1 >

Add-on name	Type	Status
-------------	------	--------

netapp_trident-operator	storage	Ready to install
-------------------------	---------	------------------

Step 2: Configure selected add-ons settings

Edit

Selected add-ons version (1)

< 1 >

Add-on name	Version	IAM role for service account (IRSA)
-------------	---------	-------------------------------------

netapp_trident-operator	v24.10.0-eksbuild.1	Not set
-------------------------	---------------------	---------

EKS Pod Identity (0)

< 1 >

Add-on name	IAM role	Service account
-------------	----------	-----------------

No Pod Identity associations

None of the selected add-on(s) have Pod Identity associations.

Cancel

Previous

Create

7. Si utiliza IRSA (roles de IAM para cuentas de servicio), consulte los pasos de configuración adicionales ["aquí"](#).

8. Seleccione **Crear**.

9. Verifique que el estado del complemento sea *Activo*.

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

10. Ejecute el siguiente comando para verificar que Trident esté correctamente instalado en el clúster:

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

11. Continúe con la configuración y configure el backend de almacenamiento. Para obtener más información, consulte "[Configurar el backend de almacenamiento](#)" .

Instalar/desinstalar el complemento Trident EKS mediante la CLI

Instale el complemento NetApp Trident EKS mediante la CLI:

El siguiente comando de ejemplo instala el complemento Trident EKS:

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

Desinstale el complemento NetApp Trident EKS mediante la CLI:

El siguiente comando desinstala el complemento Trident EKS:

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

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.