Instalar Trident Protect

Trident

NetApp
February 05, 2026

Tabla de contenidos

Instalar Trident Protect . . . 1
- Requisitos de Trident Protect . . . 1
  - Compatibilidad del clúster Kubernetes de Trident Protect . . . 1
  - Compatibilidad del backend de almacenamiento Trident Protect . . . 1
  - Requisitos para volúmenes de economía nas . . . 2
  - Protección de datos con máquinas virtuales de KubeVirt . . . 2
  - Requisitos para la replicación de SnapMirror . . . 3
- Instalar y configurar Trident Protect . . . 4
  - Instalar Trident Protect . . . 4
  - Especificar los límites de recursos del contenedor Trident Protect . . . 8
- Instalar el complemento CLI de Trident Protect . . . 9
  - Instalar el complemento CLI de Trident Protect . . . 9
  - Consulte la ayuda del complemento de la CLI de Trident . . . 11
  - Habilite el autocompletado de comandos . . . 11

Instalar Trident Protect

Requisitos de Trident Protect

Comience por verificar que su entorno operativo, clústeres de aplicaciones, aplicaciones y licencias estén listos. Asegúrese de que su entorno cumpla con estos requisitos para implementar y operar Trident Protect.

Compatibilidad del clúster Kubernetes de Trident Protect

Trident Protect es compatible con una amplia gama de ofertas de Kubernetes totalmente administradas y autoadministradas, que incluyen:

- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Microsoft Azure Kubernetes Service (AKS)
- Red Hat OpenShift
- SUSE Rancher
- Cartera de VMware Tanzania
- Subida de Kubernetes

> Asegúrese de que el clúster en el que instala Trident Protect esté configurado con un controlador de instantáneas en ejecución y los CRD relacionados. Para instalar un controlador de instantáneas, consulte "estas instrucciones" .

Compatibilidad del backend de almacenamiento Trident Protect

Trident Protect admite los siguientes backends de almacenamiento:

- Amazon FSX para ONTAP de NetApp
- Cloud Volumes ONTAP
- Cabinas de almacenamiento ONTAP de NetApp
- NetApp Volumes para Google Cloud
- Azure NetApp Files

Asegúrese de que el back-end de almacenamiento cumple los siguientes requisitos:

- Compruebe que el almacenamiento de NetApp conectado al clúster utilice Astra Trident 24,02 o una versión posterior (se recomienda Trident 24,10).
  - Si Astra Trident es anterior a la versión 24.06.1 y tienes pensado utilizar la funcionalidad de recuperación ante desastres de NetApp SnapMirror, debe habilitar manualmente el aprovisionador de Astra Control.
- Asegúrese de tener el aprovisionador de control de Astra más reciente (instalado y habilitado de forma predeterminada a partir de Astra Trident 24.06.1).
- Asegúrese de tener un back-end de almacenamiento NetApp ONTAP.

- Asegúrese de haber configurado un depósito de almacenamiento de objetos para almacenar backups.
- Cree los espacios de nombres de aplicación que planee utilizar para las aplicaciones o las operaciones de administración de datos de las aplicaciones. Trident Protect no crea estos espacios de nombres por usted; si especifica un espacio de nombres inexistente en un recurso personalizado, la operación fallará.

Requisitos para volúmenes de economía nas

Trident Protect admite operaciones de copia de seguridad y restauración en volúmenes nas-economy. Actualmente no se admiten instantáneas, clones ni replicación SnapMirror a volúmenes nas-economy. Debe habilitar un directorio de instantáneas para cada volumen nas-economy que planea usar con Trident Protect.

Algunas aplicaciones no son compatibles con volúmenes que usan un directorio Snapshot. Para estas aplicaciones, debe ocultar el directorio Snapshot mediante la ejecución del siguiente comando en el sistema de almacenamiento de ONTAP:

```
nfs modify -vserver <svm> -v3-hide-snapshot enabled
```

Para habilitar el directorio snapshot, ejecute el siguiente comando para cada volumen nas-económico, sustituyéndolo `<volume-UUID>` por el UUID del volumen que desea cambiar:

```
tridentctl update volume <volume-UUID> --snapshot-dir=true --pool-level
=true -n trident
```

Es posible habilitar los directorios de snapshots de forma predeterminada para volúmenes nuevos si se configura la opción Trident backend configuration `snapshotDir` en `true`. Los volúmenes existentes no se ven afectados.

Protección de datos con máquinas virtuales de KubeVirt

Trident Protect 24.10 y 24.10.1 y versiones más recientes tienen un comportamiento diferente cuando protege aplicaciones que se ejecutan en máquinas virtuales de KubeVirt. En ambas versiones, puede habilitar o deshabilitar la congelación y descongelación del sistema de archivos durante las operaciones de protección de datos.

Para todas las versiones de Trident Protect, para habilitar o deshabilitar la funcionalidad de congelamiento automático en entornos OpenShift, es posible que deba otorgar permisos privilegiados al espacio de nombres de la aplicación. Por ejemplo:

```
oc adm policy add-scc-to-user privileged -z default -n
<application-namespace>
```

Trident Protect 24.10

Trident Protect 24.10 no garantiza automáticamente un estado consistente para los sistemas de archivos de VM KubeVirt durante las operaciones de protección de datos. Si desea proteger los datos de su máquina virtual KubeVirt con Trident Protect 24.10, debe habilitar manualmente la funcionalidad de congelamiento/descongelamiento de los sistemas de archivos antes de la operación de protección de datos.

Esto garantiza que los sistemas de archivos se encuentren en un estado consistente.

Puede configurar Trident Protect 24.10 para administrar la congelación y descongelación del sistema de archivos de la máquina virtual durante las operaciones de protección de datos."configurar la virtualización" y luego usando el siguiente comando:

```
kubectl set env deployment/trident-protect-controller-manager
NEPTUNE_VM_FREEZE=true -n trident-protect
```

Trident Protect 24.10.1 y posteriores

A partir de Trident Protect 24.10.1, Trident Protect congela y descongela automáticamente los sistemas de archivos KubeVirt durante las operaciones de protección de datos. Opcionalmente, puedes desactivar este comportamiento automático usando el siguiente comando:

```
kubectl set env deployment/trident-protect-controller-manager
NEPTUNE_VM_FREEZE=false -n trident-protect
```

Requisitos para la replicación de SnapMirror

NetApp SnapMirror está disponible para su uso con Trident Protect para las siguientes soluciones ONTAP :

- ASA de NetApp
- AFF de NetApp
- FAS de NetApp
- ONTAP Select de NetApp
- Cloud Volumes ONTAP de NetApp
- Amazon FSX para ONTAP de NetApp

Requisitos de clústeres de ONTAP para la replicación de SnapMirror

Asegúrese de que el clúster de ONTAP cumple los siguientes requisitos si tiene pensado utilizar la replicación de SnapMirror:

- * Astra Control Provisioner o Trident*: Astra Control Provisioner o Trident debe existir tanto en los clústeres de Kubernetes de origen como de destino que utilizan ONTAP como back-end. Trident Protect admite la replicación con la tecnología NetApp SnapMirror utilizando clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`
  - `ontap-san`
- **Licencias**: Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben estar habilitadas en los clústeres de ONTAP de origen y de destino. Consulte "Información general sobre las licencias de SnapMirror en ONTAP" si desea obtener más información.

Consideraciones sobre la relación de paridad para la replicación de SnapMirror

Compruebe que el entorno cumple los siguientes requisitos si piensa utilizar la paridad de back-end de

almacenamiento:

- **Cluster y SVM**: Los back-ends de almacenamiento ONTAP deben ser peered. Consulte "Información general sobre relaciones entre iguales de clústeres y SVM" si desea obtener más información.

  Compruebe que los nombres de las SVM utilizados en la relación de replicación entre dos clústeres de ONTAP sean únicos.

- **Trident y SVM**: Las SVM remotas entre iguales deben estar disponibles para el aprovisionador de control de Astra o Trident en el clúster de destino.
- **Backends administrados**: debe agregar y administrar backends de almacenamiento ONTAP en Trident Protect para crear una relación de replicación.
- **NVMe sobre TCP**: Trident Protect no admite la replicación de NetApp SnapMirror para backends de almacenamiento que utilizan el protocolo NVMe sobre TCP.

Configuración de Trident/ONTAP para la replicación de SnapMirror

Trident Protect requiere que configure al menos un backend de almacenamiento que admita la replicación para los clústeres de origen y destino. Si los clústeres de origen y destino son los mismos, la aplicación de destino debería utilizar un backend de almacenamiento diferente al de la aplicación de origen para lograr la mejor resiliencia.

Instalar y configurar Trident Protect

Si su entorno cumple con los requisitos de Trident Protect, puede seguir estos pasos para instalar Trident Protect en su clúster. Puede obtener Trident Protect de NetApp o instalarlo desde su propio registro privado. Instalar desde un registro privado resulta útil si su clúster no puede acceder a Internet.

De forma predeterminada, Trident Protect recopila información de soporte que ayuda con cualquier caso de soporte de NetApp que pueda abrir, incluidos registros, métricas e información de topología sobre clústeres y aplicaciones administradas. Trident Protect envía estos paquetes de soporte a NetApp según una programación diaria. Opcionalmente, puede deshabilitar esta recopilación de paquetes de soporte cuando instale Trident Protect. Puedes hacerlo manualmente"generar un bundle de soporte" en cualquier momento.

Instalar Trident Protect

Instalar Trident Protect de NetApp

Pasos

1. Añada el repositorio Helm de Trident:

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

2. Instalar los CRD Trident Protect:

```
helm install trident-protect-crds netapp-trident-protect/trident-
protect-crds --version 100.2410.1 --create-namespace --namespace
trident-protect
```

3. Utilice Helm para instalar Trident Protect usando uno de los siguientes comandos. Reemplazar `<name_of_cluster>` con un nombre de clúster, que se asignará al clúster y se utilizará para identificar las copias de seguridad y las instantáneas del clúster:
   - Instale Trident Protect normalmente:

```
helm install trident-protect netapp-trident-protect/trident-
protect --set clusterName=<name_of_cluster> --version 100.2410.1
--create-namespace --namespace trident-protect
```

   - Instale Trident Protect y deshabilite las cargas programadas diarias del paquete de soporte de AutoSupport de Trident Protect:

```
helm install trident-protect netapp-trident-protect/trident-
protect --set autoSupport.enabled=false --set
clusterName=<name_of_cluster> --version 100.2410.1 --create
-namespace --namespace trident-protect
```

Instalar Trident Protect desde un registro privado

Puede instalar Trident Protect desde un registro de imágenes privado si su clúster de Kubernetes no puede acceder a Internet. En estos ejemplos, sustituya los valores entre corchetes por información de su entorno:

Pasos

1. Tire de las siguientes imágenes a su máquina local, actualice las etiquetas y, a continuación, empújelas en su registro privado:

```
netapp/controller:24.10.1
netapp/restic:24.10.1
netapp/kopia:24.10.1
netapp/trident-autosupport:24.10.0
netapp/exechook:24.10.1
netapp/resourcebackup:24.10.1
netapp/resourcerestore:24.10.1
netapp/resourcedelete:24.10.1
bitnami/kubectl:1.30.2
kubebuilder/kube-rbac-proxy:v0.16.0
```

Por ejemplo:

```
docker pull netapp/controller:24.10.1
```

```
docker tag netapp/controller:24.10.1 <private-registry-
url>/controller:24.10.1
```

```
docker push <private-registry-url>/controller:24.10.1
```

2. Cree el espacio de nombres del sistema Trident Protect:

```
kubectl create ns trident-protect
```

3. Inicie sesión en el Registro:

```
helm registry login <private-registry-url> -u <account-id> -p <api-
token>
```

4. Cree un secreto de extracción para utilizarlo en la autenticación del registro privado:

```
kubectl create secret docker-registry regcred --docker
-username=<registry-username> --docker-password=<api-token> -n
trident-protect --docker-server=<private-registry-url>
```

5. Añada el repositorio Helm de Trident:

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

6. Crea un archivo llamado `protectValues.yaml` . Asegúrese de que contenga las siguientes configuraciones de Trident Protect:

```
---
image:
  registry: <private-registry-url>
imagePullSecrets:
  - name: regcred
controller:
  image:
    registry: <private-registry-url>
rbacProxy:
  image:
    registry: <private-registry-url>
crCleanup:
  imagePullSecrets:
    - name: regcred
webhooksCleanup:
  imagePullSecrets:
    - name: regcred
```

7. Instalar los CRD Trident Protect:

```
helm install trident-protect-crds netapp-trident-protect/trident-
protect-crds --version 100.2410.1 --create-namespace --namespace
trident-protect
```

8. Utilice Helm para instalar Trident Protect usando uno de los siguientes comandos. Reemplazar `<name_of_cluster>` con un nombre de clúster, que se asignará al clúster y se utilizará para identificar las copias de seguridad y las instantáneas del clúster:
   - Instale Trident Protect normalmente:

```
helm install trident-protect netapp-trident-protect/trident-
protect --set clusterName=<name_of_cluster> --version 100.2410.1
--create-namespace --namespace trident-protect -f
protectValues.yaml
```

   - Instale Trident Protect y deshabilite las cargas programadas diarias del paquete de soporte de AutoSupport de Trident Protect:

```
helm install trident-protect netapp-trident-protect/trident-
protect --set autoSupport.enabled=false --set
clusterName=<name_of_cluster> --version 100.2410.1 --create
-namespace --namespace trident-protect -f protectValues.yaml
```

Especificar los límites de recursos del contenedor Trident Protect

Puede utilizar un archivo de configuración para especificar límites de recursos para los contenedores de Trident Protect después de instalar Trident Protect. Establecer límites de recursos le permite controlar qué cantidad de recursos del clúster consumen las operaciones de Trident Protect.

Pasos

1. Crear un archivo llamado `resourceLimits.yaml`.
2. Complete el archivo con opciones de límite de recursos para los contenedores de Trident Protect según las necesidades de su entorno.

   El siguiente archivo de configuración de ejemplo muestra la configuración disponible y contiene los vaules predeterminados para cada límite de recursos:

```
---
jobResources:
  defaults:
    limits:
      cpu: 8000m
      memory: 10000Mi
      ephemeralStorage: ""
    requests:
      cpu: 100m
      memory: 100Mi
      ephemeralStorage: ""
  resticVolumeBackup:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
  resticVolumeRestore:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
```

```
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
  kopiaVolumeBackup:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
  kopiaVolumeRestore:
    limits:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
    requests:
      cpu: ""
      memory: ""
      ephemeralStorage: ""
```

3. Aplique los valores del `resourceLimits.yaml` archivo:

```
helm upgrade trident-protect -n trident-protect -f <resourceLimits.yaml>
--reuse-values
```

Instalar el complemento CLI de Trident Protect

Puede utilizar el complemento de línea de comandos Trident Protect, que es una extensión de Trident `tridentctl` utilidad para crear e interactuar con recursos personalizados (CR) de Trident Protect.

Instalar el complemento CLI de Trident Protect

Antes de utilizar la utilidad de línea de comandos, debe instalarla en la máquina que utiliza para acceder al clúster. Siga estos pasos, dependiendo de si su máquina utiliza una CPU x64 o ARM.

Descargar plugin para CPU Linux AMD64

Pasos

1. Descargue el complemento CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-linux-amd64
```

Descargar plugin para CPU Linux ARM64

Pasos

1. Descargue el complemento CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-linux-arm64
```

Descargar plugin para CPU Mac AMD64

Pasos

1. Descargue el complemento CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-macos-amd64
```

Descargar plugin para CPU Mac ARM64

Pasos

1. Descargue el complemento CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/24.10.1/tridentctl-protect-macos-arm64
```

1. Active los permisos de ejecución para el binario del plugin:

```
chmod +x tridentctl-protect
```

2. Copie el binario del plugin a una ubicación definida en su variable PATH. Por ejemplo, `/usr/bin` o `/usr/local/bin` (puede que necesite Privileges elevado):

```
cp ./tridentctl-protect /usr/local/bin/
```

3. Opcionalmente, puede copiar el binario del plugin a una ubicación en su directorio principal. En este caso, se recomienda asegurarse de que la ubicación forma parte de la variable PATH:

```
cp ./tridentctl-protect ~/bin/
```

Copiar el plugin a una ubicación en su variable PATH le permite usar el plugin escribiendo `tridentctl-protect` o `tridentctl protect` desde cualquier ubicación.

Consulte la ayuda del complemento de la CLI de Trident

Puede utilizar las funciones de ayuda del plugin incorporado para obtener ayuda detallada sobre las capacidades del plugin:

Pasos

1. Utilice la función de ayuda para ver la guía de uso:

```
tridentctl-protect help
```

Habilite el autocompletado de comandos

Después de haber instalado el complemento CLI de Trident Protect, puede habilitar el autocompletado para ciertos comandos.

Active la finalización automática del shell Bash

Pasos

1. Descargue el script de finalización:

```
curl -L -O https://github.com/NetApp/tridentctl-
protect/releases/download/24.10.1/tridentctl-completion.bash
```

2. Cree un nuevo directorio en el directorio principal para que contenga el script:

```
mkdir -p ~/.bash/completions
```

3. Mueva el script descargado al `~/.bash/completions` directorio:

```
mv tridentctl-completion.bash ~/.bash/completions/
```

4. Añada la siguiente línea al `~/.bashrc` archivo en su directorio principal:

```
source ~/.bash/completions/tridentctl-completion.bash
```

Active la finalización automática del shell Z

Pasos

1. Descargue el script de finalización:

```
curl -L -O https://github.com/NetApp/tridentctl-
protect/releases/download/24.10.1/tridentctl-completion.zsh
```

2. Cree un nuevo directorio en el directorio principal para que contenga el script:

```
mkdir -p ~/.zsh/completions
```

3. Mueva el script descargado al `~/.zsh/completions` directorio:

```
mv tridentctl-completion.zsh ~/.zsh/completions/
```

4. Añada la siguiente línea al `~/.zprofile` archivo en su directorio principal:

```
source ~/.zsh/completions/tridentctl-completion.zsh
```

Resultado

En su próximo inicio de sesión en el shell, puede utilizar el comando auto-completado con el plugin tridentctl-Protect.

Información de copyright

Información de la marca comercial