Instalar Trident Protect

Trident

NetApp
January 15, 2026

Tabla de contenidos

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:

- Servicio Amazon Elastic Kubernetes (EKS)
- Motor Google Kubernetes (GKE)
- Servicio de Kubernetes de Microsoft Azure (AKS)
- Red Hat OpenShift
- SUSE Rancher
- Cartera de VMware Tanzu
- Kubernetes ascendente

- Las copias de seguridad de Trident Protect solo se admiten en nodos de cómputo de Linux. Los nodos de cómputo de Windows no son compatibles con operaciones de copia de seguridad.
- 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 for NetApp ONTAP
- Cloud Volumes ONTAP
- matrices de almacenamiento ONTAP
- Google Cloud NetApp Volumes
- Azure NetApp Files

Asegúrese de que su sistema de almacenamiento cumpla con los siguientes requisitos:

- Asegúrese de que el almacenamiento NetApp conectado al clúster utilice Trident 24.02 o posterior (se recomienda Trident 24.10).
- Asegúrese de tener un backend de almacenamiento NetApp ONTAP .
- Asegúrese de haber configurado un bucket de almacenamiento de objetos para almacenar las copias de seguridad.

- 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 nas-economy

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 utilizan un directorio de instantáneas. Para estas aplicaciones, debe ocultar el directorio de instantáneas ejecutando el siguiente comando en el sistema de almacenamiento ONTAP :

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

Puede habilitar el directorio de instantáneas ejecutando el siguiente comando para cada volumen nas-economy, reemplazando `<volume-UUID>` con el UUID del volumen que desea cambiar:

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

Puede habilitar los directorios de instantáneas de forma predeterminada para los nuevos volúmenes configurando la opción de configuración del backend de Trident. `snapshotDir` a `true` . Los volúmenes existentes no se ven afectados.

Protección de datos con máquinas virtuales 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.

Durante las operaciones de restauración, cualquier `VirtualMachineSnapshots` Los archivos creados para una máquina virtual (VM) no se restauran.

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."configuración de 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 de KubeVirt durante las operaciones de protección de datos. Opcionalmente, puede desactivar este comportamiento automático mediante el siguiente comando:

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

Requisitos para la replicación de SnapMirror

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

- Clústeres NetApp FAS, AFF y ASA locales
- Selección de NetApp ONTAP Select
- Volúmenes en la nube de NetApp Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP

Requisitos del clúster ONTAP para la replicación SnapMirror

Asegúrese de que su clúster ONTAP cumpla con los siguientes requisitos si planea utilizar la replicación SnapMirror :

- * NetApp Trident*: NetApp Trident debe existir tanto en el clúster de Kubernetes de origen como en el de destino que utilizan ONTAP como backend. Trident Protect admite la replicación con la tecnología NetApp SnapMirror utilizando clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`NFS
  - `ontap-san`iSCSI
  - `ontap-san`: FC
  - `ontap-san`: NVMe/TCP (requiere como mínimo la versión 9.15.1 de ONTAP)
- **Licencias**: Las licencias asíncronas de ONTAP SnapMirror que utilizan el paquete de protección de datos deben estar habilitadas tanto en el clúster ONTAP de origen como en el de destino. Referirse a "Información general sobre licencias de SnapMirror en ONTAP" Para más información.

  A partir de ONTAP 9.10.1, todas las licencias se entregan como un archivo de licencia de NetApp (NLF), que es un único archivo que habilita múltiples funciones. Referirse a"Licencias incluidas con ONTAP One" Para más información.

  Solo se admite la protección asíncrona de SnapMirror .

Consideraciones de interconexión para la replicación de SnapMirror

Asegúrese de que su entorno cumpla los siguientes requisitos si planea utilizar el emparejamiento de backend de almacenamiento:

- **Clúster y SVM**: Los backends de almacenamiento ONTAP deben estar interconectados. Referirse a "Descripción general del emparejamiento de clústeres y SVM" Para más información.

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

- * NetApp Trident y SVM*: Las SVM remotas emparejadas deben estar disponibles para NetApp 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.

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.

Requisitos del clúster de Kubernetes para la replicación de SnapMirror

Asegúrese de que sus clústeres de Kubernetes cumplan los siguientes requisitos:

- **Accesibilidad a AppVault**: Tanto el clúster de origen como el de destino deben tener acceso a la red para leer y escribir en AppVault para la replicación de objetos de la aplicación.
- **Conectividad de red**: Configure las reglas del firewall, los permisos de los buckets y las listas blancas de IP para habilitar la comunicación entre ambos clústeres y AppVault a través de las WAN.

> Muchos entornos empresariales implementan políticas de firewall estrictas en las conexiones WAN. Verifique estos requisitos de red con su equipo de infraestructura antes de configurar la replicación.

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.

Instalar Trident Protect

Instalar Trident Protect de NetApp

Pasos

1. Añadir el repositorio Trident Helm:

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

2. Utilice Helm para instalar Trident Protect. 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:

```
helm install trident-protect netapp-trident-protect/trident-protect
--set clusterName=<name-of-cluster> --version 100.2506.0 --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. Descarga las siguientes imágenes a tu máquina local, actualiza las etiquetas y luego súbelas a tu registro privado:

```
netapp/controller:25.06.0
netapp/restic:25.06.0
netapp/kopia:25.06.0
netapp/trident-autosupport:25.06.0
netapp/exechook:25.06.0
netapp/resourcebackup:25.06.0
netapp/resourcerestore:25.06.0
netapp/resourcedelete:25.06.0
bitnami/kubectl:1.30.2
kubebuilder/kube-rbac-proxy:v0.16.0
```

   Por ejemplo:

```
docker pull netapp/controller:25.06.0
```

```
docker tag netapp/controller:25.06.0 <private-registry-
url>/controller:25.06.0
```

```
docker push <private-registry-url>/controller:25.06.0
```

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

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

3. Iniciar sesión en el registro:

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

4. Crea un secreto de extracción para usar 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. Añadir el repositorio Trident Helm:

```
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. Utilice Helm para instalar Trident Protect. 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:

```
helm install trident-protect netapp-trident-protect/trident-protect
--set clusterName=<name_of_cluster> --version 100.2506.0 --create
-namespace --namespace trident-protect -f protectValues.yaml
```

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 a su clúster. Siga estos pasos, dependiendo de si su máquina utiliza una CPU x64 o ARM .

Descargar complemento para procesadores Linux AMD64

Pasos

1. Descargue el complemento CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.06.0/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/25.06.0/tridentctl-protect-linux-arm64
```

Descargar plugin para procesadores Mac AMD64

Pasos

1. Descargue el complemento CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.06.0/tridentctl-protect-macos-amd64
```

Descargar plugin para procesadores Mac ARM64

Pasos

1. Descargue el complemento CLI de Trident Protect:

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.06.0/tridentctl-protect-macos-arm64
```

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

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

2. Copie el archivo binario del plugin a una ubicación que esté definida en su variable PATH. Por ejemplo, `/usr/bin` o `/usr/local/bin` (Es posible que necesites privilegios elevados):

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

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

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

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

Consulta la ayuda del plugin Trident CLI.

Puedes utilizar las funciones de ayuda integradas del plugin para obtener ayuda detallada sobre sus capacidades:

Pasos

1. Utilice la función de ayuda para ver las instrucciones de uso:

```
tridentctl-protect help
```

Habilitar la autocompletación de comandos

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

Habilitar la autocompletación para el shell de Bash

Pasos

1. Descarga el script de finalización:

```
curl -L -O https://github.com/NetApp/tridentctl-
protect/releases/download/25.06.0/tridentctl-completion.bash
```

2. Crea un nuevo directorio en tu directorio personal para contener el script:

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

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

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

4. Agrega la siguiente línea a la `~/.bashrc` archivo en tu directorio de inicio:

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

Habilitar la autocompletación para la shell Z

Pasos

1. Descarga el script de finalización:

```
curl -L -O https://github.com/NetApp/tridentctl-
protect/releases/download/25.06.0/tridentctl-completion.zsh
```

2. Crea un nuevo directorio en tu directorio personal para contener el script:

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

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

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

4. Agrega la siguiente línea a la `~/.zprofile` archivo en tu directorio de inicio:

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

Resultado

En su próximo inicio de sesión en la shell, puede usar la autocompletación de comandos con el complemento tridentctl-protect.

Personalizar la instalación de Trident Protect

Puede personalizar la configuración predeterminada de Trident Protect para satisfacer los requisitos específicos de su entorno.

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. Crea 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 las opciones disponibles y contiene los valores 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 de `resourceLimits.yaml` archivo:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect -f resourceLimits.yaml --reuse-values
```

Personalizar las restricciones del contexto de seguridad

Puede utilizar un archivo de configuración para modificar la restricción de contexto de seguridad (SCC) de OpenShift para los contenedores de Trident Protect después de instalar Trident Protect. Estas restricciones definen las limitaciones de seguridad para los pods en un clúster de Red Hat OpenShift.

Pasos

1. Crea un archivo llamado `sccconfig.yaml` .
2. Agregue la opción SCC al archivo y modifique los parámetros según las necesidades de su entorno.

   El siguiente ejemplo muestra los valores predeterminados de los parámetros para la opción SCC:

```
scc:
  create: true
  name: trident-protect-job
  priority: 1
```

Esta tabla describe los parámetros para la opción SCC:

Parámetro	Descripción	Por defecto
crear	Determina si se puede crear un recurso SCC. Un recurso SCC se creará solo si `scc.create` está configurado para `true` y el proceso de instalación de Helm identifica un entorno OpenShift. Si no se está operando en OpenShift, o si `scc.create` está configurado para `false` , no se creará ningún recurso SCC.	verdadero
nombre	Especifica el nombre del SCC.	trabajo de protección de tridente
prioridad	Define la prioridad del SCC. Los SCC con valores de prioridad más altos se evalúan antes que aquellos con valores más bajos.	1

3. Aplique los valores de `sccconfig.yaml` archivo:

```
helm upgrade trident-protect netapp-trident-protect/trident-protect -f
sccconfig.yaml --reuse-values
```

Esto reemplazará los valores predeterminados con los especificados en el `sccconfig.yaml` archivo.

Configurar ajustes adicionales del gráfico de timón Trident Protect

Puede personalizar la configuración de AutoSupport y el filtrado de espacios de nombres para satisfacer sus requisitos específicos. La siguiente tabla describe los parámetros de configuración disponibles:

Parámetro	Tipo	Descripción
autoSupport.proxy	cadena	Configura una URL de proxy para conexiones de NetApp AutoSupport . Use esto para enrutar las cargas de paquetes de soporte a través de un servidor proxy. Ejemplo: `http://my.proxy.url` .

Parámetro	Tipo	Descripción
autoSupport.inseguro	booleano	Omite la verificación TLS para las conexiones proxy de AutoSupport cuando está configurado en `true` . Úselo sólo para conexiones proxy inseguras. (por defecto: `false`)
autoSupport.enabled	booleano	Habilita o deshabilita las cargas diarias de paquetes de AutoSupport de Trident Protect. Cuando se configura para `false` Las cargas diarias programadas están desactivadas, pero aún puede generar manualmente paquetes de soporte. (por defecto: `true`)
restaurar anotaciones de SkipNamespace	cadena	Lista separada por comas de anotaciones de espacios de nombres para excluir de las operaciones de copia de seguridad y restauración. Le permite filtrar espacios de nombres según anotaciones.
restaurar etiquetas de espacios de nombres de saltos	cadena	Lista separada por comas de etiquetas de espacios de nombres para excluir de las operaciones de copia de seguridad y restauración. Le permite filtrar espacios de nombres según etiquetas.

Puede configurar estas opciones mediante un archivo de configuración YAML o indicadores de línea de comandos:

Utilice el archivo YAML

Pasos

1. Crea un archivo de configuración y nómbralo. `values.yaml` .
2. En el archivo que ha creado, agregue las opciones de configuración que desea personalizar.

```
autoSupport:
  enabled: false
  proxy: http://my.proxy.url
  insecure: true
restoreSkipNamespaceAnnotations: "annotation1,annotation2"
restoreSkipNamespaceLabels: "label1,label2"
```

3. Después de rellenar el `values.yaml` Archivo con los valores correctos, aplicar el archivo de configuración:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect -f values.yaml --reuse-values
```

Usar la bandera CLI

Pasos

1. Utilice el siguiente comando con el `--set` bandera para especificar parámetros individuales:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set autoSupport.enabled=false \
  --set autoSupport.proxy=http://my.proxy.url \
  --set restoreSkipNamespaceAnnotations="annotation1,annotation2" \
  --set restoreSkipNamespaceLabels="label1,label2" \
  --reuse-values
```

Restringir los pods de Trident Protect a nodos específicos

Puede utilizar la restricción de selección de nodos nodeSelector de Kubernetes para controlar cuáles de sus nodos son elegibles para ejecutar pods de Trident Protect, según las etiquetas de los nodos. De forma predeterminada, Trident Protect está restringido a los nodos que ejecutan Linux. Puedes personalizar aún más estas restricciones según tus necesidades.

Pasos

1. Crea un archivo llamado `nodeSelectorConfig.yaml` .
2. Agregue la opción nodeSelector al archivo y modifique el archivo para agregar o cambiar las etiquetas de los nodos para restringirlos según las necesidades de su entorno. Por ejemplo, el siguiente archivo

contiene la restricción predeterminada del sistema operativo, pero también se dirige a una región y un nombre de aplicación específicos:

```
nodeSelector:
  kubernetes.io/os: linux
  region: us-west
  app.kubernetes.io/name: mysql
```

3. Aplique los valores de `nodeSelectorConfig.yaml` archivo:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect -f nodeSelectorConfig.yaml --reuse-values
```

Esto reemplaza las restricciones predeterminadas con las que usted especificó en el `nodeSelectorConfig.yaml` archivo.