



Instalar Trident Protect

Trident

NetApp

February 02, 2026

This PDF was generated from <https://docs.netapp.com/es-es/trident/trident-protect/trident-protect-requirements.html> on February 02, 2026. Always check docs.netapp.com for the latest.

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 5
 - Instalar Trident Protect 5
 - 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
 - Personalizar la instalación de Trident Protect 13
 - Especificar los límites de recursos del contenedor Trident Protect 13
 - Personalizar restricciones de contexto de seguridad 14
 - Configurar ajustes adicionales del gráfico de timón Trident Protect 15
 - Restringir los pods de Trident Protect a nodos específicos 17

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



- 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"](#).
- Asegúrese de que exista al menos una VolumeSnapshotClass. Para obtener más información, consulte ["VolumeSnapshotClass"](#).

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:

- Asegúrese de que el almacenamiento de NetApp conectado al clúster utilice Trident 24.02 o más reciente (se recomienda Trident 24.10).
- 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 planea 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 proporciona capacidades de congelamiento y descongelamiento del sistema de archivos para máquinas virtuales KubeVirt durante operaciones de protección de datos para garantizar la consistencia de los datos. El método de configuración y el comportamiento predeterminado para las operaciones de congelamiento de VM varían según las versiones de Trident Protect; las versiones más nuevas ofrecen una configuración simplificada a través de los parámetros del gráfico de Helm.



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

Trident Protect 25.10 y versiones posteriores

Trident Protect congela y descongela automáticamente los sistemas de archivos de KubeVirt durante las operaciones de protección de datos para garantizar la coherencia. A partir de Trident Protect 25.10, puede desactivar este comportamiento mediante el `vm.freeze` parámetro durante la instalación del gráfico Helm. El parámetro está habilitado por defecto.

```
helm install ... --set vm.freeze=false ...
```

Trident Protect 24.10.1 a 25.06

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
```

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
```

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 de NetApp FAS, AFF y ASA en las instalaciones
- 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:

- *** 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 la versión mínima de ONTAP 9.15.1)
- **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.

A partir de ONTAP 9.10.1, todas las licencias se proporcionan como archivo de licencia de NetApp (NLF), que es un solo archivo que admite varias funciones. Consulte ["Licencias incluidas con ONTAP One"](#) si desea obtener más información.



Sólo se admite la protección asíncrona SnapMirror.

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.

- **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 con los siguientes requisitos:

- **Accesibilidad de AppVault**: tanto los clústeres de origen como 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 reglas de firewall, permisos de bucket y listas de IP permitidas para habilitar la comunicación entre ambos clústeres y AppVault a través de 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. Añada el repositorio Helm de Trident:

```
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 100.2510.0 --create  
--namespace --namespace trident-protect
```

3. Opcionalmente, para habilitar el registro de depuración (recomendado para la resolución de problemas), utilice:

```
helm install trident-protect netapp-trident-protect/trident-protect  
--set clusterName=<name-of-cluster> --set logLevel=debug --version  
100.2510.0 --create-namespace --namespace trident-protect
```

El registro de depuración ayuda al soporte de NetApp a solucionar problemas sin necesidad de cambiar el nivel de registro ni reproducir el problema.

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:


```
docker.io/netapp/controller:25.10.0
docker.io/netapp/restic:25.10.0
docker.io/netapp/kopia:25.10.0
docker.io/netapp/kopiablockrestore:25.10.0
docker.io/netapp/trident-autosupport:25.10.0
docker.io/netapp/exehook:25.10.0
docker.io/netapp/resourcebackup:25.10.0
docker.io/netapp/resourcerestore:25.10.0
docker.io/netapp/resourcedelete:25.10.0
docker.io/netapp/trident-protect-utils:v1.0.0
```

Por ejemplo:

```
docker pull docker.io/netapp/controller:25.10.0
```

```
docker tag docker.io/netapp/controller:25.10.0 <private-registry-
url>/controller:25.10.0
```

```
docker push <private-registry-url>/controller:25.10.0
```



Para obtener el gráfico de Helm, primero descárguelo en una máquina con acceso a Internet usando `helm pull trident-protect --version 100.2510.0 --repo https://netapp.github.io/trident-protect-helm-chart`, luego copie el resultado `trident-protect-100.2510.0.tgz` transfiera el archivo a su entorno sin conexión e instálelo usando `helm install trident-protect ./trident-protect-100.2510.0.tgz` en lugar de la referencia al repositorio en el paso final.

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:

```
---  
imageRegistry: <private-registry-url>  
imagePullSecrets:  
  - name: regcred
```



El `imageRegistry` y `imagePullSecrets` Los valores se aplican a todas las imágenes de componentes, incluyendo `resourcebackup` y `resourcerestore`. Si envías imágenes a una ruta de repositorio específica dentro de tu registro (por ejemplo, `example.com:443/my-repo`), incluya la ruta completa en el campo del registro. Esto garantizará que todas las imágenes se extraigan de `<private-registry-url>/<image-name>:<tag>`.

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 100.2510.0 --create  
--namespace --namespace trident-protect -f protectValues.yaml
```

8. Opcionalmente, para habilitar el registro de depuración (recomendado para la resolución de problemas), utilice:

```
helm install trident-protect netapp-trident-protect/trident-protect  
--set clusterName=<name-of-cluster> --set logLevel=debug --version  
100.2510.0 --create-namespace --namespace trident-protect -f  
protectValues.yaml
```

El registro de depuración ayuda al soporte de NetApp a solucionar problemas sin necesidad de cambiar el nivel de registro ni reproducir el problema.



Para obtener opciones de configuración adicionales para el gráfico de Helm, incluidos los ajustes de AutoSupport y el filtrado de espacios de nombres, consulte "[Personalizar la instalación de Trident Protect](#)".

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/25.10.0/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/25.10.0/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/25.10.0/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/25.10.0/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. Crea el script de finalización:

```
tridentctl-protect completion bash > 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. Crea el script de finalización:

```
tridentctl-protect completion zsh > 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.

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. 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 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 del `resourceLimits.yaml` archivo:

```

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

```

Personalizar restricciones de 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. Crear 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
```

En esta tabla se describen los parámetros de la opción SCC:

Parámetro	Descripción	Predeterminado
cree	Determina si se puede crear un recurso SCC. Un recurso de SCC se creará sólo si <code>scc.create</code> se establece en <code>true</code> y el proceso de instalación de Helm identifica un entorno de OpenShift. Si no funciona en OpenShift, o si <code>scc.create</code> está establecido en <code>false</code> , no se creará ningún recurso SCC.	verdadero
nombre	Especifica el nombre del SCC.	Trident-protect-job
prioridad	Define la prioridad del SCC. Los SCCS con valores de prioridad más altos se evalúan antes que aquellos con valores más bajos.	1

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

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

Esto reemplazará los valores predeterminados por 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 se configura en <code>true</code> . Úselo sólo para conexiones proxy inseguras. (por defecto: <code>false</code>)
autoSupport.enabled	booleano	Habilita o deshabilita las cargas diarias de paquetes de AutoSupport de Trident Protect. Cuando se configura para <code>false</code> Las cargas diarias programadas están desactivadas, pero aún puede generar manualmente paquetes de soporte. (por defecto: <code>true</code>)
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, aplique 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-string
restoreSkipNamespaceAnnotations="{annotation1,annotation2}" \
  --set-string 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. Crear un archivo llamado `nodeSelectorConfig.yaml`.
2. Agregue la opción `nodeSelector` al archivo y modifique el archivo para agregar o cambiar etiquetas de

nodo para restringir según las necesidades del 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 del `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 por las especificadas en el `nodeSelectorConfig.yaml` archivo.

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.