Instale o Trident Protect

Trident

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/pt-br/trident-2410/trident-protect/trident-protect-requirements.html on September 26, 2025. Always check docs.netapp.com for the latest.

Índice

Instale o Trident Protect . . . 1
Requisitos do Trident Protect . . . 1
O Trident protege a compatibilidade de clusters do Kubernetes . . . 1
O Trident protege a compatibilidade de back-end de storage . . . 1
Requisitos para volumes nas-economia . . . 2
Proteção de dados com máquinas virtuais do KubeVirt . . . 2
Requisitos para replicação do SnapMirror . . . 3
Instalar e configurar o Trident Protect . . . 4
Instale o Trident Protect . . . 4
Especifique os limites de recursos do contêiner do Trident Protect . . . 8
Instale o plugin Trident Protect CLI . . . 9
Instale o plugin Trident Protect CLI . . . 9
Veja a ajuda do plugin Trident CLI . . . 11
Ativar a auto-conclusão do comando . . . 11

Instale o Trident Protect

Requisitos do Trident Protect

Comece verificando a prontidão do seu ambiente operacional, clusters de aplicativos, aplicativos e licenças. Certifique-se de que seu ambiente atenda a esses requisitos para implantar e operar o Trident Protect.

O Trident protege a compatibilidade de clusters do Kubernetes

O Trident Protect é compatível com uma ampla variedade de ofertas do Kubernetes totalmente gerenciadas e autogeridas, incluindo:

- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Microsoft Azure Kubernetes Service (AKS)
- Red Hat OpenShift
- SUSE Rancher
- Portfólio do VMware Tanzu
- Kubernetes upstream

> Verifique se o cluster no qual você instala o Trident Protect está configurado com um controlador de snapshot em execução e as CRDs relacionadas. Para instalar um controlador instantâneo, "estas instruções" consulte a .

O Trident protege a compatibilidade de back-end de storage

O Trident Protect suporta os seguintes backends de armazenamento:

- Amazon FSX para NetApp ONTAP
- Cloud Volumes ONTAP
- Storage arrays ONTAP
- Google Cloud NetApp volumes
- Azure NetApp Files

Certifique-se de que o back-end de storage atenda aos seguintes requisitos:

- Certifique-se de que o storage NetApp conectado ao cluster esteja usando o Astra Trident 24,02 ou mais recente (recomenda-se o Trident 24,10).
  - Se o Astra Trident for mais antigo que a versão 24.06.1 e você planeja usar a funcionalidade de recuperação de desastres do NetApp SnapMirror, é necessário habilitar manualmente o Supervisor de Controle Astra.
- Certifique-se de que você tem o mais recente software de previsão Astra Control (instalado e habilitado por padrão a partir do Astra Trident 24.06.1).
- Verifique se você tem um back-end de storage do NetApp ONTAP.

- Certifique-se de ter configurado um bucket de armazenamento de objetos para armazenar backups.
- Crie namespaces de aplicações que você planeja usar para aplicações ou operações de gerenciamento de dados de aplicações. O Trident Protect não cria esses namespaces para você; se você especificar um namespace inexistente em um recurso personalizado, a operação falhará.

Requisitos para volumes nas-economia

O Trident Protect é compatível com operações de backup e restauração em volumes com economia nas. Snapshots, clones e replicação SnapMirror para volumes nas-Economy atualmente não são compatíveis. Você precisa ativar um diretório de snapshot para cada volume de economia nas que você planeja usar com o Trident Protect.

> Alguns aplicativos não são compatíveis com volumes que usam um diretório instantâneo. Para esses aplicativos, você precisa ocultar o diretório instantâneo executando o seguinte comando no sistema de armazenamento ONTAP:
>
> ```
> nfs modify -vserver <svm> -v3-hide-snapshot enabled
> ```

Você pode ativar o diretório de snapshot executando o seguinte comando para cada volume de economia nas, substituindo `<volume-UUID>` pelo UUID do volume que deseja alterar:

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

> Você pode habilitar diretórios de snapshot por padrão para novos volumes definindo a opção de configuração de back-end do Trident `snapshotDir` como `true`. Os volumes existentes não são afetados.

Proteção de dados com máquinas virtuais do KubeVirt

O Trident Protect 24,10 e 24.10.1 e versões mais recentes têm comportamento diferente quando você protege aplicativos em execução em VMs KubeVirt. Para ambas as versões, você pode ativar ou desativar o congelamento e o descongelamento do sistema de arquivos durante operações de proteção de dados.

> Para todas as versões do Trident Protect, para habilitar ou desabilitar a funcionalidade de congelamento automático em ambientes OpenShift, talvez seja necessário conceder permissões privilegiadas para o namespace do aplicativo. Por exemplo:
>
> ```
> oc adm policy add-scc-to-user privileged -z default -n
> <application-namespace>
> ```

Trident Protect 24,10

O Trident Protect 24,10 não garante automaticamente um estado consistente para os sistemas de arquivos da VM do KubeVirt durante operações de proteção de dados. Se você quiser proteger seus dados da VM KubeVirt usando o Trident Protect 24,10, você precisa ativar manualmente a funcionalidade congelar/descongelar para os sistemas de arquivos antes da operação de proteção de dados. Isso garante

que os sistemas de arquivos estejam em um estado consistente.

Você pode configurar o Trident Protect 24,10 para gerenciar o congelamento e o descongelamento do sistema de arquivos da VM durante operações de proteção de dados "configuração da virtualização"usando o seguinte comando:

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

Trident Protect 24.10.1 e mais recente

A partir do Trident Protect 24.10.1, o Trident Protect congela e descongela automaticamente os sistemas de arquivos KubeVirt durante operações de proteção de dados. Opcionalmente, você pode desativar esse comportamento automático usando o seguinte comando:

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

Requisitos para replicação do SnapMirror

O NetApp SnapMirror está disponível para uso com o Trident Protect para as seguintes soluções da ONTAP:

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

Requisitos de cluster do ONTAP para replicação do SnapMirror

Se você planeja usar a replicação do SnapMirror, verifique se o cluster do ONTAP atende aos seguintes requisitos:

- **Parceiro de Controle Astra ou Trident**: O Trident ou o Provisioner do Astra Control devem existir nos clusters do Kubernetes de origem e destino que utilizam o ONTAP como um back-end. O Trident Protect oferece suporte à replicação com a tecnologia NetApp SnapMirror usando classes de armazenamento com os seguintes drivers:
  - `ontap-nas`
  - `ontap-san`
- **Licenças**: As licenças assíncronas do ONTAP SnapMirror usando o pacote proteção de dados devem estar ativadas nos clusters ONTAP de origem e destino. "Visão geral do licenciamento do SnapMirror no ONTAP"Consulte para obter mais informações.

Considerações de peering para replicação do SnapMirror

Certifique-se de que seu ambiente atenda aos seguintes requisitos se você planeja usar peering de back-end

de storage:

- **Cluster e SVM**: Os backends de storage do ONTAP devem ser colocados em Contato. "Visão geral do peering de cluster e SVM"Consulte para obter mais informações.

> Certifique-se de que os nomes do SVM usados na relação de replicação entre dois clusters ONTAP sejam exclusivos.

- **Supervisor de Controle Astra ou Trident e SVM**: Os SVMs remotos em Contato devem estar disponíveis para o Astra Control Provisioner ou Trident no cluster de destino.
- **Backends gerenciados**: Você precisa adicionar e gerenciar backends de armazenamento ONTAP no Trident Protect para criar uma relação de replicação.
- **NVMe em TCP**: O Trident Protect não oferece suporte à replicação NetApp SnapMirror para back-ends de armazenamento que estejam usando o protocolo NVMe em TCP.

Configuração Trident / ONTAP para replicação SnapMirror

O Trident Protect exige que você configure pelo menos um back-end de storage compatível com a replicação para os clusters de origem e destino. Se os clusters de origem e destino forem iguais, o aplicativo de destino deverá usar um back-end de storage diferente do aplicativo de origem para obter a melhor resiliência.

Instalar e configurar o Trident Protect

Se o seu ambiente atender aos requisitos do Trident Protect, siga estas etapas para instalar o Trident Protect no cluster. Você pode obter o Trident Protect do NetApp, ou instalá-lo a partir de seu próprio Registro privado. A instalação a partir de um registo privado é útil se o cluster não conseguir aceder à Internet.

> Por padrão, o Trident Protect coleta informações de suporte que ajudam em todos os casos de suporte da NetApp que você possa abrir, incluindo logs, métricas e informações de topologia sobre clusters e aplicativos gerenciados. O Trident Protect envia esses pacotes de suporte ao NetApp diariamente. Opcionalmente, você pode desativar essa coleção de pacotes de suporte ao instalar o Trident Protect. Você pode manualmente "gerar um pacote de suporte" a qualquer momento.

Instale o Trident Protect

Instale o Trident Protect do NetApp

Passos

1. Adicione o repositório Helm do Trident:

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

2. Instale as CRDs Trident Protect:

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

3. Use o Helm para instalar o Trident Protect usando um dos seguintes comandos. Substitua `<name_of_cluster>` por um nome de cluster, que será atribuído ao cluster e usado para identificar os backups e snapshots do cluster:
   - Instale o 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 o Trident Protect e desative os carregamentos diários programados do pacote de suporte do Trident Protect AutoSupport:

```
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
```

Instale o Trident Protect a partir de um registo privado

Você pode instalar o Trident Protect a partir de um Registro de imagem privado se o cluster do Kubernetes não conseguir acessar a Internet. Nestes exemplos, substitua valores entre parênteses por informações do seu ambiente:

Passos

1. Puxe as seguintes imagens para a sua máquina local, atualize as etiquetas e, em seguida, envie-as para o seu registo 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 exemplo:

```
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. Crie o namespace do sistema Trident Protect:

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

3. Inicie sessão no registo:

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

4. Crie um segredo para usar para autenticação de 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. Adicione o repositório Helm do Trident:

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

6. Crie um arquivo chamado `protectValues.yaml`. Verifique se ele contém as seguintes configurações de proteção Trident:

```yaml
---
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. Instale as CRDs Trident Protect:

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

8. Use o Helm para instalar o Trident Protect usando um dos seguintes comandos. Substitua `<name_of_cluster>` por um nome de cluster, que será atribuído ao cluster e usado para identificar os backups e snapshots do cluster:
   - Instale o 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 o Trident Protect e desative os carregamentos diários programados do pacote de suporte do Trident Protect AutoSupport:

```
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
```

Especifique os limites de recursos do contêiner do Trident Protect

Você pode usar um arquivo de configuração para especificar limites de recursos para contentores do Trident Protect depois de instalar o Trident Protect. A definição de limites de recursos permite controlar quanto dos recursos do cluster são consumidos pelas operações do Trident Protect.

Passos

1. Crie um arquivo chamado `resourceLimits.yaml`.
2. Preencha o arquivo com opções de limite de recursos para contentores do Trident Protect de acordo com as necessidades do seu ambiente.

   O seguinte exemplo de arquivo de configuração mostra as configurações disponíveis e contém os vaules padrão para cada limite 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 os valores do `resourceLimits.yaml` arquivo:

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

Instale o plugin Trident Protect CLI

Você pode usar o plugin de linha de comando Trident Protect, que é uma extensão do utilitário Trident `tridentctl`, para criar e interagir com o Trident Protect custom Resources (CRS).

Instale o plugin Trident Protect CLI

Antes de usar o utilitário de linha de comando, você precisa instalá-lo na máquina usada para acessar o cluster. Siga estes passos, dependendo se a sua máquina utiliza uma CPU x64 ou ARM.

Faça o download do plugin para CPUs Linux AMD64

Passos

1. Faça o download do plugin Trident Protect CLI:

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

Faça o download do plugin para CPUs Linux ARM64

Passos

1. Faça o download do plugin Trident Protect CLI:

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

Baixe o plugin para CPUs Mac AMD64

Passos

1. Faça o download do plugin Trident Protect CLI:

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

Baixe o plugin para CPUs Mac ARM64

Passos

1. Faça o download do plugin Trident Protect CLI:

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

1. Ativar permissões de execução para o binário do plugin:

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

2. Copie o binário do plugin para um local definido na variável PATH. Por exemplo, `/usr/bin` ou `/usr/local/bin` (você pode precisar de Privileges elevado):

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

3. Opcionalmente, você pode copiar o binário do plugin para um local em seu diretório home. Neste caso, é recomendável garantir que a localização faça parte da variável PATH:

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

> Copiar o plugin para um local em sua variável PATH permite que você use o plugin digitando `tridentctl-protect` ou `tridentctl protect` de qualquer local.

Veja a ajuda do plugin Trident CLI

Você pode usar os recursos integrados de ajuda do plugin para obter ajuda detalhada sobre os recursos do plugin:

Passos

1. Utilize a função de ajuda para visualizar as orientações de utilização:

```
tridentctl-protect help
```

Ativar a auto-conclusão do comando

Depois de instalar o plugin Trident Protect CLI, você pode ativar a auto-conclusão para determinados comandos.

Ative a auto-conclusão para o shell Bash

Passos

1. Faça o download do script de conclusão:

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

2. Crie um novo diretório em seu diretório inicial para conter o script:

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

3. Mova o script baixado para `~/.bash/completions` o diretório:

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

4. Adicione a seguinte linha ao `~/.bashrc` arquivo em seu diretório inicial:

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

Ative a auto-conclusão para o shell Z.

Passos

1. Faça o download do script de conclusão:

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

2. Crie um novo diretório em seu diretório inicial para conter o script:

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

3. Mova o script baixado para `~/.zsh/completions` o diretório:

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

4. Adicione a seguinte linha ao `~/.zprofile` arquivo em seu diretório inicial:

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

Resultado

Após o seu próximo login shell, você pode usar o comando auto-completação com o plugin tridentctl-protect.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.