



Installez Trident Protect

Trident

NetApp
September 26, 2025

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

Sommaire

Installez Trident Protect	1
Exigences de Trident Protect	1
Compatibilité des clusters Trident Protect Kubernetes	1
Trident protège la compatibilité back-end du stockage	1
Conditions requises pour les volumes d'économie nas	2
Protéger les données avec les machines virtuelles KubeVirt	2
Conditions requises pour la réplication SnapMirror	3
Installer et configurer Trident Protect	4
Installez Trident Protect	4
Spécifiez les limites des ressources du conteneur Trident Protect	8
Installez le plug-in Trident Protect CLI	9
Installez le plug-in Trident Protect CLI	9
Afficher l'Trident aide du plug-in de l'interface de ligne	11
Activer la saisie semi-automatique de la commande	11

Installez Trident Protect

Exigences de Trident Protect

Commencez par vérifier que votre environnement opérationnel, vos clusters d'applications, vos applications et vos licences sont prêts. Déploiement et exploitation de Trident Protect répondent à ces exigences.

Compatibilité des clusters Trident Protect Kubernetes

Trident Protect est compatible avec un large éventail d'offres Kubernetes entièrement gérées et autogérées, notamment :

- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Microsoft Azure Kubernetes Service (AKS)
- Red Hat OpenShift
- SUSE Rancher
- Gamme VMware Tanzu
- Kubernetes en amont



Assurez-vous que le cluster sur lequel vous installez Trident Protect est configuré avec un contrôleur de snapshot en cours d'exécution et les CRD associés. Pour installer un contrôleur de snapshot, reportez-vous à "[ces instructions](#)".

Trident protège la compatibilité back-end du stockage

Trident Protect prend en charge les systèmes back-end suivants :

- Amazon FSX pour NetApp ONTAP
- Cloud Volumes ONTAP
- Baies de stockage ONTAP
- Google Cloud NetApp volumes
- Azure NetApp Files

Assurez-vous que votre système back-end répond aux exigences suivantes :

- Assurez-vous que le stockage NetApp connecté au cluster utilise Astra Trident 24.02 ou version ultérieure (Trident 24.10 est recommandé).
 - Si Astra Trident est antérieure à la version 24.06.1 et que vous prévoyez d'utiliser la fonctionnalité de reprise d'activité NetApp SnapMirror, vous devez activer manuellement Astra Control provisionner.
- Vérifiez que vous disposez de la dernière version d'Astra Control Provisioner (installée et activée par défaut à partir d'Astra Trident 24.06.1).
- Assurez-vous de disposer d'un système back-end de stockage NetApp ONTAP.
- Assurez-vous d'avoir configuré un compartiment de stockage objet pour le stockage des sauvegardes.

- Créez tous les espaces de noms d'applications que vous prévoyez d'utiliser pour les opérations de gestion des données d'applications ou d'applications. Trident Protect ne crée pas ces espaces de noms pour vous ; si vous spécifiez un espace de noms inexistant dans une ressource personnalisée, l'opération échoue.

Conditions requises pour les volumes d'économie nas

Trident Protect prend en charge les opérations de sauvegarde et de restauration sur les volumes économiques nas. Les copies Snapshot, les clones et la réplication SnapMirror sur des volumes économiques nas ne sont pas pris en charge actuellement. Vous devez activer un répertoire d'instantanés pour chaque volume d'économie nas que vous prévoyez d'utiliser avec Trident Protect.



Certaines applications ne sont pas compatibles avec les volumes qui utilisent un répertoire de snapshots. Pour ces applications, vous devez masquer le répertoire des snapshots en exécutant la commande suivante sur le système de stockage ONTAP :

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

Vous pouvez activer le répertoire des snapshots en exécutant la commande suivante pour chaque volume nas-Economy, en remplaçant <volume-UUID> par l'UUID du volume à modifier :

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



Vous pouvez activer les répertoires de snapshots par défaut pour les nouveaux volumes en définissant l'option de configuration du back-end Trident `snapshotDir` sur `true`. Les volumes existants ne sont pas affectés.

Protéger les données avec les machines virtuelles KubeVirt

Trident Protect 24.10, 24.10.1 et versions ultérieures ont des comportements différents lorsque vous protégez les applications s'exécutant sur des machines virtuelles KubeVirt. Pour les deux versions, vous pouvez activer ou désactiver le blocage et le déblocage du système de fichiers pendant les opérations de protection des données.



Pour toutes les versions de Trident Protect, pour activer ou désactiver la fonctionnalité de blocage automatique dans les environnements OpenShift, vous devrez peut-être accorder des autorisations privilégiées à l'espace de noms d'applications. Par exemple :

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

Trident Protect 24.10

Trident Protect 24.10 ne garantit pas automatiquement un état cohérent pour les systèmes de fichiers des machines virtuelles KubeVirt lors des opérations de protection des données. Pour protéger les données de vos machines virtuelles KubeVirt à l'aide de Trident Protect 24.10, vous devez activer manuellement la fonctionnalité de gel/dégel pour les systèmes de fichiers avant l'opération de protection des données. Cela

permet de s'assurer que les systèmes de fichiers sont dans un état cohérent.

Vous pouvez configurer Trident Protect 24.10 pour gérer le gel et le déblocage du système de fichiers de la machine virtuelle pendant les opérations de protection des données par "[configuration de la virtualisation](#)" puis à l'aide de la commande suivante :

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

Trident Protect 24.10.1 et versions ultérieures

Depuis Trident Protect 24.10.1, Trident Protect gèle et débloque automatiquement les systèmes de fichiers KubeVirt pendant les opérations de protection des données. Si vous le souhaitez, vous pouvez désactiver ce comportement automatique à l'aide de la commande suivante :

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

Conditions requises pour la réplication SnapMirror

NetApp SnapMirror est disponible pour les solutions ONTAP suivantes avec Trident Protect :

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

Configuration requise pour un cluster ONTAP pour la réplication SnapMirror

Si vous prévoyez d'utiliser la réplication SnapMirror, assurez-vous que votre cluster ONTAP répond aux exigences suivantes :

- **Astra Control Provisioner ou Trident** : Astra Control Provisioner ou Trident doit exister sur les clusters Kubernetes source et de destination qui utilisent ONTAP en tant que back-end. Trident Protect prend en charge la réplication avec la technologie NetApp SnapMirror au moyen de classes de stockage basées sur les pilotes suivants :
 - `ontap-nas`
 - `ontap-san`
- **Licences** : les licences asynchrones de SnapMirror ONTAP utilisant le bundle protection des données doivent être activées sur les clusters ONTAP source et cible. Pour plus d'informations, reportez-vous à la section "[Présentation des licences SnapMirror dans ONTAP](#)".

Considérations de peering pour la réplication SnapMirror

Si vous prévoyez d'utiliser le peering back-end, assurez-vous que votre environnement répond aux exigences

suivantes :

- **Cluster et SVM** : les systèmes back-end de stockage ONTAP doivent être peering. Pour plus d'informations, reportez-vous à la section "[Présentation du cluster et de SVM peering](#)".



S'assurer que les noms de SVM utilisés dans la relation de réplication entre deux clusters ONTAP sont uniques.

- **Astra Control Provisioner ou Trident et SVM** : les SVM distants à peering doivent être disponibles pour Astra Control Provisioner ou Trident sur le cluster destination.
- **Systèmes back-end gérés** : vous devez ajouter et gérer des systèmes back-end de stockage ONTAP dans Trident Protect pour créer une relation de réplication.
- **NVMe over TCP** : Trident Protect ne prend pas en charge la réplication NetApp SnapMirror pour les systèmes back-end de stockage qui utilisent le protocole NVMe over TCP.

Configuration Trident/ONTAP pour la réplication SnapMirror

Trident Protect exige que vous configuriez au moins un système back-end de stockage qui prend en charge la réplication à la fois pour les clusters source et de destination. Si les clusters source et cible sont identiques, l'application de destination doit utiliser un back-end de stockage différent de l'application source pour une résilience optimale.

Installer et configurer Trident Protect

Si votre environnement satisfait aux exigences de Trident Protect, vous pouvez suivre ces étapes pour installer Trident Protect sur votre cluster. Vous pouvez obtenir Trident Protect de NetApp ou l'installer à partir de votre propre registre privé. L'installation à partir d'un registre privé est utile si votre cluster ne peut pas accéder à Internet.



Par défaut, Trident Protect collecte des informations sur le support que vous pouvez ouvrir dans tous les dossiers de support NetApp, y compris les journaux, les metrics et les informations de topologie des clusters et des applications gérées. Trident Protect envoie ces offres de support à NetApp selon un calendrier quotidien. Vous pouvez éventuellement désactiver cette collection de packs de prise en charge lorsque vous installez Trident Protect. Vous pouvez le faire manuellement "[générer un bundle de support](#)" à tout moment.

Installez Trident Protect

Installez Trident Protect from NetApp

Étapes

1. Ajout du référentiel Trident Helm :

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

2. Installez les CRD Trident Protect :

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

3. Utilisez Helm pour installer Trident Protect à l'aide de l'une des commandes suivantes. Remplacer `<name_of_cluster>` par un nom de cluster, qui sera attribué au cluster et utilisé pour identifier les sauvegardes et snapshots du cluster :

- Installez Trident Protect normalement :

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

- Installez Trident Protect et désactivez les téléchargements quotidiens de packs de prise en charge 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
```

Installez Trident Protect à partir d'un registre privé

Vous pouvez installer Trident Protect à partir d'un registre d'images privé si votre cluster Kubernetes ne peut pas accéder à Internet. Dans ces exemples, remplacez les valeurs entre parenthèses par les informations de votre environnement :

Étapes

1. Extrayez les images suivantes sur votre ordinateur local, mettez à jour les balises, puis envoyez-les vers votre registre privé :

```
netapp/controller:24.10.1
netapp/restic:24.10.1
netapp/kopia:24.10.1
netapp/trident-autosupport:24.10.0
netapp/execheek: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
```

Par exemple :

```
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. Créer l'espace de noms du système Trident Protect :

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

3. Connectez-vous au registre :

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

4. Créez un secret Pull à utiliser pour l'authentification de registre privé :

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

5. Ajout du référentiel Trident Helm :

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

6. Créez un fichier nommé `protectValues.yaml`. Assurez-vous qu'il contient les paramètres Trident Protect suivants :

```
---
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. Installez les CRD Trident Protect :

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

8. Utilisez Helm pour installer Trident Protect à l'aide de l'une des commandes suivantes. Remplacer `<name_of_cluster>` par un nom de cluster, qui sera attribué au cluster et utilisé pour identifier les sauvegardes et snapshots du cluster :

- Installez Trident Protect normalement :

```
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
```

- Installez Trident Protect et désactivez les téléchargements quotidiens de packs de prise en charge 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
```

Spécifiez les limites des ressources du conteneur Trident Protect

Vous pouvez utiliser un fichier de configuration pour spécifier les limites de ressources pour les conteneurs Trident Protect après avoir installé Trident Protect. La définition de limites de ressources vous permet de contrôler la quantité de ressources du cluster consommées par les opérations Trident Protect.

Étapes

1. Créez un fichier nommé `resourceLimits.yaml`.
2. Remplissez le fichier avec les options de limite de ressources pour les conteneurs Trident Protect en fonction des besoins de votre environnement.

L'exemple de fichier de configuration suivant montre les paramètres disponibles et contient les valeurs par défaut pour chaque limite de ressource :

```
---
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. Appliquer les valeurs du `resourceLimits.yaml` fichier :

```

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

```

Installez le plug-in Trident Protect CLI

Vous pouvez utiliser le plug-in de ligne de commande Trident Protect, qui est une extension de l'utilitaire Trident `tridentctl`, pour créer et interagir avec les ressources personnalisées Trident Protect (CRS).

Installez le plug-in Trident Protect CLI

Avant d'utiliser l'utilitaire de ligne de commande, vous devez l'installer sur la machine que vous utilisez pour accéder à votre cluster. Procédez comme suit, selon si votre ordinateur utilise un processeur x64 ou ARM.

Télécharger le plug-in pour les processeurs Linux AMD64

Étapes

1. Téléchargez le plug-in Trident Protect CLI :

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

Télécharger le plug-in pour les processeurs Linux ARM64

Étapes

1. Téléchargez le plug-in Trident Protect CLI :

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

Télécharger le plug-in pour les processeurs Mac AMD64

Étapes

1. Téléchargez le plug-in Trident Protect CLI :

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

Télécharger le plug-in pour les processeurs Mac ARM64

Étapes

1. Téléchargez le plug-in Trident Protect CLI :

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

1. Activer les autorisations d'exécution pour le binaire du plug-in :

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

2. Copiez le fichier binaire du plug-in à un emplacement défini dans votre variable PATH. Par exemple, /usr/bin ou /usr/local/bin (vous pouvez avoir besoin d'un Privileges élevé) :

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

3. Vous pouvez également copier le fichier binaire du plug-in vers un emplacement de votre répertoire personnel. Dans ce cas, il est recommandé de s'assurer que l'emplacement fait partie de votre variable PATH :

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



La copie du plug-in vers un emplacement de la variable PATH vous permet d'utiliser le plug-in en tapant `tridentctl-protect` ou `tridentctl protect` à partir de n'importe quel emplacement.

Afficher l'Trident aide du plug-in de l'interface de ligne

Vous pouvez utiliser les fonctions d'aide du plug-in intégré pour obtenir une aide détaillée sur les fonctionnalités du plug-in :

Étapes

1. Utilisez la fonction d'aide pour afficher les conseils d'utilisation :

```
tridentctl-protect help
```

Activer la saisie semi-automatique de la commande

Une fois que vous avez installé le plug-in de l'interface de ligne de commande Trident Protect, vous pouvez activer l'exécution automatique pour certaines commandes.

Activer la saisie semi-automatique pour le shell Bash

Étapes

1. Téléchargez le script d'achèvement :

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

2. Créez un nouveau répertoire dans votre répertoire personnel pour contenir le script :

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

3. Déplacez le script téléchargé dans le ~/.bash/completions répertoire :

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

4. Ajoutez la ligne suivante au ~/.bashrc fichier de votre répertoire personnel :

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

Activer la saisie semi-automatique pour la coque Z.

Étapes

1. Téléchargez le script d'achèvement :

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

2. Créez un nouveau répertoire dans votre répertoire personnel pour contenir le script :

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

3. Déplacez le script téléchargé dans le ~/.zsh/completions répertoire :

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

4. Ajoutez la ligne suivante au ~/.zprofile fichier de votre répertoire personnel :

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

Résultat

Lors de votre prochaine connexion au shell, vous pouvez utiliser la saisie semi-automatique de la commande avec le plugin `tridentctl-protect`.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.