Préparez le nœud de travail

Trident

NetApp
September 26, 2025

Sommaire

Préparez le nœud de travail

Tous les nœuds workers du cluster Kubernetes doivent pouvoir monter les volumes provisionnés pour vos pods. Pour préparer les nœuds workers, vous devez installer les outils NFS, iSCSI, NVMe/TCP ou FC en fonction de votre sélection de pilotes.

Choisir les bons outils

Si vous utilisez une combinaison de pilotes, vous devez installer tous les outils requis pour vos pilotes. Les versions récentes de RedHat CoreOS ont les outils installés par défaut.

Outils NFS

"Installez les outils NFS" si vous utilisez : `ontap-nas`, , `ontap-nas-economy`, `ontap-nas-flexgroup`, `azure-netapp-files` `gcp-cvs` .

Outils iSCSI

"Installez les outils iSCSI" si vous utilisez : `ontap-san`, , `ontap-san-economy` `solidfire-san` .

Outils NVMe

"Installez les outils NVMe" Si vous utilisez `ontap-san` pour le protocole NVMe (Nonvolatile Memory Express) over TCP (NVMe/TCP).

ONTAP 9.12 ou version ultérieure est recommandé pour NVMe/TCP.

Outils SCSI sur FC

SCSI over Fibre Channel (FC) est une fonctionnalité de prévisualisation technique dans la version Trident 24.10.

"Installez les outils FC" Si vous utilisez `ontap-san` avec sanType `fcp` (SCSI sur FC).

Pour plus d'informations, reportez-vous à la section "Manières de configurer FC ; hôtes SAN FC-NVMe" .

Détection des services de nœud

Trident tente de détecter automatiquement si le nœud peut exécuter des services iSCSI ou NFS.

La découverte de services de nœuds identifie les services détectés, mais ne garantit pas que les services sont correctement configurés. Inversement, l'absence d'un service découvert ne garantit pas l'échec du montage du volume.

Révision des événements

Trident crée des événements pour le nœud afin d'identifier les services détectés. Pour passer en revue ces événements, exécutez :

```
kubectl get event -A --field-selector involvedObject.name=<Kubernetes node name>
```

Examiner les services découverts

Trident identifie les services activés pour chaque nœud sur le nœud Trident CR. Pour afficher les services découverts, exécutez :

```
tridentctl get node -o wide -n <Trident namespace>
```

Volumes NFS

Installez les outils NFS à l'aide des commandes de votre système d'exploitation. Assurez-vous que le service NFS est démarré pendant le démarrage.

RHEL 8+

```
sudo yum install -y nfs-utils
```

Ubuntu

```
sudo apt-get install -y nfs-common
```

Redémarrez les nœuds workers après l'installation des outils NFS afin d'éviter toute défaillance lors de la connexion des volumes aux conteneurs.

Volumes iSCSI

Trident peut automatiquement établir une session iSCSI, analyser les LUN et détecter les périphériques à chemins d'accès multiples, les formater et les monter sur un pod.

Fonctionnalités d'auto-rétablissement de l'iSCSI

Pour les systèmes ONTAP, Trident exécute l'autorétablissement iSCSI toutes les cinq minutes pour :

1. **Identifier** l'état de session iSCSI souhaité et l'état de session iSCSI en cours.
2. **Comparer** l'état souhaité à l'état actuel pour identifier les réparations nécessaires. Trident détermine les priorités de réparation et le moment où les réparations doivent être effectuées.
3. **Effectuez les réparations** requises pour rétablir l'état de session iSCSI actuel à l'état de session iSCSI souhaité.

Les journaux d'activité d'auto-rétablissement se trouvent dans `trident-main` le conteneur sur le pod Demeset respectif. Pour afficher les journaux, vous devez avoir défini `debug` la valeur « true » lors de l'installation de Trident.

Les fonctionnalités d'auto-rétablissement iSCSI de Trident permettent d'éviter :

- Sessions iSCSI obsolètes ou non saines pouvant survenir après un problème de connectivité réseau. Dans le cas d'une session obsolète, Trident attend sept minutes avant de se déconnecter pour rétablir la

connexion avec un portail.

> Par exemple, si les secrets CHAP ont tourné sur le contrôleur de stockage et que le réseau perd la connectivité, les anciens secrets CHAP (*obsolète*) pourraient persister. L'auto-rétablissement peut reconnaître ceci et rétablir automatiquement la session pour appliquer les secrets CHAP mis à jour.

- Sessions iSCSI manquantes
- LUN manquantes

Points à prendre en compte avant de mettre à niveau Trident

- Si seuls les igroups par nœud (introduits dans 23.04+) sont utilisés, l'auto-rétablissement iSCSI lance des renumérisations SCSI pour tous les périphériques du bus SCSI.
- Si seuls les igroups dont le périmètre est back-end (obsolète à partir de la version 23.04) sont utilisés, l'auto-rétablissement iSCSI lance des renumérisations SCSI pour obtenir les ID de LUN exacts dans le bus SCSI.
- Si une combinaison d'igroups par nœud et d'igroups scoped back-end est utilisée, l'autorétablissement iSCSI lance des renumérisations SCSI pour obtenir des ID de LUN exacts sur le bus SCSI.

Installez les outils iSCSI

Installez les outils iSCSI à l'aide des commandes de votre système d'exploitation.

Avant de commencer

- Chaque nœud du cluster Kubernetes doit avoir un IQN unique. **C'est une condition préalable nécessaire**.
- Si vous utilisez RHCOS version 4.5 ou ultérieure, ou toute autre distribution Linux compatible avec RHEL, avec le `solidfire-san` pilote et Element OS 12.5 ou version antérieure, assurez-vous que l'algorithme d'authentification CHAP est défini sur MD5 dans. les `/etc/iscsi/iscsid.conf` algorithmes CHAP sécurisés conformes à la norme FIPS SHA1, SHA-256 et SHA3-256 sont disponibles avec Element 12.7.

```
sudo sed -i 's/^\(node.session.auth.chap_algs\).*/\1 = MD5/'
/etc/iscsi/iscsid.conf
```

- Lors de l'utilisation de nœuds worker exécutant RHEL/RedHat CoreOS avec iSCSI PVS, spécifiez la `discard` mountOption dans la classe de stockage pour effectuer la récupération d'espace en ligne. Reportez-vous à la "Documentation Red Hat".

RHEL 8+

1. Installez les packages système suivants :

```
sudo yum install -y lsscsi iscsi-initiator-utils device-mapper-
multipath
```

2. Vérifiez que la version iscsi-initiator-utils est 6.2.0.874-2.el7 ou ultérieure :

```
rpm -q iscsi-initiator-utils
```

3. Activer les chemins d'accès multiples :

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```

> Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

4. Assurez-vous que `iscsid` et `multipathd` sont en cours d'exécution :

```
sudo systemctl enable --now iscsid multipathd
```

5. Activer et démarrer `iscsi`:

```
sudo systemctl enable --now iscsi
```

Ubuntu

1. Installez les packages système suivants :

```
sudo apt-get install -y open-iscsi lsscsi sg3-utils multipath-tools
scsitools
```

2. Vérifiez que la version Open-iscsi est 2.0.874-5ubuntu2.10 ou ultérieure (pour bionique) ou 2.0.874-7.1ubuntu6.1 ou ultérieure (pour focaux) :

```
dpkg -l open-iscsi
```

3. Définir la numérisation sur manuelle :

```
sudo sed -i 's/^\(node.session.scan\).*/\1 = manual/'
/etc/iscsi/iscsid.conf
```

4. Activer les chemins d'accès multiples :

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```

> Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

5. Assurez-vous que `open-iscsi` et `multipath-tools` sont activés et en cours d'exécution :

```
sudo systemctl status multipath-tools
sudo systemctl enable --now open-iscsi.service
sudo systemctl status open-iscsi
```

> Pour Ubuntu 18.04, vous devez détecter les ports cibles avec `iscsiadm` avant de démarrer `open-iscsi` pour que le démon iSCSI démarre. Vous pouvez également modifier le `iscsi` service pour qu'il démarre `iscsid` automatiquement.

Configurez ou désactivez l'auto-rétablissement iSCSI

Vous pouvez configurer les paramètres d'auto-rétablissement iSCSI Trident suivants pour corriger les sessions obsolètes :

- **Intervalle d'auto-rétablissement iSCSI** : détermine la fréquence à laquelle l'auto-rétablissement iSCSI est appelé (par défaut : 5 minutes). Vous pouvez le configurer pour qu'il s'exécute plus fréquemment en définissant un nombre plus petit ou moins fréquemment en définissant un nombre plus grand.

> La définition de l'intervalle d'auto-rétablissement iSCSI sur 0 arrête complètement l'auto-rétablissement iSCSI. Nous ne recommandons pas de désactiver l'auto-rétablissement iSCSI. Il ne doit être désactivé que dans certains cas lorsque l'auto-rétablissement iSCSI ne fonctionne pas comme prévu ou à des fins de débogage.

- **Délai d'attente d'auto-rétablissement iSCSI** : détermine la durée d'attente de l'auto-rétablissement iSCSI avant de se déconnecter d'une session défectueuse et de tenter de se reconnecter (par défaut : 7

minutes). Vous pouvez le configurer sur un nombre plus grand de sorte que les sessions identifiées comme non saines doivent attendre plus longtemps avant d'être déconnectées, puis une tentative de connexion est faite, ou un nombre plus petit pour se déconnecter et se connecter plus tôt.

Gouvernail

Pour configurer ou modifier les paramètres d'autorétablissement iSCSI, passez les `iscsiSelfHealingInterval` paramètres et `iscsiSelfHealingWaitTime` lors de l'installation de Helm ou de la mise à jour Helm.

L'exemple suivant définit l'intervalle d'auto-rétablissement iSCSI sur 3 minutes et le temps d'attente d'auto-rétablissement sur 6 minutes :

```
helm install trident trident-operator-100.2410.0.tgz --set
iscsiSelfHealingInterval=3m0s --set iscsiSelfHealingWaitTime=6m0s -n
trident
```

tridentctl

Pour configurer ou modifier les paramètres d'auto-rétablissement iSCSI, passez les `iscsi-self-healing-interval` paramètres et `iscsi-self-healing-wait-time` lors de l'installation ou de la mise à jour de tridentctl.

L'exemple suivant définit l'intervalle d'auto-rétablissement iSCSI sur 3 minutes et le temps d'attente d'auto-rétablissement sur 6 minutes :

```
tridentctl install --iscsi-self-healing-interval=3m0s --iscsi-self
-healing-wait-time=6m0s -n trident
```

Volumes NVMe/TCP

Installez les outils NVMe à l'aide des commandes correspondant à votre système d'exploitation.

- NVMe requiert RHEL 9 ou version ultérieure.
- Si la version du noyau de votre nœud Kubernetes est trop ancienne ou si le package NVMe n'est pas disponible pour votre version du noyau, vous devrez peut-être mettre à jour la version du noyau de votre nœud avec le package NVMe.

RHEL 9

```
sudo yum install nvme-cli
sudo yum install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

Ubuntu

```
sudo apt install nvme-cli
sudo apt -y install linux-modules-extra-$(uname -r)
sudo modprobe nvme-tcp
```

Vérifiez l'installation

Après l'installation, vérifiez que chaque nœud du cluster Kubernetes dispose d'un NQN unique via la commande :

```
cat /etc/nvme/hostnqn
```

Trident modifie la `ctrl_device_tmo` valeur pour s'assurer que NVMe ne renonce pas au chemin s'il tombe en panne. Ne modifiez pas ce paramètre.

Installez les outils FC

Installez les outils FC à l'aide des commandes de votre système d'exploitation.

- Lors de l'utilisation de nœuds worker exécutant RHEL/RedHat CoreOS avec FC PVS, spécifiez la `discard` mountOption dans la classe de stockage pour effectuer la récupération d'espace en ligne. Reportez-vous à la "Documentation Red Hat".

RHEL 8+

1. Installez les packages système suivants :

```
sudo yum install -y lsscsi device-mapper-multipath
```

2. Activer les chemins d'accès multiples :

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```

> Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

3. Assurez-vous que `multipathd` est en cours d'exécution :

```
sudo systemctl enable --now multipathd
```

Ubuntu

1. Installez les packages système suivants :

```
sudo apt-get install -y lsscsi sg3-utils multipath-tools scsitools
```

2. Activer les chemins d'accès multiples :

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```

> Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

3. Assurez-vous que `multipath-tools` est activé et en cours d'exécution :

```
sudo systemctl status multipath-tools
```

Prise en charge de Fibre Channel (FC)

Vous pouvez désormais utiliser le protocole Fibre Channel (FC) avec Trident pour provisionner et gérer les ressources de stockage sur un système ONTAP.

SCSI over Fibre Channel (FC) est une fonctionnalité de prévisualisation technique dans la version Trident 24.10.

Fibre Channel est un protocole largement adopté dans les environnements de stockage d'entreprise en raison de ses performances élevées, de sa fiabilité et de son évolutivité. Il fournit un canal de communication robuste et efficace pour les périphériques de stockage, permettant des transferts de données rapides et sécurisés. En utilisant SCSI over Fibre Channel, vous pouvez exploiter leur infrastructure de stockage SCSI existante tout en bénéficiant des performances élevées et des capacités longue distance de Fibre Channel. Il permet de consolider les ressources de stockage et de créer des réseaux de stockage (SAN) évolutifs et efficaces, capables de gérer d'importants volumes de données à faible latence.

La fonctionnalité FC de Trident vous permet d'effectuer les opérations suivantes :

- Provisionnez les demandes de service virtuels de manière dynamique en fonction des spécifications de déploiement.
- Prenez des snapshots de volume et créez un nouveau volume à partir de l'instantané.
- Cloner une FC-PVC existante.
- Redimensionner un volume déjà déployé.

Prérequis

Configurez les paramètres réseau et nœud requis pour FC.

Paramètres réseau

1. Obtenez le WWPN des interfaces cibles. Pour plus d'informations, reportez-vous à la section "interface réseau affiche" .
2. Procurez-vous le WWPN pour les interfaces sur l'initiateur (hôte).

   Reportez-vous aux utilitaires correspondants du système d'exploitation hôte.

3. Configurer la segmentation sur le commutateur FC à l'aide des WWPN de l'hôte et de la cible.

   Pour plus d'informations, reportez-vous à la documentation du fournisseur du commutateur Respecive.

   Pour plus d'informations, reportez-vous à la documentation ONTAP suivante :

   - "Présentation de la segmentation Fibre Channel et FCoE"
   - "Manières de configurer FC ; hôtes SAN FC-NVMe"

Préparez le nœud de travail

Tous les nœuds workers du cluster Kubernetes doivent pouvoir monter les volumes provisionnés pour vos pods. Pour préparer les nœuds worker pour FC, vous devez installer les outils requis.

Installez les outils FC

Installez les outils FC à l'aide des commandes de votre système d'exploitation.

- Lors de l'utilisation de nœuds worker exécutant RHEL/RedHat CoreOS avec FC PVS, spécifiez la `discard` mountOption dans la classe de stockage pour effectuer la récupération d'espace en ligne. Reportez-vous à la "Documentation Red Hat".

RHEL 8+

1. Installez les packages système suivants :

```
sudo yum install -y lsscsi device-mapper-multipath
```

2. Activer les chemins d'accès multiples :

```
sudo mpathconf --enable --with_multipathd y --find_multipaths n
```

> Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

3. Assurez-vous que `multipathd` est en cours d'exécution :

```
sudo systemctl enable --now multipathd
```

Ubuntu

1. Installez les packages système suivants :

```
sudo apt-get install -y lsscsi sg3-utils multipath-tools scsitools
```

2. Activer les chemins d'accès multiples :

```
sudo tee /etc/multipath.conf <<-EOF
defaults {
    user_friendly_names yes
    find_multipaths no
}
EOF
sudo systemctl enable --now multipath-tools.service
sudo service multipath-tools restart
```

> Assurez-vous que `etc/multipath.conf` contient `find_multipaths no` moins de `defaults`.

3. Assurez-vous que `multipath-tools` est activé et en cours d'exécution :

```
sudo systemctl status multipath-tools
```

Créer une configuration back-end

Créez un backend Trident pour le `ontap-san` pilote et `fcp` comme sanType.

Se reporter à :

- "Préparez la configuration du système back-end avec les pilotes SAN ONTAP"
- "Options et exemples de configuration du SAN ONTAP"

Exemple de configuration back-end avec FC

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-san
spec:
  version: 1
  backendName: ontap-san-backend
  storageDriverName: ontap-san
  managementLIF: 10.0.0.1
  sanType: fcp
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-san-secret
```

Créer une classe de stockage

Pour plus d'informations, se reporter à :

- "Options de configuration du stockage"

Exemple de classe de stockage

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: fcp-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  storagePools: "ontap-san-backend:.*"
  fsType: "ext4"
allowVolumeExpansion: True
```