Tridentプロテクトのインストール

Trident

NetApp
November 14, 2025

目次

Tridentプロテクトのインストール

Trident保護の要件

まず、運用環境、アプリケーションクラスタ、アプリケーション、ライセンスの準備状況を確認します。Trident保護を導入して運用するには、環境がこれらの要件を満たしていることを確認してください。

TridentによるKubernetesクラスタ互換性の保護

Trident Protectは、次のようなフルマネージドおよび自己管理型の幅広いKubernetes製品と互換性があります。

- Amazon Elastic Kubernetes Service（EKS）
- Google Kubernetes Engine （ GKE ）
- Microsoft Azure Kubernetes Service （ AKS ）
- Red Hat OpenShift のサービスです
- SUSE Rancher
- VMware Tanzuポートフォリオ
- アップストリームKubernetes

- Trident Protect バックアップは、Linux コンピューティング ノードでのみサポートされます。 Windows コンピューティング ノードはバックアップ操作ではサポートされていません。
- Trident保護をインストールするクラスタに、実行中のSnapshotコントローラと関連するCRDが設定されていることを確認します。スナップショットコントローラを取り付けるには、を参照してください "以下の手順を参照して"。

Tridentはストレージバックエンドの互換性を保護

Trident保護は、次のストレージバックエンドをサポートします。

- NetApp ONTAP 対応の Amazon FSX
- Cloud Volumes ONTAP
- ONTAPストレエシアレイ
- Google Cloud NetAppボリューム
- Azure NetApp Files の特長

ストレージバックエンドが次の要件を満たしていることを確認します。

- クラスターに接続されている NetApp ストレージが Trident 24.02 以降を使用していることを確認します (Trident 24.10 を推奨)。
- NetApp ONTAPストレージバックエンドがあることを確認します。

- バックアップを格納するオブジェクトストレージバケットを設定しておきます。
- アプリケーションまたはアプリケーションデータの管理処理に使用するアプリケーションネームスペースを作成します。Trident保護では、これらのネームスペースは作成されません。カスタムリソースに存在しないネームスペースを指定すると、処理は失敗します。

NASエコノミーボリュームの要件

Trident Protectは、NASエコノミーボリュームへのバックアップおよびリストア処理をサポートします。Snapshot、クローン、NASエコノミーボリュームへのSnapMirrorレプリケーションは、現在サポートされていません。Trident保護で使用するNASエコノミーボリュームごとに、スナップショットディレクトリを有効にする必要があります。

一部のアプリケーションは、Snapshotディレクトリを使用するボリュームと互換性がありません。これらのアプリケーションでは、ONTAPストレージシステムで次のコマンドを実行して、snapshotディレクトリを非表示にする必要があります。

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

snapshotディレクトリを有効にするには、NASエコノミーボリュームごとに次のコマンドを実行し、を変更するボリュームのUUIDに置き換え `<volume-UUID>`ます。

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

新しいボリュームに対してSnapshotディレクトリをデフォルトで有効にするには、Tridentバックエンド構成オプションをに `true`設定し `snapshotDir`ます。既存のボリュームには影響しません。

KubeVirt VMによるデータ保護

Trident Protect は、データ保護操作中に KubeVirt 仮想マシンのファイルシステムのフリーズおよびアンフリーズ機能を提供して、データの一貫性を確保します。VM フリーズ操作の構成方法とデフォルトの動作はTrident Protect のバージョンによって異なり、新しいリリースでは Helm チャート パラメータを通じて簡素化された構成が提供されています。

復元操作中は、 `VirtualMachineSnapshots`仮想マシン (VM) 用に作成されたものは復元されません。

Trident Protect 25.10以降

Trident Protect は、データ保護操作中に KubeVirt ファイルシステムを自動的にフリーズおよびアンフリーズして一貫性を確保します。Trident protect 25.10以降では、 `vm.freeze` Helm チャート インストール時のパラメーター。このパラメータはデフォルトで有効になっています。

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

Tridentプロテクト 24.10.1 から 25.06

Trident protect 24.10.1以降では、Trident protectでは、データ保護処理中にKubeVirtファイルシステムが自動的にフリーズおよびフリーズ解除されます。必要に応じて、次のコマンドを使用してこの自動動作を無効にできます。

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

Trident保護24.10

Trident protect 24.10では、データ保護処理中にKubeVirt VMファイルシステムの一貫した状態が自動的に保証されません。Trident protect 24.10を使用してKubeVirt VMデータを保護する場合は、データ保護処理の前にファイルシステムのフリーズ/フリーズ解除機能を手動で有効にする必要があります。これにより、ファイルシステムが一貫した状態であることが保証されます。

データ保護処理中のVMファイルシステムのフリーズおよびフリーズ解除を管理するようにTrident protect 24.10を設定するには、"仮想化の設定"次のコマンドを使用します。

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

SnapMirrorレプリケーションの要件

NetApp SnapMirrorレプリケーションは、次のONTAPソリューションのTrident protectで使用できます。

- オンプレミスのNetApp FAS、AFF、ASAクラスタ
- NetApp ONTAP Select の略
- NetApp Cloud Volumes ONTAP の略
- NetApp ONTAP 対応の Amazon FSX

SnapMirrorレプリケーション用のONTAPクラスタの要件

SnapMirrorレプリケーションを使用する場合は、ONTAPクラスタが次の要件を満たしていることを確認しま

す。

- **NetApp Trident**: NetApp Trident は、ONTAP をバックエンドとして使用するソース Kubernetes クラスターと宛先 Kubernetes クラスターの両方に存在する必要があります。Trident保護では、次のドライバに基づくストレージクラスを使用したNetApp SnapMirrorテクノロジによるレプリケーションがサポートされます。
  - `ontap-nas` : NFS
  - `ontap-san` : iSCSI
  - `ontap-san` : FC
  - `ontap-san` : NVMe/TCP (最低でも ONTAP バージョン 9.15.1 が必要)
- ライセンス：Data Protection Bundleを使用するONTAP SnapMirror非同期ライセンスが、ソースとデスティネーションの両方のONTAPクラスタで有効になっている必要があります。詳細については、を参照してください "ONTAP のSnapMirrorライセンスの概要" 。

  ONTAP 9.10.1 以降、すべてのライセンスは、複数の機能を有効にする単一のファイルである NetApp ライセンス ファイル (NLF) として提供されます。詳細については、を参照してください "ONTAP Oneに含まれるライセンス" 。

  SnapMirror 非同期保護のみがサポートされます。

SnapMirrorレプリケーションのピアリングに関する考慮事項

ストレージバックエンドピアリングを使用する場合は、環境が次の要件を満たしていることを確認してください。

- *クラスタとSVM *：ONTAPストレージバックエンドにピア関係が設定されている必要があります。詳細については、を参照してください "クラスタと SVM のピアリングの概要" 。

  2つのONTAPクラスタ間のレプリケーション関係で使用されるSVM名が一意であることを確認してください。

- **NetApp Trident** と **SVM**: ピアリングされたリモート SVM は、宛先クラスタ上の NetApp Trident で使用できる必要があります。
- 管理バックエンド：レプリケーション関係を作成するには、Trident保護でONTAPストレージバックエンドを追加および管理する必要があります。

SnapMirrorレプリケーション用の**Trident / ONTAP**の設定

Trident保護を使用するには、ソースとデスティネーションの両方のクラスタのレプリケーションをサポートするストレージバックエンドを少なくとも1つ設定する必要があります。ソースクラスタとデスティネーションクラスタが同じである場合は、耐障害性を最大限に高めるために、デスティネーションアプリケーションでソースアプリケーションとは別のストレージバックエンドを使用する必要があります。

SnapMirrorレプリケーションの**Kubernetes**クラスタ要件

Kubernetes クラスターが次の要件を満たしていることを確認します。

- **AppVault** のアクセシビリティ: アプリケーション オブジェクトのレプリケーションでは、ソース クラス

ターと宛先クラスターの両方に、AppVault の読み取りと書き込みを行うためのネットワーク アクセスが必要です。

- ネットワーク接続: ファイアウォール ルール、バケット権限、IP 許可リストを構成して、WAN を介した両方のクラスターと AppVault 間の通信を有効にします。

> 多くの企業環境では、WAN 接続全体に厳格なファイアウォール ポリシーが実装されています。レプリケーションを構成する前に、インフラストラクチャ チームとこれらのネットワーク要件を確認してください。

Trident保護のインストールと設定

ご使用の環境がTrident保護の要件を満たしている場合は、次の手順に従ってクラスタにTrident保護をインストールします。NetAppからTrident protectを取得するか、独自のプライベートレジストリからインストールできます。プライベートレジストリからインストールすると、クラスタがインターネットにアクセスできない場合に役立ちます。

Tridentプロテクトのインストール

Trident protect from NetAppのインストール

手順

1. Trident Helmリポジトリを追加します。

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

2. Helmを使用してTrident protectをインストールします。をクラスタ名に置き換えます `<name-of-cluster>`。クラスタに割り当てられ、クラスタのバックアップとスナップショットの識別に使用されます。

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

3. オプションで、デバッグ ログを有効にするには (トラブルシューティングに推奨)、次のコマンドを使用します。

```
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
```

デバッグ ログにより、 NetAppサポートは、ログ レベルの変更や問題の再現を必要とせずに、問題のトラブルシューティングを行うことができます。

Trident protectをプライベートレジストリからインストールする

Kubernetesクラスタがインターネットにアクセスできない場合は、プライベートイメージレジストリからTrident protectをインストールできます。次の例では、括弧内の値を環境の情報に置き換えます。

手順

1. 次のイメージをローカルマシンにプルし、タグを更新して、プライベートレジストリにプッシュします。

```
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/exechook: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
```

例：

```
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
```

> Helmチャートを取得するには、まずインターネットにアクセスできるマシンにHelmチャートをダウンロードします。 `helm pull trident-protect --version 100.2510.0 --repo https://netapp.github.io/trident-protect-helm-chart`をコピーし、その結果を `trident-protect-100.2510.0.tgz` ファイルをオフライン環境にアップロードし、 `helm install trident-protect ./trident-protect-100.2510.0.tgz` 最後のステップのリポジトリ参照の代わりに使用します。

2. Trident protect systemネームスペースを作成します。

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

3. レジストリにログインします。

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

4. プライベートレジストリ認証に使用するプルシークレットを作成します。

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

5. Trident Helmリポジトリを追加します。

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

6. という名前のファイルを作成します `protectValues.yaml`。次のTrident保護設定が含まれていることを確認します。

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

> その `imageRegistry`そして `imagePullSecrets`値は、以下のすべてのコンポーネント画像に適用されます。 `resourcebackup`そして `resourcerestore`。レジストリ内の特定のリポジトリパスにイメージをプッシュする場合（例：`example.com:443/my-repo`) の場合は、レジストリ フィールドに完全なパスを含めます。これにより、すべての画像が `<private-registry-url>/<image-name>:<tag>`。

7. Helmを使用してTrident protectをインストールします。をクラスタ名に置き換えます `<name_of_cluster>`。クラスタに割り当てられ、クラスタのバックアップとスナップショットの識別に使用されます。

```
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. オプションで、デバッグ ログを有効にするには (トラブルシューティングに推奨)、次のコマンドを使用します。

```
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
```

デバッグ ログにより、 NetAppサポートは、ログ レベルの変更や問題の再現を必要とせずに、問題のトラブルシューティングを行うことができます。

AutoSupport設定や名前空間フィルタリングなどのHelmチャートの追加設定オプションについては、以下を参照してください。 "Trident保護インストールのカスタマイズ"。

Trident保護CLIプラグインのインストール

Tridentユーティリティの拡張機能であるTrident protectコマンドラインプラグインを使用すると、Trident protectカスタムリソース（CRS）を作成して操作できます `tridentctl`。

Trident保護CLIプラグインのインストール

コマンドラインユーティリティを使用する前に、クラスタへのアクセスに使用するマシンにインストールする必要があります。マシンがx64またはARM CPUを使用しているかどうかに応じて、次の手順を実行します。

Linux AMD64 CPU用プラグインのダウンロード

手順

1. Trident保護CLIプラグインをダウンロードします。

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.10.0/tridentctl-protect-linux-amd64
```

Linux ARM64 CPU用プラグインのダウンロード

手順

1. Trident保護CLIプラグインをダウンロードします。

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.10.0/tridentctl-protect-linux-arm64
```

Mac AMD64 CPU用プラグインのダウンロード

手順

1. Trident保護CLIプラグインをダウンロードします。

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.10.0/tridentctl-protect-macos-amd64
```

Mac ARM64 CPU用プラグインのダウンロード

手順

1. Trident保護CLIプラグインをダウンロードします。

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/25.10.0/tridentctl-protect-macos-arm64
```

1. プラグインバイナリの実行権限を有効にします。

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

2. プラグインバイナリをPATH変数で定義されている場所にコピーします。たとえば、 `/usr/bin`または `/usr/local/bin`（昇格されたPrivilegesが必要な場合があります）。

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

3. 必要に応じて、プラグインバイナリをホームディレクトリ内の場所にコピーできます。この場合、locationがPATH変数の一部であることを確認することをお勧めします。

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

プラグインをPATH変数の場所にコピーすると、任意の場所からまたはを `tridentctl protect`入力してプラグインを使用でき `tridentctl-protect`ます。

Trident CLIプラグインのヘルプを表示

組み込みプラグインヘルプ機能を使用して、プラグインの機能に関する詳細なヘルプを表示できます。

手順

1. ヘルプ機能を使用して、使用方法に関するガイダンスを表示します。

```
tridentctl-protect help
```

コマンドの自動補完を有効にする

Trident保護CLIプラグインをインストールしたあとで、特定のコマンドの自動補完を有効にすることができます。

Bashシェルの自動補完を有効にする

手順

1. 完了スクリプトを作成します。

```
tridentctl-protect completion bash > tridentctl-completion.bash
```

2. ホームディレクトリにスクリプトを格納する新しいディレクトリを作成します。

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

3. ダウンロードしたスクリプトをディレクトリに移動し `~/.bash/completions`ます。

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

4. ホームディレクトリ内のファイルに次の行を追加し `~/.bashrc`ます。

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

Zシェルの自動補完を有効にする

手順

1. 完了スクリプトを作成します。

```
tridentctl-protect completion zsh > tridentctl-completion.zsh
```

2. ホームディレクトリにスクリプトを格納する新しいディレクトリを作成します。

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

3. ダウンロードしたスクリプトをディレクトリに移動し `~/.zsh/completions`ます。

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

4. ホームディレクトリ内のファイルに次の行を追加し `~/.zprofile`ます。

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

結果

次のシェルログイン時に、tridentctl-protectプラグインで自動補完コマンドを使用できます。

Trident保護インストールのカスタマイズ

Trident保護のデフォルト設定をカスタマイズして、環境の特定の要件を満たすことができます。

Trident保護コンテナのリソース制限を指定

Trident保護のインストール後に、構成ファイルを使用してTrident保護コンテナのリソース制限を指定できます。リソース制限を設定すると、Trident保護処理で消費されるクラスタのリソースの量を制御できます。

手順

1. という名前のファイルを作成します `resourceLimits.yaml`。
2. 環境のニーズに応じて、Trident保護コンテナのリソース制限オプションをファイルに入力します。

   次の構成ファイルの例は、使用可能な設定を示しています。このファイルには、各リソース制限のデフォルト値が含まれています。

```
---
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. ファイルから値を適用し `resourceLimits.yaml`ます。

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

セキュリティコンテキスト制約のカスタマイズ

Tridentプロテクトのインストール後、構成ファイルを使用して、TridentプロテクトコンテナのOpenShift Security Context Constraint（SCC；セキュリティコンテキスト制約）を変更できます。これらの制約により、Red Hat OpenShiftクラスタ内のポッドのセキュリティ制限が定義されます。

手順

1. という名前のファイルを作成します `sccconfig.yaml`。
2. SCCオプションをファイルに追加し、環境のニーズに応じてパラメータを変更します。

   次に、SCCオプションのパラメータのデフォルト値の例を示します。

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

次の表では、SCCオプションのパラメータについて説明します。

パラメータ	説明	デフォルト
作成	SCCリソースを作成できるかどうかを決定します。SCCリソースは、がに設定され `true`、Helmのインストールプロセスでの場合にのみ作成されOpenShift環境が指定されている `scc.create`ます。`OpenShift`で動作していない場合、またはがに設定されている `false`場合 `scc.create`、SCCリソースは作成されません。	正しいです
名前	SCCの名前を指定します。	Trident - protect-job
優先度	SCCのプライオリティを定義します。優先度の高いSCCSは、低い値のSCCSよりも先に評価されます。	1

3. ファイルから値を適用し `sccconfig.yaml`ます。

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

これにより、デフォルト値がファイルで指定された値に置き換えられ `sccconfig.yaml`ます。

追加のTrident Protect Helm チャート設定を構成する

特定の要件に合わせて、 AutoSupport設定と名前空間フィルタリングをカスタマイズできます。次の表は、使用可能な構成パラメータを示しています。

パラメータ	を入力します	説明
自動サポートプロキシ	文字列	NetApp AutoSupport接続用のプロキシ URL を構成します。これを使用して、サポート バンドルのアップロードをプロキシ サーバー経由でルーティングします。例： `http://my.proxy.url` 。

パラメータ	を入力します	説明
autoSupport.insecure	ブール値	設定すると、 AutoSupportプロキシ接続のTLS検証をスキップします。 `true` 。安全でないプロキシ接続にのみ使用してください。 （デフォルト： `false` ）
自動サポートが有効	ブール値	毎日のTrident Protect AutoSupportバンドルのアップロードを有効または無効にします。に設定すると `false`、スケジュールされた毎日のアップロードは無効になっていますが、サポート バンドルを手動で生成することはできます。 （デフォルト： `true` ）
スキップ名前空間注釈の復元	文字列	バックアップおよび復元操作から除外する名前空間注釈のコンマ区切りリスト。注釈に基づいて名前空間をフィルタリングできます。
スキップ名前空間ラベルの復元	文字列	バックアップおよび復元操作から除外する名前空間ラベルのコンマ区切りリスト。ラベルに基づいて名前空間をフィルタリングできます。

これらのオプションは、YAML 構成ファイルまたはコマンドライン フラグを使用して構成できます。

YAMLファイルを使用する

手順

1. 設定ファイルを作成し、名前を付けます `values.yaml`。
2. 作成したファイルに、カスタマイズする構成オプションを追加します。

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

3. 入力したら `values.yaml`正しい値を持つファイルの場合は、構成ファイルを適用します。

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

CLIフラグを使用する

手順

1. 次のコマンドを `--set`個々のパラメータを指定するためのフラグ:

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

Trident保護ポッドを特定のノードに制限する

KubernetesのnodeSelectorノード選択制約を使用すると、ノードラベルに基づいて、Trident保護ポッドを実行できるノードを制御できます。デフォルトでは、Trident保護はLinuxを実行しているノードに制限されます。必要に応じて、これらの制約をさらにカスタマイズできます。

手順

1. という名前のファイルを作成します `nodeSelectorConfig.yaml`。
2. nodeSelectorオプションをファイルに追加し、ファイルを変更してノードラベルを追加または変更して、環境のニーズに応じて制限します。たとえば、次のファイルにはデフォルトのOS制限が含まれていますが、特定の地域とアプリ名も対象としています。

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

3. ファイルから値を適用し `nodeSelectorConfig.yaml`ます。

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

これにより、デフォルトの制限がファイルで指定した制限に置き換えられます `nodeSelectorConfig.yaml`。

著作権に関する情報

商標に関する情報