Gérer Trident Protect

Trident

NetApp
February 02, 2026

Sommaire

Gérer Trident Protect

Gérer l’autorisation et le contrôle d’accès de Trident Protect

Trident Protect utilise le modèle Kubernetes de contrôle d’accès basé sur les rôles (RBAC). Par défaut, Trident Protect fournit un seul espace de noms système et son compte de service par défaut associé. Si votre organisation compte de nombreux utilisateurs ou des besoins de sécurité spécifiques, vous pouvez utiliser les fonctionnalités RBAC de Trident Protect pour obtenir un contrôle plus précis sur l’accès aux ressources et aux espaces de noms.

L’administrateur du cluster a toujours accès aux ressources de l’espace de noms par défaut `trident-protect` et peut également accéder aux ressources de tous les autres espaces de noms. Pour contrôler l’accès aux ressources et aux applications, vous devez créer des espaces de noms supplémentaires et ajouter des ressources et des applications à ces espaces de noms.

Notez qu’aucun utilisateur ne peut créer de CRS de gestion des données d’application dans l’espace de noms par défaut `trident-protect`. Vous devez créer une CRS de gestion des données d’application dans un espace de noms d’application (pour cela, il est recommandé de créer une CRS de gestion des données d’application dans le même espace de nom que l’application associée).

> Seuls les administrateurs devraient avoir accès aux objets de ressources personnalisés privilégiés de Trident Protect, notamment :
>
> - **AppVault** : nécessite les données d’informations d’identification du compartiment
> - **AutoSupportBundle** : Collecte les métriques, les journaux et autres données sensibles de Trident Protect
> - **AutoSupportBundleSchedule** : gère les plannings de collecte de journaux
>
> Comme bonne pratique, utilisez RBAC pour limiter l’accès aux objets privilégiés aux administrateurs.

Pour plus d’informations sur la façon dont RBAC réglemente l’accès aux ressources et aux espaces de noms, reportez-vous à la section "Documentation Kubernetes RBAC" .

Pour plus d’informations sur les comptes de service, reportez-vous au "Documentation du compte de service Kubernetes".

Exemple : gestion de l’accès pour deux groupes d’utilisateurs

Par exemple, une organisation dispose d’un administrateur de cluster, d’un groupe d’utilisateurs techniques et d’un groupe d’utilisateurs marketing. L’administrateur du cluster doit effectuer les tâches suivantes pour créer un environnement dans lequel le groupe d’ingénierie et le groupe marketing ont chacun accès uniquement aux ressources affectées à leurs espaces de noms respectifs.

Étape 1 : créez un espace de noms pour contenir des ressources pour chaque groupe

La création d’un espace de noms vous permet de séparer logiquement les ressources et de mieux contrôler qui a accès à ces ressources.

Étapes

1. Créer un espace de nom pour le groupe d'ingénierie :

```
kubectl create ns engineering-ns
```

2. Créez un espace de nom pour le groupe marketing :

```
kubectl create ns marketing-ns
```

Étape 2 : créez de nouveaux comptes de service pour interagir avec les ressources de chaque espace de noms

Chaque nouvel espace de noms que vous créez est fourni avec un compte de service par défaut, mais vous devez créer un compte de service pour chaque groupe d'utilisateurs afin de pouvoir diviser davantage Privileges entre les groupes si nécessaire.

Étapes

1. Créer un compte de service pour le groupe d'ingénierie :

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: eng-user
  namespace: engineering-ns
```

2. Créez un compte de service pour le groupe marketing :

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: mkt-user
  namespace: marketing-ns
```

Étape 3 : créez un secret pour chaque nouveau compte de service

Un secret de compte de service est utilisé pour s'authentifier auprès du compte de service et peut facilement être supprimé et recréé si compromis.

Étapes

1. Créez un secret pour le compte de service d'ingénierie :

```
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: eng-user
  name: eng-user-secret
  namespace: engineering-ns
type: kubernetes.io/service-account-token
```

2. Créez un secret pour le compte de service marketing :

```
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: mkt-user
  name: mkt-user-secret
  namespace: marketing-ns
type: kubernetes.io/service-account-token
```

Étape 4 : créez un objet RoleBinding pour lier l'objet ClusterRole à chaque nouveau compte de service

Un objet ClusterRole par défaut est créé lors de l'installation de Trident Protect. Vous pouvez lier ce ClusterRole au compte de service en créant et en appliquant un objet RoleBinding.

Étapes

1. Liez ClusterRole au compte de service d'ingénierie :

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: engineering-ns-tenant-rolebinding
  namespace: engineering-ns
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-protect-tenant-cluster-role
subjects:
- kind: ServiceAccount
  name: eng-user
  namespace: engineering-ns
```

2. Associez ClusterRole au compte de service marketing :

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: marketing-ns-tenant-rolebinding
  namespace: marketing-ns
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-protect-tenant-cluster-role
subjects:
- kind: ServiceAccount
  name: mkt-user
  namespace: marketing-ns
```

Étape 5 : autorisations de test

Vérifiez que les autorisations sont correctes.

Étapes

1. Vérifier que les utilisateurs d'ingénierie peuvent accéder aux ressources d'ingénierie :

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get applications.protect.trident.netapp.io -n engineering-ns
```

2. Vérifiez que les utilisateurs d'ingénierie ne peuvent pas accéder aux ressources marketing :

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get applications.protect.trident.netapp.io -n marketing-ns
```

Étape 6 : accorder l'accès aux objets AppVault

Pour effectuer des tâches de gestion des données telles que les sauvegardes et les snapshots, l'administrateur du cluster doit accorder l'accès aux objets AppVault à des utilisateurs individuels.

Étapes

1. Créez et appliquez un fichier YAML de combinaison AppVault et secret qui accorde à un utilisateur l'accès à un AppVault. Par exemple, la CR suivante accorde l'accès à un AppVault à l'utilisateur `eng-user`:

```
apiVersion: v1
data:
  accessKeyID: <ID_value>
  secretAccessKey: <key_value>
kind: Secret
metadata:
  name: appvault-for-eng-user-only-secret
  namespace: trident-protect
type: Opaque
---
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: appvault-for-eng-user-only
  namespace: trident-protect # Trident Protect system namespace
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: testbucket
      endpoint: 192.168.0.1:30000
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-for-eng-user-only-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-for-eng-user-only-secret
  providerType: GenericS3
```

2. Créez et appliquez une CR de rôle pour permettre aux administrateurs de cluster d'accorder l'accès à des ressources spécifiques dans un espace de noms. Par exemple :

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: eng-user-appvault-reader
  namespace: trident-protect
rules:
- apiGroups:
  - protect.trident.netapp.io
  resourceNames:
  - appvault-for-enguser-only
  resources:
  - appvaults
  verbs:
  - get
```

3. Créez et appliquez une CR RoleBinding pour lier les autorisations à l'utilisateur eng-user. Par exemple :

```
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: eng-user-read-appvault-binding
  namespace: trident-protect
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: eng-user-appvault-reader
subjects:
- kind: ServiceAccount
  name: eng-user
  namespace: engineering-ns
```

4. Vérifiez que les autorisations sont correctes.

   a. Tentative de récupération des informations d'objet AppVault pour tous les espaces de noms :

   ```
   kubectl get appvaults -n trident-protect
   --as=system:serviceaccount:engineering-ns:eng-user
   ```

   Vous devez voir les résultats similaires à ce qui suit :

```
Error from server (Forbidden): appvaults.protect.trident.netapp.io is
forbidden: User "system:serviceaccount:engineering-ns:eng-user"
cannot list resource "appvaults" in API group
"protect.trident.netapp.io" in the namespace "trident-protect"
```

b. Testez pour voir si l'utilisateur peut obtenir les informations AppVault qu'il a maintenant l'autorisation d'accéder :

```
kubectl auth can-i --as=system:serviceaccount:engineering-ns:eng-user
get appvaults.protect.trident.netapp.io/appvault-for-eng-user-only -n
trident-protect
```

Vous devez voir les résultats similaires à ce qui suit :

```
yes
```

Résultat

Les utilisateurs auxquels vous avez accordé des autorisations AppVault doivent pouvoir utiliser des objets AppVault autorisés pour les opérations de gestion des données applicatives et ne doivent pas pouvoir accéder à des ressources en dehors des espaces de noms attribués ou créer de nouvelles ressources auxquelles ils n'ont pas accès.

Surveiller les ressources de Trident Protect

Vous pouvez utiliser les outils open source kube-state-metrics, Prometheus et Alertmanager pour surveiller l'état des ressources protégées par Trident Protect.

Le service kube-state-metrics génère des métriques à partir des communications de l'API Kubernetes. Son utilisation conjointe avec Trident Protect permet d'obtenir des informations utiles sur l'état des ressources de votre environnement.

Prometheus est une boîte à outils capable d'ingérer les données générées par kube-state-metrics et de les présenter sous forme d'informations facilement lisibles sur ces objets. Ensemble, kube-state-metrics et Prometheus vous permettent de surveiller l'état et la santé des ressources que vous gérez avec Trident Protect.

AlertManager est un service qui ingère les alertes envoyées par des outils tels que Prometheus et les redirige vers les destinations que vous configurez.

Les configurations et les conseils inclus dans ces étapes ne sont que des exemples ; vous devez les personnaliser en fonction de votre environnement. Reportez-vous à la documentation officielle suivante pour obtenir des instructions et une assistance spécifiques :

- "documentation sur les indicateurs d'état kube"
- "Documentation Prometheus"
- "Documentation d'AlertManager"

Étape 1 : installez les outils de surveillance

Pour activer la surveillance des ressources dans Trident Protect, vous devez installer et configurer kube-state-metrics, Promethus et Alertmanager.

Installez les indicateurs kube-state

Vous pouvez installer kube-state-metrics à l'aide de Helm.

Étapes

1. Ajoutez le graphique Helm kube-state-metrics. Par exemple :

```
helm repo add prometheus-community https://prometheus-
community.github.io/helm-charts
helm repo update
```

2. Appliquez le CRD Prometheus ServiceMonitor au cluster :

```
kubectl apply -f https://raw.githubusercontent.com/prometheus-
operator/prometheus-operator/main/example/prometheus-operator-
crd/monitoring.coreos.com_servicemonitors.yaml
```

3. Créez un fichier de configuration pour le graphique Helm (par exemple, `metrics-config.yaml`). Vous pouvez personnaliser l'exemple de configuration suivant en fonction de votre environnement :

Metrics-config.yaml : configuration du graphique Helm kube-state-metrics

```
---
extraArgs:
  # Collect only custom metrics
  - --custom-resource-state-only=true

customResourceState:
  enabled: true
  config:
    kind: CustomResourceStateMetrics
    spec:
      resources:
      - groupVersionKind:
          group: protect.trident.netapp.io
          kind: "Backup"
          version: "v1"
        labelsFromPath:
          backup_uid: [metadata, uid]
          backup_name: [metadata, name]
          creation_time: [metadata, creationTimestamp]
        metrics:
        - name: backup_info
          help: "Exposes details about the Backup state"
          each:
            type: Info
            info:
              labelsFromPath:
                appVaultReference: ["spec", "appVaultRef"]
                appReference: ["spec", "applicationRef"]
rbac:
  extraRules:
  - apiGroups: ["protect.trident.netapp.io"]
    resources: ["backups"]
    verbs: ["list", "watch"]

# Collect metrics from all namespaces
namespaces: ""

# Ensure that the metrics are collected by Prometheus
prometheus:
  monitor:
    enabled: true
```

4. Installez les indicateurs d'état kube en déployant le graphique Helm. Par exemple :

```
helm install custom-resource -f metrics-config.yaml prometheus-
community/kube-state-metrics --version 5.21.0
```

5. Configurez kube-state-metrics pour générer des métriques pour les ressources personnalisées utilisées par Trident Protect en suivant les instructions du guide. "documentation sur les ressources personnalisées kube-state-metrics" .

Installez Prometheus

Vous pouvez installer Prometheus en suivant les instructions de la "Documentation Prometheus".

Installez AlertManager

Vous pouvez installer AlertManager en suivant les instructions de la "Documentation d'AlertManager".

Étape 2 : configurer les outils de surveillance pour qu'ils fonctionnent ensemble

Après avoir installé les outils de surveillance, vous devez les configurer pour qu'ils fonctionnent ensemble.

Étapes

1. Intégrez des metrics kube-state avec Prometheus. Modifiez le fichier de configuration Prometheus (`prometheus.yaml`) et ajoutez les informations du service kube-state-metrics. Par exemple :

   prometheus.yaml : intégration du service kube-state-metrics avec Prometheus

```
---
apiVersion: v1
kind: ConfigMap
metadata:
  name: prometheus-config
  namespace: trident-protect
data:
  prometheus.yaml: |
    global:
      scrape_interval: 15s
    scrape_configs:
      - job_name: 'kube-state-metrics'
        static_configs:
          - targets: ['kube-state-metrics.trident-protect.svc:8080']
```

2. Configurez Prometheus pour acheminer les alertes vers AlertManager. Modifiez le fichier de configuration Prometheus (`prometheus.yaml`) et ajoutez la section suivante :

prometheus.yaml : envoyer des alertes à Alertmanager

```
alerting:
  alertmanagers:
    - static_configs:
        - targets:
            - alertmanager.trident-protect.svc:9093
```

Résultat

Prometheus peut désormais collecter des metrics à partir de metrics kube-state et envoyer des alertes à AlertManager. Vous êtes maintenant prêt à configurer les conditions qui déclenchent une alerte et l'emplacement où les alertes doivent être envoyées.

Étape 3 : configuration des alertes et des destinations d'alertes

Une fois que vous avez configuré les outils pour qu'ils fonctionnent ensemble, vous devez configurer le type d'informations qui déclenche des alertes et l'emplacement où elles doivent être envoyées.

Exemple d'alerte : échec de la sauvegarde

L'exemple suivant définit une alerte critique qui est déclenchée lorsque l'état de la ressource personnalisée de sauvegarde est défini sur `Error` pendant 5 secondes ou plus. Vous pouvez personnaliser cet exemple pour l'adapter à votre environnement et inclure cet extrait YAML dans votre `prometheus.yaml` fichier de configuration :

rules.yaml : définir une alerte Prometheus pour les sauvegardes ayant échoué

```
rules.yaml: |
  groups:
    - name: fail-backup
        rules:
          - alert: BackupFailed
            expr: kube_customresource_backup_info{status="Error"}
            for: 5s
            labels:
              severity: critical
            annotations:
              summary: "Backup failed"
              description: "A backup has failed."
```

Configurez AlertManager pour envoyer des alertes à d'autres canaux

Vous pouvez configurer AlertManager pour envoyer des notifications à d'autres canaux, tels que les e-mails, PagerDuty, Microsoft Teams ou d'autres services de notification en spécifiant la configuration respective dans le `alertmanager.yaml` fichier.

L'exemple suivant configure AlertManager pour envoyer des notifications à un canal Slack. Pour personnaliser cet exemple en fonction de votre environnement, remplacez la valeur de la `api_url` clé par l'URL Slack

webhook utilisée dans votre environnement :

alertmanager.yaml : envoyer des alertes à un canal Slack

```
data:
  alertmanager.yaml: |
    global:
      resolve_timeout: 5m
    route:
      receiver: 'slack-notifications'
    receivers:
      - name: 'slack-notifications'
        slack_configs:
          - api_url: '<your-slack-webhook-url>'
            channel: '#failed-backups-channel'
            send_resolved: false
```

Générer un ensemble de support Trident Protect

Trident Protect permet aux administrateurs de générer des ensembles contenant des informations utiles au support NetApp , notamment des journaux, des métriques et des informations de topologie sur les clusters et les applications gérés. Si vous êtes connecté à Internet, vous pouvez télécharger des bundles de support sur le site de support NetApp (NSS) à l'aide d'un fichier de ressources personnalisé (CR).

Créez un bundle de support à l'aide d'une CR

Étapes

1. Créez le fichier de ressource personnalisée (CR) et nommez-le (par exemple, `trident-protect-support-bundle.yaml`).
2. Configurez les attributs suivants :
   - **metadata.name**: (*required*) le nom de cette ressource personnalisée; choisissez un nom unique et sensible pour votre environnement.
   - **Spec.triggerType**: (*required*) détermine si le bundle de support est généré immédiatement ou planifié. La génération planifiée du bundle a lieu à 12 h UTC. Valeurs possibles :
     - Planifié
     - Manuel
   - **Spec.uploadEnabled**: (*Optional*) détermine si le bundle de support doit être téléchargé sur le site de support NetApp après sa génération. Si ce n'est pas le cas, la valeur par défaut est `false` . Valeurs possibles :
     - vrai
     - false (valeur par défaut)
   - **Spec.dataWindowStart**: (*Optional*) chaîne de date au format RFC 3339 qui spécifie la date et l'heure auxquelles la fenêtre des données incluses dans le paquet de support doit commencer. Si ce n'est pas le cas, la valeur par défaut est de 24 heures. La date de fenêtre la plus ancienne que vous pouvez spécifier est il y a 7 jours.

     Exemple YAML :

```
---
apiVersion: protect.trident.netapp.io/v1
kind: AutoSupportBundle
metadata:
  name: trident-protect-support-bundle
spec:
  triggerType: Manual
  uploadEnabled: true
  dataWindowStart: 2024-05-05T12:30:00Z
```

3. Après avoir rempli le `trident-protect-support-bundle.yaml` fichier avec les valeurs correctes, appliquez le CR :

```
kubectl apply -f trident-protect-support-bundle.yaml -n trident-protect
```

Créez un bundle de support à l'aide de l'interface de ligne de commande

Étapes

1. Créez le pack de support en remplaçant les valeurs entre parenthèses par les informations de votre

environnement. `trigger-type`Détermine si le bundle est créé immédiatement ou si l'heure de création est déterminée par le planning, et peut être `Manual` ou `Scheduled`. Le paramètre par défaut est `Manual`.

Par exemple :

```
tridentctl-protect create autosupportbundle <my-bundle-name>
--trigger-type <trigger-type> -n trident-protect
```

Surveiller et récupérer le pack de support

Après avoir créé un bundle de support à l'aide de l'une ou l'autre méthode, vous pouvez surveiller sa progression de génération et le récupérer sur votre système local.

Étapes

1. Attendez le `status.generationState` atteindre `Completed` État. Vous pouvez surveiller la progression de la génération avec la commande suivante :

   ```
   kubectl get autosupportbundle trident-protect-support-bundle -n trident-protect
   ```

2. Récupérez le pack de support sur votre système local. Obtenez la commande de copie à partir du bundle AutoSupport terminé :

   ```
   kubectl describe autosupportbundle trident-protect-support-bundle -n trident-protect
   ```

   Trouver le `kubectl cp` commande à partir de la sortie et exécutez-la, en remplaçant l'argument de destination par votre répertoire local préféré.

Amélioration de Trident Protect

Vous pouvez mettre à jour Trident Protect vers la dernière version pour bénéficier des nouvelles fonctionnalités ou des correctifs de bugs.

- Lors d'une mise à niveau depuis la version 24.10, les snapshots exécutés pendant la mise à niveau peuvent échouer. Cet échec n'empêche pas la création de futurs snapshots, qu'ils soient manuels ou planifiés. Si un snapshot échoue pendant la mise à niveau, vous pouvez en créer un manuellement pour garantir la protection de votre application.

  Pour éviter d'éventuels échecs, vous pouvez désactiver toutes les planifications d'instantanés avant la mise à niveau et les réactiver ensuite. Cependant, cela entraînera l'absence d'instantanés planifiés pendant la période de mise à niveau.

- Pour les installations de registre privé, assurez-vous que le graphique Helm et les images requis pour la version cible sont disponibles dans votre registre privé et vérifiez que vos valeurs Helm personnalisées sont compatibles avec la nouvelle version du graphique. Pour plus d'informations, veuillez consulter"Installez Trident Protect à partir d'un registre privé" .

Pour mettre à niveau Trident Protect, procédez comme suit.

Étapes

1. Mettez à jour le référentiel Trident Helm :

```
helm repo update
```

2. Mettez à niveau les CRD Trident Protect :

   Cette étape est nécessaire si vous effectuez une mise à niveau depuis une version antérieure à la 25.06, car les CRD sont désormais inclus dans le tableau Trident Protect Helm.

   a. Exécutez cette commande pour déplacer la gestion des CRD de `trident-protect-crds` à `trident-protect` :

```
kubectl get crd | grep protect.trident.netapp.io | awk '{print $1}' |
xargs -I {} kubectl patch crd {} --type merge -p '{"metadata":
{"annotations":{"meta.helm.sh/release-name": "trident-protect"}}}'
```

   b. Exécutez cette commande pour supprimer le secret Helm pour le `trident-protect-crds` graphique:

   Ne désinstallez pas le `trident-protect-crds` graphique à l'aide de Helm, car cela pourrait supprimer vos CRD et toutes les données associées.

```
kubectl delete secret -n trident-protect -l name=trident-protect-
crds,owner=helm
```

3. Mise à niveau de Trident Protect :

```
helm upgrade trident-protect netapp-trident-protect/trident-protect
--version 100.2510.0 --namespace trident-protect
```

Vous pouvez configurer le niveau de journalisation lors de la mise à niveau en ajoutant `--set logLevel=debug` à la commande de mise à niveau. Le niveau de journalisation par défaut est `warn` . L'activation de la journalisation de débogage est recommandée pour le dépannage, car elle aide le support NetApp à diagnostiquer les problèmes sans nécessiter de modifications du niveau de journalisation ni de reproduction du problème.