Gestisci Trident Protect

Trident

NetApp
November 03, 2026

This PDF was generated from https://docs.netapp.com/it-it/trident-2410/trident-protect/manage-authorization-access-control.html on November 03, 2026. Always check docs.netapp.com for the latest.

Sommario

Gestisci Trident Protect 1
Gestisci l’autorizzazione e il controllo degli accessi Trident Protect 1
Esempio: Gestire l’accesso per due gruppi di utenti 1
Genera un pacchetto di supporto Trident Protect 7
Aggiorna Trident Protect 8

Gestisci Trident Protect

Gestisci l'autorizzazione e il controllo degli accessi Trident Protect

Trident Protect utilizza il modello Kubernetes di controllo degli accessi basato sui ruoli (RBAC). Per impostazione predefinita, Trident Protect fornisce un singolo namespace di sistema e il relativo account di servizio predefinito. Se la tua organizzazione ha molti utenti o esigenze di sicurezza specifiche, puoi utilizzare le funzionalità RBAC di Trident Protect per ottenere un controllo più granulare sull'accesso alle risorse e agli spazi dei nomi.

L'amministratore del cluster ha sempre accesso alle risorse nello spazio dei nomi predefinito `trident-protect` e può anche accedere alle risorse in tutti gli altri namespace. Per controllare l'accesso a risorse e applicazioni, è necessario creare spazi dei nomi aggiuntivi e aggiungere risorse e applicazioni a tali spazi dei nomi.

Si noti che nessun utente può creare CRS per la gestione dei dati delle applicazioni nello spazio dei nomi predefinito `trident-protect`. È necessario creare CRS per la gestione dei dati delle applicazioni in uno spazio dei nomi delle applicazioni (come Best practice, creare CRS per la gestione dei dati delle applicazioni nello stesso spazio dei nomi dell'applicazione associata).

> Solo gli amministratori dovrebbero avere accesso agli oggetti di risorse personalizzate Trident Protect privilegiati, tra cui:
>
> - **AppVault**: Richiede i dati delle credenziali del bucket
> - **AutoSupportBundle**: raccoglie metriche, registri e altri dati sensibili Trident Protect
> - **AutoSupportBundleSchedule**: Gestisce i programmi di raccolta dei log
>
> Come Best practice, utilizzare RBAC per limitare l'accesso agli oggetti con privilegi agli amministratori.

Per ulteriori informazioni su come RBAC regola l'accesso alle risorse e agli spazi dei nomi, fare riferimento alla "Documentazione RBAC di Kubernetes" .

Per informazioni sugli account di servizio, fare riferimento alla "Documentazione dell'account del servizio Kubernetes" .

Esempio: Gestire l'accesso per due gruppi di utenti

Ad esempio, un'organizzazione dispone di un amministratore cluster, di un gruppo di utenti di progettazione e di un gruppo di utenti di marketing. L'amministratore del cluster dovrebbe completare le seguenti attività per creare un ambiente in cui il gruppo di progettazione e il gruppo di marketing hanno ciascuno accesso solo alle risorse assegnate ai rispettivi namespace.

Passaggio 1: Creare uno spazio dei nomi che contenga risorse per ciascun gruppo

La creazione di uno spazio dei nomi consente di separare logicamente le risorse e di controllare meglio chi ha accesso a tali risorse.

Fasi

1. Creare uno spazio dei nomi per il gruppo tecnico:

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

2. Creare uno spazio dei nomi per il gruppo di marketing:

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

Passaggio 2: Creare nuovi account di servizio per interagire con le risorse in ogni spazio dei nomi

Ogni nuovo spazio dei nomi creato viene fornito con un account di servizio predefinito, ma è necessario creare un account di servizio per ogni gruppo di utenti in modo da poter dividere ulteriormente Privileges tra i gruppi in futuro, se necessario.

Fasi

1. Creare un account di servizio per il gruppo tecnico:

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

2. Creare un account di servizio per il gruppo di marketing:

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

Passaggio 3: Creare un segreto per ogni nuovo account di servizio

Un segreto dell'account di servizio viene utilizzato per l'autenticazione con l'account di servizio e può essere facilmente eliminato e ricreato se compromesso.

Fasi

1. Creare un segreto per l'account del servizio tecnico:

```
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. Creare un segreto per l'account del servizio di 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
```

Passaggio 4: Creare un oggetto RoleBinding per associare l'oggetto ClusterRole a ogni nuovo account di servizio

Quando si installa Trident Protect, viene creato un oggetto ClusterRole predefinito. È possibile associare questo ClusterRole all'account di servizio creando e applicando un oggetto RoleBinding.

Fasi

1. Associare ClusterRole all'account del servizio tecnico:

```
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. Associare ClusterRole all'account del servizio di 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
```

Passaggio 5: Verifica delle autorizzazioni

Verificare che le autorizzazioni siano corrette.

Fasi

1. Verificare che gli utenti tecnici possano accedere alle risorse di progettazione:

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

2. Verificare che gli utenti tecnici non possano accedere alle risorse di marketing:

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

Passaggio 6: Concedere l'accesso agli oggetti AppVault

Per eseguire attività di gestione dei dati come backup e snapshot, l'amministratore del cluster deve garantire l'accesso agli oggetti AppVault ai singoli utenti.

Fasi

1. Creare e applicare un file YAML di combinazione di AppVault e segreto che consenta a un utente di accedere a un AppVault. Ad esempio, la seguente CR concede l'accesso ad AppVault all'utente `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. Creare e applicare un ruolo CR per consentire agli amministratori del cluster di concedere l'accesso a risorse specifiche in uno spazio dei nomi. Ad esempio:

```
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. Creare e applicare un RoleBinding CR per associare le autorizzazioni all'utente eng-user. Ad esempio:

```
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. Verificare che le autorizzazioni siano corrette.

   a. Tentativo di recuperare le informazioni sull'oggetto AppVault per tutti gli spazi dei nomi:

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

   L'output dovrebbe essere simile a quanto segue:

   ```
   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. Verificare se l'utente può ottenere le informazioni AppVault a cui ora dispone dell'autorizzazione per accedere:

   ```
   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
   ```

   L'output dovrebbe essere simile a quanto segue:

```
yes
```

Risultato

Gli utenti a cui sono state concesse le autorizzazioni AppVault dovrebbero essere in grado di utilizzare gli oggetti AppVault autorizzati per le operazioni di gestione dei dati delle applicazioni e non dovrebbero essere in grado di accedere a risorse esterne agli spazi dei nomi assegnati o creare nuove risorse a cui non hanno accesso.

Genera un pacchetto di supporto Trident Protect

Trident Protect consente agli amministratori di generare bundle che includono informazioni utili al supporto NetApp , tra cui registri, metriche e informazioni sulla topologia dei cluster e delle app in gestione. Se sei connesso a Internet, puoi caricare i bundle di supporto sul sito di supporto NetApp (NSS) utilizzando un file di risorse personalizzato (CR).

Creare un pacchetto di supporto utilizzando una CR

Fasi

1. Creare il file di risorsa personalizzata (CR) e assegnargli un nome (ad esempio, `trident-protect-support-bundle.yaml`).
2. Configurare i seguenti attributi:
   - **metadata.name**: (*required*) il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per il proprio ambiente.
   - **Spec.triggerType**: (*required*) determina se il bundle di supporto viene generato immediatamente o pianificato. La generazione pianificata del pacchetto avviene alle 12am:00 UTC. Valori possibili:
     - Pianificato
     - Manuale
   - **Spec.uploadEnabled**: (*Optional*) Controlla se il bundle di supporto deve essere caricato nel sito di supporto NetApp dopo che è stato generato. Se non specificato, il valore predefinito è `false` . Valori possibili:
     - vero
     - false (impostazione predefinita)
   - **Spec.dataWindowStart**: (*Optional*) stringa di data in formato RFC 3339 che specifica la data e l'ora di inizio della finestra dei dati inclusi nel pacchetto di supporto. Se non specificato, il valore predefinito è 24 ore fa. La prima data della finestra che è possibile specificare è 7 giorni fa.

     Esempio 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. Dopo aver popolato il `astra-support-bundle.yaml` file con i valori corretti, applicare la CR:

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

Creare un bundle di supporto utilizzando la CLI

Fasi

1. Creare il pacchetto di supporto, sostituendo i valori tra parentesi con le informazioni dell'ambiente. `trigger-type`Determina se il bundle viene creato immediatamente o se l'ora di creazione è dettata dalla pianificazione e può essere `Manual` o `Scheduled`. L'impostazione predefinita è `Manual`.

   Ad esempio:

```
tridentctl-protect create autosupportbundle <my_bundle_name>
--trigger-type <trigger_type>
```

Aggiorna Trident Protect

Puoi aggiornare Trident Protect all'ultima versione per sfruttare le nuove funzionalità o le correzioni di bug.

Per aggiornare Trident Protect, procedere come segue.

Fasi

1. Aggiornare il repository di Trident Helm:

```
helm repo update
```

2. Aggiorna i CRD Trident Protect:

```
helm upgrade trident-protect-crds netapp-trident-protect/trident-
protect-crds --version 100.2410.1  --namespace trident-protect
```

3. Aggiorna Trident Protect:

```
helm upgrade trident-protect netapp-trident-protect/trident-protect
```

```
--version 100.2410.1 --namespace trident-protect
```

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.