



使用 **Trident Protect** 保護應用程式 Trident

NetApp
October 30, 2026

目錄

使用 Trident Protect 保護應用程式	1
了解 Trident Protect	1
接下來呢？	1
安裝 Trident Protect	1
Trident Protect 要求	1
安裝並設定 Trident Protect	5
安裝 Trident Protect CLI 外掛程式	7
自訂 Trident Protect 安裝	10
管理 Trident Protect	15
管理 Trident Protect 授權和存取控制	15
監控 Trident Protect 資源	20
產生 Trident Protect 支援套件	25
升級 Trident Protect	26
管理和保護應用程式	28
使用 Trident Protect AppVault 物件來管理儲存桶	28
使用 Trident Protect 定義管理應用程式	39
使用 Trident Protect 保護應用程式	43
還原應用程式	52
使用 NetApp SnapMirror 和 Trident Protect 複製應用程式	72
使用 Trident Protect 遷移應用程式	85
使用 Trident Protect 保護 KubeVirt 虛擬機器	88
管理 Trident Protect 執行掛鉤	98
解除安裝 Trident Protect	105

使用 Trident Protect 保護應用程式

了解 Trident Protect

NetApp Trident Protect 提供進階應用程式資料管理功能，可增強由 NetApp ONTAP 儲存系統和 NetApp Trident CSI 儲存設定器支援的有狀態 Kubernetes 應用程式的功能和可用性。Trident Protect 簡化了跨公有雲和本地環境的容器化工作負載的管理、保護和遷移。它還透過其 API 和 CLI 提供自動化功能。

您可以透過建立自訂資源（CR）或使用 Trident Protect CLI 來使用 Trident Protect 保護應用程式。

接下來呢？

您可以在安裝 Trident Protect 之前先了解其相關需求：

- ["Trident Protect 要求"](#)

安裝 Trident Protect

Trident Protect 要求

首先，請驗證您的運作環境、應用程式叢集、應用程式和授權是否已準備就緒。確保您的環境符合這些要求，以部署和執行 Trident Protect。

Trident Protect Kubernetes 叢集相容性

Trident Protect 與各種完全託管和自架的 Kubernetes 產品相容，包括：

- Amazon Elastic Kubernetes Service (EKS)
- Google Kubernetes Engine (GKE)
- Microsoft Azure Kubernetes Service (AKS)
- Red Hat OpenShift
- SUSE Harvester 1.7.0 (ONTAP iSCSI)
- SUSE Rancher
- VMware Tanzu Portfolio
- 上游 Kubernetes



- Trident Protect 備份僅支援 Linux 運算節點。Windows 運算節點不支援備份作業。
- 確保安裝 Trident Protect 的叢集已配置正在執行中的快照控制器和相關的 CRD。若要安裝快照控制器，請參閱 ["這些說明"](#)。
- 確保至少存在一個 VolumeSnapshotClass。如需詳細資訊，請參閱 ["VolumeSnapshotClass"](#)。

- 安裝 Trident Protect 需要 Helm 4.x 或更高版本。

Trident Protect 儲存後端相容性

Trident Protect 支援以下儲存後端：

- Amazon FSx for NetApp ONTAP
- Cloud Volumes ONTAP
- ONTAP 儲存陣列
- Google Cloud NetApp Volumes
- Azure NetApp Files

請確保您的儲存後端符合以下要求：

- 確保連接到叢集的 NetApp 儲存裝置使用 Trident 24.02 或更高版本（建議使用 Trident 24.10）。
- 請確保您擁有 NetApp ONTAP 儲存後端。
- 請確保您已設定用於儲存備份的物件儲存貯體。
- 建立您計劃用於應用程式或應用程式資料管理作業的任何應用程式命名空間。Trident Protect 不會為您建立這些命名空間；如果您在自訂資源中指定了不存在的命名空間，則操作將會失敗。

nas-economy Volume 的需求

Trident Protect 支援對 nas-economy 磁碟區進行備份和還原作業。目前不支援對 nas-economy 磁碟區進行快照、複製和 SnapMirror 複寫。您需要為計劃與 Trident Protect 搭配使用的每個 nas-economy 磁碟區啟用快照目錄。



某些應用程式與使用快照目錄的磁碟區不相容。對於這些應用程式，您需要在 ONTAP 儲存系統上執行以下命令來隱藏快照目錄：

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

您可以透過對每個 nas-economy 磁碟區執行以下命令來啟用快照目錄，並將 ``<volume-UUID>`` 替換為您要變更的磁碟區的 UUID：

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



您可以將 Trident 後端組態選項 `snapshotDir` 設為 `true`，為新磁碟區預設啟用快照目錄。現有磁碟區不受影響。

利用 KubeVirt VM 保護資料

Trident Protect 在資料保護作業期間為 KubeVirt 虛擬機器提供檔案系統凍結和解凍功能，以確保資料一致性。虛擬機器凍結操作的配置方法和預設行為因 Trident Protect 版本而異，較新版本透過 Helm Chart 參數提供了更

簡化的配置方式。



在復原作業期間，不會復原為虛擬機器 (VM) 建立的任何 `VirtualMachineSnapshots`。

▼ Trident Protect 25.10 及更新版本

Trident Protect 會在資料保護作業期間自動凍結和解凍 KubeVirt 檔案系統，以確保資料一致性。從 Trident Protect 25.10 開始，您可以在 Helm chart 安裝過程中使用 `vm.freeze` 參數來停用此功能。此參數預設為啟用。

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

▼ Trident Protect 24.10.1 至 25.06

從 Trident Protect 24.10.1 版本開始，Trident Protect 會在資料保護作業期間自動凍結和解凍 KubeVirt 檔案系統。您也可以選擇使用以下命令停用此自動行為：

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

▼ Trident Protect 24.10

Trident Protect 24.10 在資料保護作業期間不會自動確保 KubeVirt VM 檔案系統的一致性狀態。如果您想使用 Trident Protect 24.10 保護 KubeVirt VM 資料，則需要在執行資料保護作業之前手動啟用檔案系統的凍結/解凍功能。這樣可以確保檔案系統處於一致狀態。

您可以設定 Trident Protect 24.10 來管理資料保護作業期間 VM 檔案系統的凍結和解凍，方法是["配置虛擬化"](#)然後使用下列指令：

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

若要了解如何使用 Trident Protect 定義應用程式和還原 VM，請參閱["使用 Trident Protect 保護 KubeVirt 虛擬機器"](#)。

SnapMirror 複寫的需求

NetApp SnapMirror 複寫可用於 Trident Protect，支援以下 ONTAP 解決方案：

- 本地端 NetApp FAS、AFF 和 ASA 系統。目前 ASA r2 系統尚不支援使用 Trident protect 的 SnapMirror 複寫。
- NetApp ONTAP Select
- NetApp Cloud Volumes ONTAP
- Amazon FSx for NetApp ONTAP

ONTAP 叢集 SnapMirror 複製要求

如果您打算使用 SnapMirror 複製功能，請確保您的 ONTAP 叢集符合下列要求：

- **NetApp Trident**：NetApp Trident 必須同時存在於使用 ONTAP 作為後端的來源和目標 Kubernetes 叢集上。Trident Protect 支援使用 NetApp SnapMirror 技術，透過以下驅動程式支援的儲存類別進行複製：
 - `ontap-nas`：NFS
 - `ontap-san`：iSCSI
 - `ontap-san`：FC
 - `ontap-san`：NVMe/TCP（需要最低 ONTAP 版本 9.15.1）
- **授權**：必須在來源和目的地 ONTAP 叢集上啟用使用資料保護套件的 ONTAP SnapMirror 非同步授權。請參閱 ["SnapMirror 授權總覽 \(ONTAP\)"](#) 以了解更多資訊。

從 ONTAP 9.10.1 開始，所有授權均以 NetApp 授權檔案（NLF）的形式提供，這是一個可啟用多項功能的單一檔案。如需詳細資訊，請參閱 ["ONTAP One 隨附的授權"](#)。



僅支援 SnapMirror 非同步保護。

SnapMirror 複製的對等考量

如果您打算使用儲存後端對等互連，請確保您的環境符合以下要求：

- **叢集和 SVM**：ONTAP 儲存後端必須建立對等連線。請參閱 ["叢集和 SVM 對等連接概述"](#) 以了解更多資訊。



確保兩個 ONTAP 叢集之間複製關係中使用的 SVM 名稱是唯一的。

- **NetApp Trident 和 SVM**：對等遠端 SVM 必須可供目標叢集上的 NetApp Trident 使用。
- **託管後端**：您需要在 Trident Protect 中新增和管理 ONTAP 儲存後端，以建立複製關係。

Trident / ONTAP 用於 SnapMirror 複製的配置

Trident Protect 要求您至少設定一個支援來源叢集和目標叢集複製的儲存後端。如果來源叢集和目標叢集相同，為了獲得最佳的恢復能力，目標應用程式應使用與來源應用程式不同的儲存後端。

Kubernetes 叢集 SnapMirror 複製要求

請確保您的 Kubernetes 叢集符合以下要求：

- **AppVault 可存取性**：來源叢集和目標叢集都必須具有網路存取權限，才能從 AppVault 讀取和寫入資料以進行應用程式物件複製。
- **網路連線**：設定防火牆規則、儲存桶權限和 IP 允許列表，以啟用兩個叢集之間以及 AppVault 跨 WAN 的通訊。



許多企業環境在 WAN 連線上實施嚴格的防火牆原則。在設定複製之前，請先與您的基礎架構團隊確認這些網路需求。

安裝並設定 Trident Protect

如果您的環境符合 Trident Protect 的要求，您可以依照下列步驟在叢集上安裝 Trident Protect。您可以從 NetApp 取得 Trident Protect，也可以從您自己的私人登錄安裝。如果您的叢集無法存取網際網路，從私人登錄安裝會很有幫助。

安裝 Trident Protect

從 NetApp 安裝 Trident Protect

步驟

1. 新增 Trident Helm 儲存庫：

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

2. 使用 Helm 安裝 Trident Protect。將 `<name-of-cluster>` 替換為叢集名稱，該名稱將分配給叢集並用於識別叢集的備份和快照：

```
helm install trident-protect netapp-trident-protect/trident-protect  
--set clusterName=<name-of-cluster> --version 100.2606.0 --create  
--namespace --namespace trident-protect
```

3. (選用) 若要啟用偵錯日誌記錄 (建議用於疑難排解)，請使用：

```
helm install trident-protect netapp-trident-protect/trident-protect  
--set clusterName=<name-of-cluster> --set logLevel=debug --version  
100.2606.0 --create-namespace --namespace trident-protect
```

偵錯日誌有助於 NetApp 支援人員在無需更改日誌等級或重現問題的情況下排查問題。

從私人註冊表安裝 Trident Protect

如果您的 Kubernetes 叢集無法存取網際網路，您可以從私人映像登錄安裝 Trident Protect。在這些範例中，請將方括號中的值替換為您環境中的資訊：

步驟

1. 將以下映像拉取到本機、更新標籤、然後將其推送到您的私有登錄：

```
docker.io/netapp/controller:26.06.0  
docker.io/netapp/restic:26.06.0  
docker.io/netapp/kopia:26.06.0  
docker.io/netapp/kopiablockrestore:26.06.0  
docker.io/netapp/trident-autosupport:26.06.0
```

```
docker.io/netapp/exehook:26.06.0
docker.io/netapp/resourcebackup:26.06.0
docker.io/netapp/resourcerestore:26.06.0
docker.io/netapp/resourcedelete:26.06.0
docker.io/netapp/trident-protect-utils:v1.0.0
```

例如：

```
docker pull docker.io/netapp/controller:26.06.0
```

```
docker tag docker.io/netapp/controller:26.06.0 <private-registry-  
url>/controller:26.06.0
```

```
docker push <private-registry-url>/controller:26.06.0
```



若要取得 Helm chart，請先在可存取互聯網的機器上使用 `helm pull trident-protect --version 100.2606.0 --repo <https://netapp.github.io/trident-protect-helm-chart>` 下載 Helm chart，然後將產生的 `trident-protect-100.2606.0.tgz` 檔案複製到您的離線環境中，並在最後一步中使用 `helm install trident-protect ./trident-protect-100.2606.0.tgz` 而不是儲存庫引用進行安裝。

2. 建立 Trident Protect 系統命名空間：

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

3. 登入登錄：

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

4. 建立用於私有登錄驗證的 pull secret：

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

5. 新增 Trident Helm 儲存庫：

```
helm repo add netapp-trident-protect
```

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

6. 建立一個名為 `protectValues.yaml` 的檔案。確保該檔案包含以下 Trident Protect 設定：

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



imageRegistry 和 imagePullSecrets 值適用於所有組件鏡像，包括 resourcebackup 和 resourcerestore。如果您將鏡像推送到登錄中的特定儲存庫路徑（例如，example.com:443/my-repo），請在登錄欄位中包含完整路徑。這將確保所有鏡像都從 <private-registry-url>/<image-name>:<tag> 拉取。

7. 使用 Helm 安裝 Trident Protect。將 `<name\_of\_cluster>` 替換為叢集名稱，該名稱將分配給叢集並用於識別叢集的備份和快照：

```
helm install trident-protect netapp-trident-protect/trident-protect
--set clusterName=<name_of_cluster> --version 100.2606.0 --create
--namespace --namespace trident-protect -f protectValues.yaml
```

8. （選用）若要啟用偵錯日誌記錄（建議用於疑難排解），請使用：

```
helm install trident-protect netapp-trident-protect/trident-protect
--set clusterName=<name-of-cluster> --set logLevel=debug --version
100.2606.0 --create-namespace --namespace trident-protect -f
protectValues.yaml
```

偵錯日誌有助於 NetApp 支援人員在無需更改日誌等級或重現問題的情況下排查問題。



有關 Helm chart 配置的其他選項，包括 AutoSupport 設定和命名空間過濾，請參閱 "[自訂 Trident Protect 安裝](#)"。

安裝 Trident Protect CLI 外掛程式

您可以使用 Trident Protect 命令列外掛程式（Trident tridentctl 實用程式的擴充功能）來建立和與 Trident Protect 自訂資源（CR）進行互動。

安裝 Trident Protect CLI 外掛程式

在使用命令列實用程式之前，需要將其安裝到用於存取叢集的電腦上。請根據您的電腦使用的是 x64 還是 ARM CPU，依照以下步驟操作。

下載適用於 **Linux AMD64 CPU** 的外掛程式

步驟

1. 下載 Trident Protect CLI 外掛程式：

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/v26.06.0/tridentctl-protect-linux-amd64
```

下載適用於 **Linux ARM64 CPU** 的外掛程式

步驟

1. 下載 Trident Protect CLI 外掛程式：

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/v26.06.0/tridentctl-protect-linux-arm64
```

下載適用於 **Mac AMD64 CPU** 的外掛程式

步驟

1. 下載 Trident Protect CLI 外掛程式：

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/v26.06.0/tridentctl-protect-macos-amd64
```

下載適用於 **Mac ARM64 CPU** 的外掛程式

步驟

1. 下載 Trident Protect CLI 外掛程式：

```
curl -L -o tridentctl-protect https://github.com/NetApp/tridentctl-protect/releases/download/v26.06.0/tridentctl-protect-macos-arm64
```

1. 啟用外掛程式二進位檔案的執行權限：

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

2. 將插件二進位檔案複製到 PATH 環境變數中定義的某個位置。例如， /usr/bin 或 /usr/local/bin（您可能需要管理員權限）：

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

- 您也可以選擇將插件二進位檔案複製到您主目錄下的某個位置。在這種情況下，建議確保該位置已新增至您的 PATH 環境變數：

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



將外掛程式複製到 PATH 變數中的某個位置,即可透過鍵入 `tridentctl-protect` 或 `tridentctl protect` 從任何位置使用該外掛程式。

查看 **Trident CLI** 外掛程式說明

您可以使用內建的外掛程式說明功能，以取得外掛程式功能的詳細說明：

步驟

- 使用說明功能檢視使用指南：

```
tridentctl-protect help
```

啟用命令自動完成

安裝 Trident Protect CLI 外掛程式後、您可以為某些命令啟用自動完成功能。

為 **Bash shell** 啟用自動完成功能

步驟

- 建立完成指令碼：

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

- 在您的使用者目錄下建立一個新目錄，用於存放腳本：

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

- 將下載的腳本移至 `~/.bash/completions` 目錄：

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

- 將以下行新增至您主目錄中的 `~/.bashrc` 檔案：

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

為 Z shell 啟用自動完成

步驟

1. 建立完成指令碼：

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

2. 在您的使用者目錄下建立一個新目錄，用於存放腳本：

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

3. 將下載的腳本移至 ~/.zsh/completions 目錄：

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

4. 將以下行新增至您主目錄中的 ~/.zprofile 檔案：

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

結果

下次登入 shell 時、您可以使用 tridentctl-protect 外掛程式進行命令自動完成。

自訂 Trident Protect 安裝

您可以自訂 Trident Protect 的預設組態，以符合您環境的特定需求。

指定 Trident Protect 容器資源限制

安裝 Trident Protect 後，您可以使用組態檔為 Trident Protect 容器指定資源限制。設定資源限制可讓您控制 Trident Protect 作業所消耗的叢集資源量。

步驟

1. 建立一個名為 `resourceLimits.yaml` 的檔案。
2. 根據您的環境需求，在檔案中填入 Trident Protect 容器的資源限制選項。

以下範例組態檔顯示可用的設定，並包含每個資源限制的預設值：

```
---  
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. 應用 resourceLimits.yaml 檔案中的值：

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

自訂安全內容限制

安裝 Trident Protect 後，您可以使用組態檔修改 Trident Protect 容器的 OpenShift 安全性內容限制（SCC）。這些限制定義了 Red Hat OpenShift 叢集中 Pod 的安全性限制。

步驟

1. 建立一個名為 `sccconfig.yaml` 的檔案。
2. 在檔案中新增 SCC 選項，並根據您的環境需求修改參數。

以下範例顯示 SCC 選項的參數預設值：

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

下表描述了 SCC 選項的參數：

參數	說明	預設
建立	確定是否可以建立 SCC 資源。僅當 `scc.create` 設定為 `true` 且 Helm 安裝程序識別 OpenShift 環境時，才會建立 SCC 資源。如果未在 OpenShift 中執行，或 `scc.create` 設定為 `false`，則不會建立 SCC 資源。	true
姓名	指定 SCC 的名稱。	Trident 保護工作
優先順序	定義 SCC 的優先順序。優先順序值較高的 SCC 會在優先順序值較低的 SCC 之前進行評估。	1

3. 應用 `sccconfig.yaml` 檔案中的值：

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

這將把預設值替換為 `sccconfig.yaml` 檔案中指定的值。

設定其他 Trident Protect Helm Chart 設定

您可以自訂 AutoSupport 設定、命名空間篩選和 OpenShift Webhook 憑證管理，以滿足您的特定需求。下表說明可用的組態參數：

參數	類型	說明
autoSupport.proxy	字串	設定 NetApp AutoSupport 連線的代理 URL。使用此功能可將支援包上傳路由至代理伺服器。例如： http://my.proxy.url 。
autoSupport.insecure	布林值	設定為 true 時，會跳過 AutoSupport Proxy 連線的 TLS 驗證。僅用於不安全的 Proxy 連線。（預設值：false）
autoSupport.enabled	布林值	啟用或停用每日 Trident Protect AutoSupport 捆綁包上傳。設定為 false 時，每日定時上傳將被停用，但您仍然可以手動產生支援捆綁包。（預設值：true）
restoreSkipNamespaceAnnotations	字串	以逗號分隔的命名空間註解清單，用於從備份和還原作業中排除。讓您根據註解篩選命名空間。
restoreSkipNamespaceLabels	字串	以逗號分隔的命名空間標籤清單，用於從備份和還原作業中排除。允許您根據標籤篩選命名空間。
useOpenshiftServiceCA	布林值	啟用與 OpenShift 原生 Service CA Operator 的整合，以便為 Trident Protect 准入 Webhook 自動建立和注入 TLS 憑證。設定為 true 時，Service CA Operator 將自動管理 Webhook TLS 憑證。僅在 OpenShift 叢集上使用。（預設值：false）

您可以使用 YAML 組態檔或命令列旗標來設定這些選項：

使用 YAML 檔案

步驟

1. 建立一個設定檔並將其命名為 values.yaml。
2. 在您建立的檔案中，新增您想要自訂的組態選項。

```
autoSupport:
  enabled: false
  proxy: http://my.proxy.url
  insecure: true
```

```
restoreSkipNamespaceAnnotations: "annotation1,annotation2"
restoreSkipNamespaceLabels: "label1,label2"
useOpenshiftServiceCA: true
```

3. 在 `values.yaml` 檔案中填入正確的值後，套用設定檔：

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

使用 CLI 標誌

步驟

1. 使用以下命令並加上 `--set` 標誌位元來指定各個參數：

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

將 Trident Protect Pod 限制在特定節點上

您可以使用 Kubernetes `nodeSelector` 節點選擇約束，根據節點標籤來控制哪些節點可以執行 Trident Protect Pod。預設情況下，Trident Protect 僅限於執行 Linux 的節點。您可以根據需要進一步自訂這些約束。

步驟

1. 建立一個名為 `'nodeSelectorConfig.yaml'` 的檔案。
2. 將 `nodeSelector` 選項新增至檔案中，並修改該檔案以新增或變更節點標籤，從而根據您的環境需求進行限制。例如，以下檔案包含預設的作業系統限制，但也針對特定區域和應用程式名稱：

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

3. 應用 `nodeSelectorConfig.yaml` 檔案中的值：

```
helm upgrade trident-protect -n trident-protect netapp-trident-
```

```
protect/trident-protect -f nodeSelectorConfig.yaml --reuse-values
```

這將預設限制替換為您 `nodeSelectorConfig.yaml` 文件中指定的限制。

管理 Trident Protect

管理 Trident Protect 授權和存取控制

Trident Protect 使用 Kubernetes 的角色型存取控制 (RBAC) 模型。預設情況下，Trident Protect 提供單一系統命名空間及其相關的預設服務帳戶。如果您的組織擁有眾多使用者或有特定的安全需求，則可以使用 Trident Protect 的 RBAC 功能來更精細地控制對資源和命名空間的存取。

叢集管理員始終擁有對預設 `trident-protect` 命名空間中資源的存取權限，並且還可以存取所有其他命名空間中的資源。要控制對資源和應用程式的存取，您需要建立其他命名空間，並將資源和應用程式新增至這些命名空間。

請注意，任何使用者都無法在預設 `trident-protect` 命名空間中建立應用程式資料管理 CR。您需要在應用程式命名空間中建立應用程式資料管理 CR（最佳實踐是將應用程式資料管理 CR 建立在與其關聯應用程式相同的命名空間中）。

只有管理員才能存取具有特權的 Trident Protect 自訂資源物件，其中包括：



- **AppVault**：需要儲存桶憑證資料
- **AutoSupportBundle**：收集指標、日誌和其他敏感的 Trident Protect 數據
- **AutoSupportBundleSchedule**：管理日誌收集排程

最佳實踐是使用 RBAC 將對特權物件的存取限制在管理員範圍內。

如需有關 RBAC 如何管理對資源和命名空間的存取的詳細資訊，請參閱 ["Kubernetes RBAC 文件"](#)。

如需服務帳戶的相關資訊，請參閱 ["Kubernetes 服務帳戶文件"](#)。

範例：管理兩組使用者的存取權限

例如，一個組織有一名 cluster 管理員、一組工程用戶和一組行銷用戶。cluster 管理員需要完成以下任務，以建立一個環境，使工程使用者群組和行銷使用者群組各自只能存取分配給其各自 namespace 的資源。

步驟 1：建立命名空間以包含每個群組的資源

建立命名空間可讓您以邏輯方式分隔資源，並更有效地控制誰可以存取這些資源。

步驟

1. 為工程群組建立命名空間：

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

2. 為行銷組建立命名空間：

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

步驟 2：建立新的服務帳戶、以便與每個命名空間中的資源互動

您建立的每個新命名空間都附帶一個預設服務帳戶，但您應該為每個使用者群組建立一個服務帳戶，以便將來必要時可以進一步在群組之間劃分權限。

步驟

1. 為工程群組建立服務帳戶：

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

2. 為行銷群組建立服務帳戶：

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

步驟 3：為每個新服務帳戶建立一個密碼

服務帳戶密碼用於對服務帳戶進行身分驗證，如果遭到洩露，可以輕鬆刪除並重新建立。

步驟

1. 為工程服務帳戶建立密鑰：

```
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. 為行銷服務帳戶建立密鑰：

```

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

```

步驟 4：建立一個 **RoleBinding** 對象，並將該 **ClusterRole** 對象綁定到每個新的服務帳戶

當您安裝 Trident Protect 時，會自動建立一個預設的 ClusterRole 物件。您可以透過建立並套用 RoleBinding 物件，將此 ClusterRole 綁定至服務帳戶。

步驟

1. 將 ClusterRole 綁定到工程服務帳戶：

```

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. 將 ClusterRole 綁定到行銷服務帳戶：

```

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
```

步驟 5：測試權限

測試權限是否正確。

步驟

1. 確認工程使用者可以存取工程資源：

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

2. 確認工程使用者無法存取行銷資源：

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

步驟 6：授予 AppVault 物件存取權限

要執行備份和快照等資料管理任務，叢集管理員需要授予個別使用者對 AppVault 物件的存取權限。

步驟

1. 建立並套用 AppVault 和密碼組合 YAML 檔案，授予使用者存取 AppVault 的權限。例如，以下 CR 授予使用者存取 AppVault 的權限 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. 建立並套用 Role CR，以使叢集管理員能夠授予對命名空間中特定資源的存取權。例如：

```

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. 建立並套用 RoleBinding CR，將權限綁定到使用者 eng-user。例如：

```

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. 確認權限是否正確。

a. 嘗試檢索所有命名空間的 AppVault 物件資訊：

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

您應該會看到類似以下內容的輸出：

```
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. 測試用戶是否可以獲得他們現在有權訪問的 AppVault 資訊：

```
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
```

您應該會看到類似以下內容的輸出：

```
yes
```

結果

您授予 AppVault 權限的使用者應該能夠使用授權 AppVault 物件進行應用程式資料管理操作，並且不應該能夠存取指派的命名空間以外的任何資源，或建立他們無權存取的新資源。

監控 Trident Protect 資源

您可以使用 kube-state-metrics、Prometheus 和 Alertmanager 這些開源工具來監控由 Trident Protect 保護的資源健康狀況。

kube-state-metrics 服務會從 Kubernetes API 通訊產生指標。將其與 Trident Protect 結合使用，可公開有關環境中資源狀態的實用資訊。

Prometheus 是一個工具包，可以接收由 kube-state-metrics 產生的數據，並將其呈現為易於閱讀的這些物件資訊。kube-state-metrics 和 Prometheus 結合使用，為你提供一種方式來監控你使用 Trident Protect 管理的資源的健康狀態和狀態。

Alertmanager 是一項服務，它可以接收 Prometheus 等工具發送的警報，並將它們路由到您配置的目標位置。

這些步驟中包含的組態和指南僅為範例；您需要根據自己的環境進行自訂。有關具體說明和支援，請參閱以下官方文件：



- ["kube-state-metrics 說明文件"](#)
- ["Prometheus 說明文件"](#)
- ["Alertmanager 文件"](#)

步驟 1：安裝監控工具

要在 Trident Protect 中啟用資源監控，您需要安裝和設定 kube-state-metrics、Prometheus 和 Alertmanager。

安裝 kube-state-metrics

您可以使用 Helm 安裝 kube-state-metrics。

步驟

1. 新增 kube-state-metrics Helm chart。例如：

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

2. 將 Prometheus ServiceMonitor CRD 應用於叢集：

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

3. 為 Helm chart 建立一個設定檔（例如，metrics-config.yaml）。您可以自訂以下範例設定以符合您的環境：

metrics-config.yaml：kube-state-metrics Helm chart 配置

```
---  
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. 透過部署 Helm chart 來安裝 kube-state-metrics。例如：

```

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

```

5. 請依照 "[kube-state-metrics 自訂資源文件](#)"中的說明配置 kube-state-metrics，以產生 Trident Protect 使用的自訂資源的指標。

安裝 Prometheus

您可以按照 "[Prometheus 說明文件](#)"中的說明安裝 Prometheus。

安裝 Alertmanager

您可以按照 "[Alertmanager 文件](#)"中的說明安裝 Alertmanager。

步驟 2：設定監控工具以協同運作

安裝監控工具後，您需要設定它們以使其協同工作。

步驟

1. 將 kube-state-metrics 與 Prometheus 整合。編輯 Prometheus 配置文件 (prometheus.yaml) 並新增 kube-state-metrics 服務資訊。例如：

prometheus.yaml：kube-state-metrics 服務與 Prometheus 的整合

```
---
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. 設定 Prometheus 將警示路由至 Alertmanager。編輯 Prometheus 組態檔 (prometheus.yaml)，並新增以下區段：

prometheus.yaml：將警報傳送至 Alertmanager

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

結果

Prometheus 現在可以從 kube-state-metrics 收集指標，並向 Alertmanager 發送警報。現在您可以設定觸發警報的條件以及警報的發送位置。

步驟 3：設定警示和警示目的地

配置好工具協同工作後，您需要配置哪些類型的資訊會觸發警示，以及警示應該發送到哪裡。

警示範例：備份失敗

以下範例定義了一個關鍵警報，當備份自訂資源的狀態設定為 `Error` 且持續時間達到 5 秒或更長時，將觸發該警報。您可以根據自己的環境自訂此範例，並將此 YAML 程式碼片段新增至您的 `prometheus.yaml` 組態檔：

rules.yaml：定義備份失敗的 **Prometheus** 警報

```
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."
```

配置 **Alertmanager** 以將警示傳送至其他管道

您可以設定 Alertmanager，使其會向其他管道（例如電子郵件、PagerDuty、Microsoft Teams 或其他通知服務）發送通知，只需在 `alertmanager.yaml` 文件中指定相應的配置即可。

以下範例配置 Alertmanager 向 Slack 頻道發送通知。若要根據您的環境自訂此範例，請將 `api_url` 鍵值替換為您環境中使用的 Slack webhook URL：

alertmanager.yaml：向 **Slack** 頻道發送警報

```
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
```

產生 Trident Protect 支援套件

Trident Protect 讓管理員產生包含對 NetApp 支援團隊有用的資訊的軟體包，例如受管理叢集和應用程式的日誌、指標和拓撲資訊。如果您已連接到互聯網，則可以使用自訂資源（CR）檔案將支援軟體包上傳至 NetApp 支援網站（NSS）。

使用 **CR** 建立支援套件

步驟

1. 建立自訂資源（CR）檔案並將其命名為（例如、`trident-protect-support-bundle.yaml`）。
2. 設定下列屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.triggerType**：（必填）確定支援包是立即產生還是定時產生。定時產生會在 UTC 時間凌晨 12 點進行。可選值：
 - 已排程
 - 手動
 - **spec.uploadEnabled**：（選用）控制產生支援服務包後是否應將其上傳至 NetApp 支援網站。如果未指定、則預設為 `false`。可選值：
 - `true`
 - `false`（預設）
 - **spec.dataWindowStart**：（選用）RFC 3339 格式的日期字串，用於指定支援套件中包含的資料視窗的起始日期和時間。如果未指定，則預設為 24 小時前。您可以指定的最早視窗日期為 7 天前。

YAML 範例：

```
---
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. 在 `trident-protect-support-bundle.yaml` 檔案中填入正確的值後，套用 CR：

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

使用 CLI 建立支援套件

步驟

1. 建立支援包，將括號中的值替換為您環境中的資訊。trigger-type`決定是立即建立支援包還是根據排程建立，其值可以是 `Manual` 或 `Scheduled`。預設設定為 Manual。

例如：

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

監控並擷取支援服務包

使用任一方法建立支援套件後，您可以監控其產生進度並將其擷取到本機系統。

步驟

1. 等待 status.generationState 達到 Completed 狀態。您可以使用以下命令監控產生進度：

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

2. 將支援套件組合擷取至本機系統。從已完成的 AutoSupport 套件組合取得複製命令：

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

從輸出中找到 `kubectl cp` 命令並運行它，將目標參數替換為您首選的本機目錄。

升級 Trident Protect

您可以將 Trident Protect 升級至最新版本，以利用新功能或錯誤修正。



- 從 24.10 版本升級時，升級期間執行的快照可能會失敗。此失敗不會阻止未來的快照（無論是手動還是排程）被建立。如果快照在升級期間失敗，您可以手動建立新快照以確保應用程式受到保護。

為避免潛在故障，您可以在升級前停用所有快照排程，並在升級後重新啟用。但是，這樣做會導致升級期間所有已排程的快照遺失。

- 對於私有鏡像倉庫安裝，請確保目標版本所需的 Helm chart 和鏡像已存在於您的私有鏡像倉庫中，並驗證您的自訂 Helm 值與新 chart 版本相容。如需詳細資訊，請參閱 ["從私人註冊表安裝 Trident Protect"](#)。

步驟 1：選擇版本

Trident Protect 版本遵循基於日期的 `YY.MM` 命名規則，其中「YY」代表年份的後兩位數字，「MM」代表月份。小版本更新遵循 `YY.MM.X` 規則，其中「X」代表補丁級別。您將根據要升級的版本選擇要升級到的版本。

- 您可以將目前版本直接升級到與其相差不超過四個版本號的目標版本。例如，您可以直接從 24.10（或任何 24.10 的小版本）升級到 25.10。
- 如果您要從超出四版本週期範圍的版本升級，請執行多步驟升級。使用您要升級的 ["早期版本"](#) 版本對應的升級說明，升級到符合四版本視窗期的最新版本。例如，如果您目前執行的是 24.10 版本，並且想要升級至 26.06 版本：
 - a. 首次從 24.10 升級到 25.02。
 - b. 然後從 25.02 升級到 26.06。

步驟 2：升級 Trident Protect

若要升級 Trident Protect，請執行下列步驟。

步驟

1. 更新 Trident Helm 儲存庫：

```
helm repo update
```

2. 升級 Trident Protect CRD：



如果您是從 25.06 之前的版本升級，則需要執行此步驟，因為 CRD 現在已包含在 Trident Protect Helm 圖表中。

- a. 執行此命令將 CRD 的管理權限從 `trident-protect-crds` 切換到 `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. 執行以下指令刪除 `trident-protect-crds` chart 的 Helm secret：



請勿使用 Helm 卸載 `trident-protect-crds` 圖表，因為這可能會刪除您的 CRD 和任何相關資料。

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

3. 升級 Trident Protect：

```
helm upgrade trident-protect netapp-trident-protect/trident-protect
--version 100.2606.0 --namespace trident-protect
```



您可以透過在升級命令中新增 `--set logLevel=debug` 來配置升級期間的日誌等級。預設日誌等級為 `warn`。建議啟用偵錯日誌以進行故障排除，因為它有助於 NetApp 支援人員診斷問題，而無需更改日誌等級或重現問題。

管理和保護應用程式

使用 Trident Protect AppVault 物件來管理儲存桶

Trident Protect 的儲存桶自訂資源 (CR) 稱為 AppVault。AppVault 物件是儲存桶的聲明式 Kubernetes 工作流程表示。AppVault CR 包含儲存設備貯體在保護作業（例如備份、快照、還原作業和 SnapMirror 複寫）中使用所需的組態。只有管理員才能建立 AppVaults。

在對應用程式執行資料保護操作時，您需要手動或透過命令列建立 AppVault CR。AppVault CR 是針對您的環境而設定的，您可以參考此頁面上的範例來建立 AppVault CR。



請確保 AppVault CR 位於安裝了 Trident Protect 的叢集上。如果 AppVault CR 不存在或無法訪問，命令列將顯示錯誤。

設定 AppVault 驗證和密碼

在建立 AppVault CR 之前，請確保 AppVault 和您選擇的資料移動程式能夠透過提供者和任何相關資源進行身份驗證。

Data mover 儲存庫密碼

當您使用 CR 或 Trident Protect CLI 外掛程式建立 AppVault 物件時，您可以指定 Kubernetes Secret，其中包含用於 Restic 和 Kopia 加密的自訂密碼。如果您未指定 Secret，Trident Protect 將使用預設密碼。

- 手動建立 AppVault CR 時，請使用 `spec.dataMoverPasswordSecretRef` 欄位指定金鑰。
- 使用 Trident Protect CLI 建立 AppVault 物件時，請使用 `--data-mover-password-secret-ref` 參數指定金鑰。

建立資料移動器儲存庫密碼密鑰

請使用以下範例建立密碼密鑰。建立 AppVault 物件時，您可以指示 Trident Protect 使用此密鑰向資料移動器儲存庫進行驗證。



- 根據您使用的資料遷移工具，您只需包含該資料遷移工具對應的密碼即可。例如，如果您使用的是 Restic，並且將來不打算使用 Kopia，則在建立 secret 時只需包含 Restic 的密碼即可。
- 請妥善保管密碼。您需要使用此密碼在同一叢集或其他叢集上還原資料。如果叢集或 `trident-protect` 命名空間被刪除，沒有密碼您將無法還原備份或快照。

使用 CR

```
---
apiVersion: v1
data:
  KOPIA_PASSWORD: <base64-encoded-password>
  RESTIC_PASSWORD: <base64-encoded-password>
kind: Secret
metadata:
  name: my-optional-data-mover-secret
  namespace: trident-protect
type: Opaque
```

使用 CLI

```
kubectl create secret generic my-optional-data-mover-secret \
--from-literal=KOPIA_PASSWORD=<plain-text-password> \
--from-literal=RESTIC_PASSWORD=<plain-text-password> \
-n trident-protect
```

S3 相容儲存 IAM 權限

當您使用 Trident Protect 存取 S3 相容儲存（例如 Amazon S3、Generic S3 "[StorageGrid S3](#)"或 "[ONTAP S3](#)"）時，您需要確保所提供的使用者認證具有存取儲存貯體的必要權限。以下是授予使用 Trident Protect 存取所需最低權限的原則範例。您可以將此原則套用至管理 S3 相容儲存貯體原則的使用者。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    }
  ]
}
```

有關 Amazon S3 策略的更多資訊，請參閱 "[Amazon S3 文件](#)" 中的範例。

用於 Amazon S3 (AWS) 驗證的 EKS Pod Identity

Trident Protect 支援 EKS Pod Identity 進行 Kopia 資料遷移操作。此功能可安全存取 S3 儲存貯體，而無需將 AWS 認證儲存在 Kubernetes Secret 中。

使用 Trident Protect 的 EKS Pod Identity 需求

在將 EKS Pod Identity 與 Trident Protect 結合使用之前，請確保以下事項：

- 您的 EKS 叢集已啟用 Pod Identity。
- 您已建立具有必要 S3 儲存桶權限的 IAM 角色。若要深入瞭解，請參閱 ["S3 相容儲存 IAM 權限"](#)。
- IAM 角色與下列 Trident Protect 服務帳戶相關聯：
 - <trident-protect>-controller-manager
 - <trident-protect>-resource-backup
 - <trident-protect>-resource-restore
 - <trident-protect>-resource-delete

有關啟用 Pod Identity 並將 IAM 角色與服務帳戶關聯的詳細說明，請參閱 ["AWS EKS Pod Identity 文件"](#)。

AppVault 設定 使用 EKS Pod Identity 時，請使用 `useIAM: true` 標誌設定 AppVault CR，而不是明確憑證：

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: eks-protect-vault
  namespace: trident-protect
spec:
  providerType: AWS
  providerConfig:
    s3:
      bucketName: trident-protect-aws
      endpoint: s3.example.com
      useIAM: true
```

AppVault 雲端服務提供者的金鑰產生範例

定義 AppVault CR 時，除非使用 IAM 驗證，否則您需要包含存取提供者託管資源的憑證。憑證金鑰的產生方式因提供者而異。以下是幾個提供者的命令列金鑰產生範例。您可以使用以下範例為每個雲端提供者的憑證建立金鑰。

Google Cloud

```
kubectl create secret generic <secret-name> \
--from-file=credentials=<mycreds-file.json> \
-n trident-protect
```

Amazon S3 (AWS)

```
kubectl create secret generic <secret-name> \  
--from-literal=accessKeyID=<objectstorage-accesskey> \  
--from-literal=secretAccessKey=<amazon-s3-trident-protect-src-bucket  
-secret> \  
-n trident-protect
```

Microsoft Azure

```
kubectl create secret generic <secret-name> \  
--from-literal=accountKey=<secret-name> \  
-n trident-protect
```

通用 S3

```
kubectl create secret generic <secret-name> \  
--from-literal=accessKeyID=<objectstorage-accesskey> \  
--from-literal=secretAccessKey=<generic-s3-trident-protect-src-bucket  
-secret> \  
-n trident-protect
```

ONTAP S3

```
kubectl create secret generic <secret-name> \  
--from-literal=accessKeyID=<objectstorage-accesskey> \  
--from-literal=secretAccessKey=<ontap-s3-trident-protect-src-bucket  
-secret> \  
-n trident-protect
```

StorageGrid S3

```
kubectl create secret generic <secret-name> \  
--from-literal=accessKeyID=<objectstorage-accesskey> \  
--from-literal=secretAccessKey=<storagegrid-s3-trident-protect-src  
-bucket-secret> \  
-n trident-protect
```

AppVault 建立範例

以下是各提供者的 AppVault 定義範例。

AppVault CR 範例

您可以使用以下 CR 範例為每個雲端提供者建立 AppVault 物件。



- 您可以選擇指定一個 Kubernetes Secret，其中包含 Restic 和 Kopia 儲存庫加密的自訂密碼。如需詳細資訊，請參閱 [Data mover 儲存庫密碼](#)。
- 對於 Amazon S3 (AWS) AppVault 物件，您可以選擇性地指定 sessionToken，如果您使用單一登入（SSO）進行身份驗證，這將非常有用。此令牌在您為提供者產生金鑰時建立 [AppVault 雲端服務提供者的金鑰產生範例](#)。
- 對於 S3 AppVault 對象，您可以使用 spec.providerConfig.S3.proxyURL 鍵選擇性地指定出站 S3 流量的出口代理 URL。

Google Cloud

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: gcp-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: GCP
  providerConfig:
    gcp:
      bucketName: trident-protect-src-bucket
      projectID: project-id
  providerCredentials:
    credentials:
      valueFromSecret:
        key: credentials
        name: gcp-trident-protect-src-bucket-secret
```

Amazon S3 (AWS)

```
---
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: amazon-s3-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: AWS
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
```

```

    endpoint: s3.example.com
    proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret
    sessionToken:
      valueFromSecret:
        key: sessionToken
        name: s3-secret

```



對於使用 Pod Identity 與 Kopia data mover 的 EKS 環境，您可以移除 `providerCredentials` 區段，並將 `useIAM: true` 新增到 `s3` 設定下方。

Microsoft Azure

```

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: azure-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: Azure
  providerConfig:
    azure:
      accountName: account-name
      bucketName: trident-protect-src-bucket
  providerCredentials:
    accountKey:
      valueFromSecret:
        key: accountKey
        name: azure-trident-protect-src-bucket-secret

```

通用 S3

```

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: generic-s3-trident-protect-src-bucket

```

```

namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: GenericS3
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
      proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret

```

ONTAP S3

```

apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: OntapS3
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
      proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret

```

StorageGrid S3

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: storagegrid-s3-trident-protect-src-bucket
  namespace: trident-protect
spec:
  dataMoverPasswordSecretRef: my-optional-data-mover-secret
  providerType: StorageGridS3
  providerConfig:
    s3:
      bucketName: trident-protect-src-bucket
      endpoint: s3.example.com
      proxyURL: http://10.1.1.1:3128
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: s3-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: s3-secret
```

使用 **Trident Protect CLI** 建立 **AppVault** 的範例

您可以使用以下 CLI 命令範例為每個提供者建立 AppVault CR。



- 您可以選擇指定一個 Kubernetes Secret，其中包含 Restic 和 Kopia 儲存庫加密的自訂密碼。如需詳細資訊，請參閱 [Data mover 儲存庫密碼](#)。
- 對於 S3 AppVault 對象，您可以使用 `--proxy-url <ip_address:port>` 參數選擇性地指定出站 S3 流量的出口代理 URL。

Google Cloud

```
tridentctl-protect create vault GCP <vault-name> \
--bucket <mybucket> \
--project <my-gcp-project> \
--secret <secret-name>/credentials \
--data-mover-password-secret-ref <my-optional-data-mover-secret> \
-n trident-protect
```

Amazon S3 (AWS)

```
tridentctl-protect create vault AWS <vault-name> \  
--bucket <bucket-name> \  
--secret <secret-name> \  
--endpoint <s3-endpoint> \  
--data-mover-password-secret-ref <my-optional-data-mover-secret> \  
-n trident-protect
```

Microsoft Azure

```
tridentctl-protect create vault Azure <vault-name> \  
--account <account-name> \  
--bucket <bucket-name> \  
--secret <secret-name> \  
--data-mover-password-secret-ref <my-optional-data-mover-secret> \  
-n trident-protect
```

通用 S3

```
tridentctl-protect create vault GenericS3 <vault-name> \  
--bucket <bucket-name> \  
--secret <secret-name> \  
--endpoint <s3-endpoint> \  
--data-mover-password-secret-ref <my-optional-data-mover-secret> \  
-n trident-protect
```

ONTAP S3

```
tridentctl-protect create vault OntapS3 <vault-name> \  
--bucket <bucket-name> \  
--secret <secret-name> \  
--endpoint <s3-endpoint> \  
--data-mover-password-secret-ref <my-optional-data-mover-secret> \  
-n trident-protect
```

StorageGrid S3

```
tridentctl-protect create vault StorageGridS3 <vault-name> \  
--bucket <bucket-name> \  
--secret <secret-name> \  
--endpoint <s3-endpoint> \  
--data-mover-password-secret-ref <my-optional-data-mover-secret> \  
-n trident-protect
```

支援的 `providerConfig.s3` 配置選項

請參閱下表以了解 S3 提供者組態選項：

參數	說明	預設	範例
<code>providerConfig.s3.skipCertValidation</code>	停用 SSL/TLS 憑證驗證。	錯誤	"true"、"false"
<code>providerConfig.s3.secure</code>	啟用與 S3 端點的安全 HTTPS 通訊。	true	"true"、"false"
<code>providerConfig.s3.proxyURL</code>	指定用於連接到 S3 的 Proxy 伺服器 URL。	無	http://proxy.example.com:8080
<code>providerConfig.s3.rootCA</code>	提供用於 SSL/TLS 驗證的自訂根 CA 憑證。	無	"CN=MyCustomCA"
<code>providerConfig.s3.useIAM</code>	啟用 IAM 驗證以存取 S3 儲存桶。適用於 EKS Pod Identity。	錯誤	true、false

查看 **AppVault** 資訊

您可以使用 Trident Protect CLI 外掛程式查看有關您在叢集上建立的 AppVault 物件的資訊。

步驟

1. 查看 AppVault 物件的內容：

```
tridentctl-protect get appvaultcontent gcp-vault \
--show-resources all \
-n trident-protect
```

範例輸出：

```
+-----+-----+-----+-----+
+-----+
|  CLUSTER  | APP  | TYPE  | NAME                                     |
|TIMESTAMP  |      |       |                                         |
+-----+-----+-----+-----+
+-----+
|           | mysql | snapshot | mysnap                                     | 2024-
08-09 21:02:11 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815180300 | 2024-
08-15 18:03:06 (UTC) |
```

```

| production1 | mysql | snapshot | hourly-e7db6-20240815190300 | 2024-
08-15 19:03:06 (UTC) |
| production1 | mysql | snapshot | hourly-e7db6-20240815200300 | 2024-
08-15 20:03:06 (UTC) |
| production1 | mysql | backup | hourly-e7db6-20240815180300 | 2024-
08-15 18:04:25 (UTC) |
| production1 | mysql | backup | hourly-e7db6-20240815190300 | 2024-
08-15 19:03:30 (UTC) |
| production1 | mysql | backup | hourly-e7db6-20240815200300 | 2024-
08-15 20:04:21 (UTC) |
| production1 | mysql | backup | mybackup5 | 2024-
08-09 22:25:13 (UTC) |
| | mysql | backup | mybackup | 2024-
08-09 21:02:52 (UTC) |
+-----+-----+-----+-----+
+-----+

```

2. (可選) 若要查看每個資源的 AppVaultPath，請使用標誌 `--show-paths`。

只有在 Trident Protect Helm 安裝過程中指定了叢集名稱時，表格第一列中的叢集名稱才可用。例如：
`--set clusterName=production1`。

移除 AppVault

您可以隨時移除 AppVault 物件。



在刪除 AppVault 物件之前，請勿移除 AppVault CR 中的 `finalizers` 金鑰。否則，可能會導致 AppVault 儲存桶中殘留資料，並在叢集中產生孤立資源。

開始之前

請確保您已刪除要刪除的 AppVault 所使用的所有快照和備份 CR。

使用 Kubernetes CLI 刪除 AppVault

1. 刪除 AppVault 物件，將 `appvault-name` 替換為要刪除的 AppVault 物件名稱：

```
kubectl delete appvault <appvault-name> \
-n trident-protect
```

使用 Trident Protect CLI 刪除 AppVault

1. 刪除 AppVault 物件，將 `appvault-name` 替換為要刪除的 AppVault 物件名稱：

```
tridentctl-protect delete appvault <appvault-name> \
-n trident-protect
```

使用 Trident Protect 定義管理應用程式

您可以透過建立應用程式 CR 和關聯的 AppVault CR 來定義要使用 Trident Protect 管理的應用程式。

建立 AppVault CR

您需要建立一個 AppVault CR，該 CR 將在對應用程式執行資料保護作業時使用，且該 AppVault CR 必須位於安裝了 Trident Protect 的叢集上。AppVault CR 特定於您的環境；有關 AppVault CR 的範例，請參閱["AppVault 自訂資源"](#)。

定義應用程式

您需要定義要使用 Trident Protect 管理的每個應用程式。您可以透過手動建立應用程式 CR 或使用 Trident Protect CLI 來定義要管理的應用程式。



若要定義 VM 範圍的應用程式，以按名稱而非整個命名空間來保護特定的 KubeVirt 虛擬機器 (VM)，請使用 Application CR 中的 `spec.includedVirtualMachines` 欄位或 CLI 中的 `--virtual-machines` 旗標。如需詳細資訊、欄位參考和 YAML 範例，請參閱["使用 Trident Protect 保護 KubeVirt 虛擬機器"](#)。

使用 CR 新增應用程式

步驟

1. 建立目的地應用程式 CR 檔案：

- 建立自訂資源 (CR) 檔案並將其命名為 (例如、`maria-app.yaml`)。
- 設定下列屬性：

- **metadata.name**：(必填) 應用程式自訂資源的名稱。請記住您選擇的名稱，因為保護作業所需的其他 CR 檔案會參照此值。
- **spec.includedNamespaces**：(必要) 使用命名空間和標籤選擇器來指定應用程式使用的命名空間和資源。應用程式命名空間必須包含在此清單中。標籤選擇器是可選的，可用來篩選每個指定命名空間中的資源。
- **spec.includedClusterScopedResources**：(選用) 使用此屬性指定要包含在應用程式定義中的叢集範圍資源。此屬性可讓您根據資源的群組、版本、類型和標籤來選擇這些資源。
 - **groupVersionKind**：(必要) 指定叢集範圍資源的 API 群組、版本和類型。
 - **labelSelector**：(可選) 依照標籤篩選叢集範圍的資源。
- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**：(可選) 此註解僅適用於從虛擬機器定義的應用程式，例如在 KubeVirt 環境中，檔案系統會在快照之前凍結。指定此應用程式在快照期間是否可以寫入檔案系統。如果設定為 `true`，則應用程式將忽略全域設定，並且可以在快照期間寫入檔案系統。如果設定為 `false`，則應用程式將忽略全域設定，並且檔案系統將在快照期間凍結。如果指定了此註解，但應用程式定義中沒有虛擬機器，則該註解將被忽略。如果未指定，則應用程式會遵循["全球 Trident Protect 凍結設定"](#)。

如果需要在應用程式建立後套用此註解，可以使用以下命令：

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
YAML 範例：

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (選用) 如有需要、您可以將資源篩選新增至相同的 CR、以包含或排除特定資源：

◦ 通用篩選器範例：

- **resourceFilter.resourceSelectionCriteria**：(篩選必需) 使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：
- **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，它們之間將按 OR 運算匹配，每個元素內的欄位 (group、kind、version) 之間將按 AND 運算匹配。

- **resourceMatchers[].group**：（可選）要篩選的資源群組。
- **resourceMatchers[].kind**：（可選）要篩選的資源類型。
- **resourceMatchers[].version**：（可選）要篩選的資源版本。
- **resourceMatchers[].names**：（可選）要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
- **resourceMatchers[].namespaces**：（可選）要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
- **resourceMatchers[].labelSelectors**：（可選）資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如：
"trident.netapp.io/os=linux"。



當兩者 resourceFilter 和 labelSelector 同時使用時，resourceFilter 首先運行，然後 labelSelector 將應用於生成的資源。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

◦ 僅限 **PVC** 的篩選器範例：

要定義僅限 PVC 的應用程式、您還必須在資源篩選器中包含 PersistentVolume 和 VolumeSnapshotClass。快照和備份操作依賴 PersistentVolume（綁定到每個 PVC 的叢集範圍磁碟區）和 VolumeSnapshotClass（快照驅動程式），缺少它們將會失敗。例如：

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: my-pvc-app
```

```

namespace: my-app-namespace
spec:
  includedNamespaces:
  - namespace: my-app-namespace
  resourceFilter:
    resourceMatchers:
    - kind: PersistentVolumeClaim
      version: v1
    - kind: PersistentVolume
      version: v1
    - kind: VolumeSnapshotClass
      version: v1
    resourceSelectionCriteria: Include

```

2. 建立與您的環境相符的應用程式 CR 後、套用該 CR。例如：

```
kubectl apply -f maria-app.yaml
```

步驟

1. 使用以下範例之一建立並應用應用程式定義，並將括號中的值替換為您環境中的資訊。您可以使用範例中所示的參數，以逗號分隔的清單在應用程式定義中包含命名空間和資源。

建立應用程式時、您可以選擇使用註解來指定應用程式在快照期間是否可以寫入檔案系統。這僅適用於從虛擬機器定義的應用程式、例如在 KubeVirt 環境中、快照之前會發生檔案系統凍結。如果將註解設為 true、則應用程式會忽略全域設定、並可在快照期間寫入檔案系統。如果將其設為 false、則應用程式會忽略全域設定、且檔案系統會在快照期間凍結。如果您使用註解、但應用程式定義中沒有虛擬機器、則會忽略該註解。如果您不使用註解、則應用程式會遵循["全球 Trident Protect 凍結設定"](#)。

+ 在使用 CLI 建立應用程式時，若要指定註釋，可以使用 `--annotation` 標誌。

+ * 建立應用程式並使用全域設定來控制檔案系統凍結行為：

+

```

tridentctl-protect create application <my_new_app_cr_name> --namespaces
<namespaces_to_include> --csr <cluster_scoped_resources_to_include>
--namespace <my-app-namespace>

```

+ * 建立應用程式並配置本機應用程式設定以控制檔案系統凍結行為：

+

```

tridentctl-protect create application <my_new_app_cr_name> --namespaces
<namespaces_to_include> --csr <cluster_scoped_resources_to_include>
--namespace <my-app-namespace> --annotation

```

```
protect.trident.netapp.io/skip-vm-freeze=<"true"|"false">
```

+ * 您可以使用 `--resource-filter-include` 和 `--resource-filter-exclude` 標誌，根據 `resourceSelectionCriteria`（例如群組、種類、版本、標籤、名稱和命名空間）來包含或排除資源，如下例所示：

+

```
tridentctl-protect create application <my_new_app_cr_name> --namespaces
<namespaces_to_include> --csr <cluster_scoped_resources_to_include>
--namespace <my-app-namespace> --resource-filter-include
' [{"Group": "apps", "Kind": "Deployment", "Version": "v1", "Names": ["my-
deployment"], "Namespaces": ["my-namespace"], "LabelSelectors": ["app=my-
app"]} ] '
```

+ * 要定義僅限 PVC 的應用程式，您還必須在資源篩選器中包含 `PersistentVolume` 和 `VolumeSnapshotClass`。快照和備份操作依賴 `PersistentVolume`（綁定到每個 PVC 的叢集範圍磁碟區）和 `VolumeSnapshotClass`（快照驅動程式），缺少它們將會失敗。例如：

+

```
tridentctl-protect create app my-pvc-app --namespaces <my-app-
namespace> --resource-filter-include
' [{"Kind": "PersistentVolumeClaim", "Version": "v1"}, {"Kind": "PersistentVo
lume", "Version": "v1"}, {"Kind": "VolumeSnapshotClass", "Version": "v1"} ] '
-n <my-app-namespace>
```

使用 Trident Protect 保護應用程式

您可以使用自動保護原則或臨機方式拍攝快照和備份，以保護 Trident Protect 管理的所有應用程式。



您可以設定 Trident Protect 在資料保護作業期間凍結及解除凍結檔案系統。["深入瞭解如何使用 Trident Protect 設定檔案系統凍結"](#)。

建立隨需快照

您可以隨時建立隨需快照。



如果叢集範圍的資源在應用程式定義中被明確引用，或引用了任何應用程式命名空間，則這些資源將包含在備份、快照或複製中。

使用 CR 建立快照

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `trident-protect-snapshot-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.applicationRef**：要建立快照的應用程式的 Kubernetes 名稱。
 - **spec.appVaultRef**：（必填）應儲存快照內容（元資料）的 AppVault 名稱。
 - **spec.reclaimPolicy**：（選用）定義當快照 CR 刪除時，快照的 AppArchive 會發生什麼情況。這意味著即使設為 `Retain`，快照也會被刪除。有效選項：
 - `Retain` (預設)
 - `Delete`

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Delete
```

3. 在 `trident-protect-snapshot-cr.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-snapshot-cr.yaml
```

使用 CLI 建立快照

步驟

1. 建立快照，並將括號中的值替換為您環境中的資訊。例如：

```
tridentctl-protect create snapshot <my_snapshot_name> --appvault
<my_appvault_name> --app <name_of_app_to_snapshot> -n
<application_namespace>
```

建立隨需備份

您可以隨時備份應用程式。



如果叢集範圍的資源在應用程式定義中被明確引用，或引用了任何應用程式命名空間，則這些資源將包含在備份、快照或複製中。

開始之前

請確保 AWS 會話令牌的有效期限足以應付任何長時間運行的 s3 備份作業。如果令牌在備份作業期間過期，則操作可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 說明文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 說明文件"](#)。

使用 CR 建立備份

步驟

1. 建立自訂資源 (CR) 檔案並將其命名為 `trident-protect-backup-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：(必填) 此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.applicationRef**：(必需) 要備份的應用程式的 Kubernetes 名稱。
 - **spec.appVaultRef**：(必填) 應儲存備份內容的 AppVault 名稱。
 - **spec.dataMover**：(選用) 一個字串，指示要用於備份作業的備份工具。可能的值 (區分大小寫)：
 - Restic
 - Kopia (預設)
 - **spec.reclaimPolicy**：(選用) 定義備份從其聲明中釋放後會發生什麼。可選值：
 - Delete
 - Retain (預設)
 - **spec.snapshotRef**：(可選)：要用作備份來源的快照名稱。如果未提供，則會建立並備份一個臨時快照。

YAML 範例：

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: Kopia
```

3. 在 `trident-protect-backup-cr.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-backup-cr.yaml
```

使用 CLI 建立備份

步驟

1. 建立備份，並將括號中的值替換為您環境中的資訊。例如：

```
tridentctl-protect create backup <my_backup_name> --appvault <my-vault-name> --app <name_of_app_to_back_up> --data-mover <Kopia_or_Restic> -n <application_namespace>
```

您可以選擇使用 `--full-backup` 標誌來指定備份是否為非增量備份。預設情況下，所有備份都是增量備份。使用此標誌後，備份將變為非增量備份。最佳實踐是定期執行完整備份，並在兩次完整備份之間執行增量備份，以最大程度地降低還原風險。

支援的備份註釋

下表說明建立備份 CR 時可使用的註解：

註解	類型	說明	預設值
<code>protect.trident.netapp.io/full-backup</code>	字串	指定備份是否為非增量備份。設定為 <code>'true'</code> 可建立非增量備份。最佳實踐是定期執行完整備份，並在兩次完整備份之間執行增量備份，以最大程度地降低還原風險。	<code>"false"</code>
<code>protect.trident.netapp.io/snapshots-hot-completion-timeout</code>	字串	允許完成整個快照作業的最長時間。	<code>"60 分鐘"</code>
<code>protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout</code>	字串	磁碟區快照達到可用狀態所允許的最長時間。	<code>"30 分鐘"</code>
<code>protect.trident.netapp.io/volume-snapshots-created-timeout</code>	字串	建立磁碟區快照所允許的最長時間。	<code>"5 分鐘"</code>
<code>protect.trident.netapp.io/pvc-bind-timeout-sec</code>	字串	等待所有新建立的 PersistentVolumeClaims (PVC) 達到 <code>'Bound'</code> 階段的最長時間（以秒為單位），超過此時間操作將會失敗。	<code>"1200"</code> （20 分鐘）

建立資料保護排程

保護原則透過按定義的排程建立快照、備份或兩者來保護應用程式。您可以選擇每小時、每天、每週和每月建立快照和備份，並可指定要保留的副本數量。您可以使用 `full-backup-rule` 註解來排程非增量完整備份。預設情況下，所有備份都是增量備份。定期執行完整備份以及其間的增量備份，有助於降低與還原相關的風險。



- 您可以透過將 `'backupRetention'` 設為零並將 `'snapshotRetention'` 設為大於零的值來建立僅用於快照的排程。將 `'snapshotRetention'` 設為零表示任何排程的備份仍會建立快照，但這些快

照是暫時的，並會在備份完成後立即刪除。

- 如果叢集範圍的資源在應用程式定義中被明確引用，或引用了任何應用程式命名空間，則這些資源將包含在備份、快照或複製中。

使用 CR 建立排程

步驟

1. 建立自訂資源 (CR) 檔案並將其命名為 `trident-protect-schedule-cr.yaml`。

2. 在您建立的檔案中、設定以下屬性：

- **metadata.name**：(必填) 此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
- **spec.dataMover**：(選用) 一個字串，指示要用於備份作業的備份工具。可能的值 (區分大小寫)：
 - Restic
 - Kopia (預設)
- **spec.applicationRef**：要備份的應用程式的 Kubernetes 名稱。
- **spec.appVaultRef**：(必填) 應儲存備份內容的 AppVault 名稱。
- **spec.backupRetention**：(必填) 要保留的備份數量。零表示不應建立任何備份 (僅快照)。
- **spec.backupReclaimPolicy**：(選用) 決定如果在保留期間內刪除備份 CR 時，備份會發生什麼情況。保留期間過後，備份一律會被刪除。可能的值 (區分大小寫)：
 - Retain (預設)
 - Delete
- **spec.snapshotRetention**：(必填) 要保留的快照數量。零表示不建立任何快照。
- **spec.snapshotReclaimPolicy**：(選用) 決定在保留期間內刪除快照 CR 時，快照會發生什麼情況。保留期間過後，快照一律會被刪除。可能的值 (區分大小寫)：
 - Retain
 - Delete (預設)
- **spec.granularity**：排程應執行的頻率。可能的值以及相關的必填欄位：
 - Hourly (需要您指定 `spec.minute`)
 - Daily (需要您指定 `spec.minute` 和 `spec.hour`)
 - Weekly (需要您指定 `spec.minute`, `spec.hour`、`spec.dayOfWeek`)
 - Monthly (需要您指定 `spec.minute`, `spec.hour`、`spec.dayOfMonth`)
 - Custom
- **spec.dayOfMonth**：(選用) 排程應執行的月份日期 (1 - 31)。如果精細度設為 `Monthly`，則此欄位為必填項。該值必須以字串形式提供。
- **spec.dayOfWeek**：(選用) 排程應執行的星期幾 (0 - 7)。值為 0 或 7 表示星期日。如果精細度設為 `Weekly`，則此欄位為必填項。該值必須以字串形式提供。
- **spec.hour**：(選用) 排程應執行的一天中的小時 (0 - 23)。如果粒度設定為 `Daily`、`Weekly`、

或 `Monthly`，則此欄位為必填項。該值必須以字串形式提供。

- **spec.minute**：（選用）排程應執行的小時分鐘數（0 - 59）。如果粒度設定為 `Hourly``、`Daily``、`Weekly`` 或 `Monthly``，則此欄位為必填項。該值必須以字串形式提供。
- **spec.runImmediately**：（選用）設定為 `true`` 以在建立排程時觸發一次性立即基準執行（根據保留設定進行備份和 / 或快照）。預設為 `false``。這不會修改後續的重複執行。

備份和快照排程的範例 YAML：

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  dataMover: Kopia
  applicationRef: my-application
  appVaultRef: appvault-name
  backupRetention: "15"
  snapshotRetention: "15"
  granularity: Daily
  hour: "0"
  minute: "0"
```

僅快照排程的範例 YAML：

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  namespace: my-app-namespace
  name: my-snapshot-schedule
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  backupRetention: "0"
  snapshotRetention: "15"
  granularity: Daily
  hour: "2"
  minute: "0"
```

範例 YAML 文件，用於實現立即運行的排程任務：

```

---
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  namespace: my-app-namespace
  name: my-daily-schedule-run-immediately
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  backupRetention: "7"
  snapshotRetention: "7"
  granularity: Daily
  hour: "3"
  minute: "0"
  runImmediately: true

```

3. 在 trident-protect-schedule-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-schedule-cr.yaml
```

使用 CLI 建立排程

步驟

1. 建立保護排程，並將括號中的值替換為您環境中的資訊。例如：



您可以使用 `tridentctl-protect create schedule --help` 來查看此命令的詳細說明資訊。

```

tridentctl-protect create schedule <my_schedule_name> \
  --appvault <my_appvault_name> \
  --app <name_of_app_to_snapshot> \
  --backup-retention <how_many_backups_to_retain> \
  --backup-reclaim-policy <Retain|Delete (default Retain)> \
  --data-mover <Kopia_or_Restic> \
  --day-of-month <day_of_month_to_run_schedule> \
  --day-of-week <day_of_week_to_run_schedule> \
  --granularity <frequency_to_run> \
  --hour <hour_of_day_to_run> \
  --minute <minute_of_hour_to_run> \
  --recurrence-rule <recurrence> \
  --snapshot-retention <how_many_snapshots_to_retain> \
  --snapshot-reclaim-policy <Retain|Delete (default Delete)> \
  --full-backup-rule <string> \
  --run-immediately <true|false> \

```

```
-n <application_namespace>
```

以下旗標可讓您對排程進行更多控制：

- 完整備份排程：使用 `--full-backup-rule` 標誌來排程非增量完整備份。此標誌僅適用於 `--granularity Daily`。可選值：

- `Always`：每天都要建立完整備份。
- 特定工作日：指定一個或多個以逗號分隔的日期（例如，`"Monday, Thursday"`）。有效值：`Monday`、`Tuesday`、`Wednesday`、`Thursday`、`Friday`、`Saturday`、`Sunday`。



`--full-backup-rule` 標誌不適用於每小時、每週或每月粒度。

- 立即基線保護：使用 `--run-immediately true` 在建立排程時立即建立初始備份或快照，而不是等待首次排程執行時間。預設為 `false`。
- 僅快照排程：設定 `--backup-retention 0` 並為 `--snapshot-retention` 指定大於零的值。

支援的排程註釋

下表描述了建立排程 CR 時可以使用的註釋：

註解	類型	說明	預設值
<code>protect.trident.netapp.io/full-backup-rule</code>	字串	指定完整備份的調度規則。您可以將其設定為 <code>Always</code> 、持續完整備份，或根據您的需求進行自訂。例如，如果您選擇每日粒度，則可以指定執行完整備份的星期幾（例如， <code>"Monday, Thursday"</code> ）。有效的星期幾值為：星期一、星期二、星期三、星期四、星期五、星期六、星期日。請注意，此註解只能與已將 <code>'granularity'</code> 設定為 <code>'Daily'</code> 的計劃一起使用。	未設定（所有備份均為增量備份）
<code>protect.trident.netapp.io/snapshot-completion-timeout</code>	字串	允許完成整個快照作業的最長時間。	"60 分鐘"
<code>protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout</code>	字串	磁碟區快照達到可用狀態所允許的最長時間。	"30 分鐘"
<code>protect.trident.netapp.io/volume-snapshots-created-timeout</code>	字串	建立磁碟區快照所允許的最長時間。	"5 分鐘"
<code>protect.trident.netapp.io/pvc-bind-timeout-sec</code>	字串	等待所有新建立的 <code>PersistentVolumeClaims</code> (PVC) 達到 <code>'Bound'</code> 階段的最長時間（以秒為單位），超過此時間操作將會失敗。	"1200"（20 分鐘）

刪除快照

刪除不再需要的已排程或隨需快照。

步驟

1. 刪除與快照相關聯的快照 CR：

```
kubectl delete snapshot <snapshot_name> -n my-app-namespace
```

刪除備份

刪除不再需要的排程備份或隨需備份。



請確保將回收策略設定為 Delete，以從物件儲存中刪除所有備份資料。此策略的預設設定為 Retain，以避免意外資料遺失。如果未將策略變更為 Delete，則備份資料將保留在物件儲存中，需要手動刪除。

步驟

1. 刪除與備份相關聯的備份 CR：

```
kubectl delete backup <backup_name> -n my-app-namespace
```

檢查備份作業的狀態

您可以使用命令列來檢查正在進行、已完成或已失敗的備份作業狀態。

步驟

1. 使用以下命令檢索備份作業的狀態，將括號中的值替換為您環境中的資訊：

```
kubectl get backup -n <namespace_name> <my_backup_cr_name> -o jsonpath='{.status}'
```

啟用 **azure-netapp-files** (ANF) 作業的備份和還原

如果您已安裝 Trident Protect，則可以為使用 azure-netapp-files 儲存類別且在 Trident 24.06 之前建立的儲存後端啟用節省空間的備份和還原功能。此功能適用於 NFSv4 磁碟區，並且不會佔用容量池中的額外空間。

開始之前

請確保以下事項：

- 您已安裝 Trident Protect。
- 您已在 Trident Protect 中定義了一個應用程式。在您完成此程序之前，該應用程式的保護功能將受到限制。
- 您已選擇 `azure-netapp-files` 作為儲存後端的預設儲存類別。

▼ 展開以檢視設定步驟

1. 如果 ANF 磁碟區是在升級到 Trident 24.10 之前建立的，請在 Trident 中執行以下操作：
 - a. 為每個基於 azure-netapp-files 且與應用程式相關聯的 PV 啟用 Snapshot 目錄：

```
tridentctl update volume <pv name> --snapshot-dir=true -n trident
```

b. 確認已為每個關聯的 PV 啟用 Snapshot 目錄：

```
tridentctl get volume <pv name> -n trident -o yaml | grep  
snapshotDir
```

回應：

```
snapshotDirectory: "true"
```

+

如果未啟用快照目錄，Trident Protect 將選擇常規備份功能，該功能會在備份過程中暫時佔用容量池中的空間。在這種情況下，請確保容量池中有足夠的空間來建立一個與待備份磁碟區大小相同的臨時磁碟區。

結果

該應用程式已準備好使用 Trident Protect 進行備份和還原。每個 PVC 也可供其他應用程式用於備份和還原。

還原應用程式

使用 **Trident Protect** 恢復應用程式

您可以使用 Trident Protect 從快照或備份還原應用程式。如果要將應用程式還原到同一個叢集，從現有快照還原速度會更快。



- 還原應用程式時，所有為該應用程式配置的執行鉤子都會隨應用程式一起還原。如果存在復原後執行鉤子，它會在復原操作過程中自動執行。
- qtree 磁碟區支援從備份還原到不同的命名空間或原始命名空間。但是，qtree 磁碟區不支援從快照還原到不同的命名空間或原始命名空間。
- 您可以使用進階設定來自訂還原操作。若要深入瞭解，請參閱 ["使用進階 Trident Protect 還原設定"](#)。
- 若要從歸檔中復原特定的 KubeVirt 虛擬機器 (VM) 而不還原所有命名空間資源，請使用復原 CR 上的 `includedVirtualMachines` 欄位。有關支援的 CR、欄位參考和 YAML 範例，請參閱 ["使用 Trident Protect 保護 KubeVirt 虛擬機器"](#)。

從備份還原到不同的命名空間

當您使用 BackupRestore CR 將備份還原到不同的命名空間時，Trident Protect 會在新的命名空間中還原應用程式，並為還原後的應用程式建立一個應用程式 CR。若要保護還原的應用程式，您可以建立隨需備份或快照，或建立保護排程。



- 將備份還原到具有現有資源的不同命名空間不會變更與備份中資源同名的任何資源。若要還原備份中的所有資源，請刪除並重新建立目標命名空間，或將備份還原到新的命名空間。
- 使用 CR 還原到新命名空間時，必須先手動建立目標命名空間，然後再套用 CR。Trident

Protect 僅在使用 CLI 時才會自動建立命名空間。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期、作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 說明文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 說明文件"](#)。



當您使用 Kopia 作為資料移動工具還原備份時，您可以選擇在 CR 中或使用 CLI 指定註釋，以控制 Kopia 使用的暫存的行為。有關可配置選項的更多資訊，請參閱 ["Kopia 說明文件"](#)。使用 ``tridentctl-protect create --help`` 命令以取得有關使用 Trident Protect CLI 指定註釋的更多資訊。

使用 CR

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `trident-protect-backup-restore-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appArchivePath**：AppVault 內儲存備份內容的路徑。您可以使用以下命令來尋找此路徑：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o  
jsonpath='{.status.appArchivePath}'
```

- **spec.appVaultRef**：（必填）儲存備份內容的 AppVault 名稱。
- **spec.destinationApplicationName**：（選用）還原應用程式的名稱。如果提供、還原的應用程式會使用此名稱。如果未提供、還原的應用程式會使用來源應用程式名稱。
- **spec.namespaceMapping**：復原作業的來源命名空間到目標命名空間的對應。請將 ``my-source-namespace`` 和 ``my-destination-namespace`` 替換為您環境中的資訊。

```
---  
apiVersion: protect.trident.netapp.io/v1  
kind: BackupRestore  
metadata:  
  name: my-cr-name  
  namespace: my-destination-namespace  
spec:  
  appArchivePath: my-backup-path  
  appVaultRef: appvault-name  
  destinationApplicationName: my-new-app-name  
  namespaceMapping: [{"source": "my-source-namespace",  
"destination": "my-destination-namespace"}]
```

3. (可選) 如果您只需要選擇應用程式的某些資源進行恢復，請新增篩選條件，以包含或排除帶有特定標籤的資源：



Trident Protect 會自動選擇一些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持續性磁碟區宣告資源，且該資源關聯了一個 Pod，則 Trident Protect 也會還原該關聯 Pod。

- **resourceFilter.resourceSelectionCriteria**：(篩選必需) 使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：
 - **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，它們之間將按 OR 運算匹配，每個元素內的欄位 (group、kind、version) 之間將按 AND 運算匹配。
 - **resourceMatchers[].group**：(可選) 要篩選的資源群組。
 - **resourceMatchers[].kind**：(可選) 要篩選的資源類型。
 - **resourceMatchers[].version**：(可選) 要篩選的資源版本。
 - **resourceMatchers[].names**：(可選) 要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
 - **resourceMatchers[].namespaces**：(可選) 要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
 - **resourceMatchers[].labelSelectors**：(可選) 資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如：
"trident.netapp.io/os=linux"。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 trident-protect-backup-restore-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

使用 CLI

步驟

1. 將備份還原到不同的命名空間，並將方括號中的值替換為您環境中的資訊。namespace-mapping`引數使用冒號分隔的命名空間，將來源命名空間對應到正確的目標命名空間，格式為`source1:dest1,source2:dest2`。例如：

```
tridentctl-protect create backuprestore <my_restore_name> \  
--backup <backup_namespace>/<backup_to_restore> \  
--namespace-mapping <source_to_destination_namespace_mapping> \  
--destination-app-name<custom_app_name>\  
-n <application_namespace>
```

從備份還原到原始命名空間

您可以隨時將備份還原到原始命名空間。執行就地還原時，Trident Protect 會自動管理保護排程和進行中的作業，以防止無效的還原點：

- 在還原開始之前，應用程式的所有已啟用保護排程都會停用。這可防止在還原應用程式資源時執行排程的備份或快照。
- 恢復成功完成後，只有恢復前已啟用的排程會重新啟用。先前已停用的排程仍保持停用狀態。
- 任何正在進行的備份或快照操作都會在還原開始前取消。如果操作在 5 分鐘內未取消，則還原將繼續進行，並在還原 CR 狀態中記錄警告。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期、作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 說明文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 說明文件"](#)。



當您使用 Kopia 作為資料移動工具還原備份時，您可以選擇在 CR 中或使用 CLI 指定註釋，以控制 Kopia 使用的暫存的行為。有關可配置選項的更多資訊，請參閱 ["Kopia 說明文件"](#)。使用`tridentctl-protect create --help`命令以取得有關使用 Trident Protect CLI 指定註釋的更多資訊。

使用 CR

步驟

1. 建立自訂資源（CR）檔案並將其命名為 trident-protect-backup-ipr-cr.yaml。
2. 在您建立的檔案中、設定以下屬性：

- **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。

- **spec.appArchivePath**：AppVault 內儲存備份內容的路徑。您可以使用以下命令來尋找此路徑：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o  
jsonpath='{.status.appArchivePath}'
```

- **spec.appVaultRef**：（必填）儲存備份內容的 AppVault 名稱。

例如：

```
---  
apiVersion: protect.trident.netapp.io/v1  
kind: BackupInplaceRestore  
metadata:  
  name: my-cr-name  
  namespace: my-app-namespace  
spec:  
  appArchivePath: my-backup-path  
  appVaultRef: appvault-name
```

3. （可選）如果您只需要選擇應用程式的某些資源進行恢復，請新增篩選條件，以包含或排除帶有特定標籤的資源：



Trident Protect 會自動選擇一些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持續性磁碟區宣告資源，且該資源關聯了一個 Pod，則 Trident Protect 也會還原該關聯 Pod。

- **resourceFilter.resourceSelectionCriteria**：（篩選必需）使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：

- **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，它們之間將按 OR 運算匹配，每個元素內的欄位（group、kind、version）之間將按 AND 運算匹配。

- **resourceMatchers[].group**：（可選）要篩選的資源群組。
- **resourceMatchers[].kind**：（可選）要篩選的資源類型。
- **resourceMatchers[].version**：（可選）要篩選的資源版本。
- **resourceMatchers[].names**：（可選）要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
- **resourceMatchers[].namespaces**：（可選）要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
- **resourceMatchers[].labelSelectors**：（可選）資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如：
"trident.netapp.io/os=linux"。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 trident-protect-backup-ipr-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

使用 CLI

步驟

1. 將備份還原到原始命名空間，並將方括號中的值替換為您環境中的資訊。backup 參數使用命名空間和備份名稱，格式為 <namespace>/<name>。例如：

```
tridentctl-protect create backupinplacerestore <my_restore_name> \
--backup <namespace/backup_to_restore> \
-n <application_namespace>
```

從備份還原到不同的叢集

如果原始叢集出現問題、您可以將備份還原至不同的叢集。



- 當您使用 Kopia 作為資料移動工具還原備份時，您可以選擇在 CR 中或使用 CLI 指定註釋，以控制 Kopia 使用的暫存的行為。有關可配置選項的更多資訊，請參閱 ["Kopia 說明文件"](#)。使用 `tridentctl-protect create --help` 命令以取得有關使用 Trident Protect CLI 指定註釋的更多資訊。
- 使用 CR 還原到新命名空間時，必須先手動建立目標命名空間，然後再套用 CR。Trident Protect 僅在使用 CLI 時才會自動建立命名空間。

開始之前

請確保符合下列先決條件：

- 目標叢集已安裝 Trident Protect。
- 目標叢集可以存取與來源叢集相同的 AppVault 儲存桶路徑，備份檔案就儲存在該路徑中。
- 執行 `tridentctl-protect get appvaultcontent` 命令時，請確保本機環境可以連接到 AppVault CR 中定義的物件儲存桶。如果網路限制導致無法存取，請改為在目標叢集的 Pod 內執行 Trident Protect CLI。
- 請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的還原作業。如果權杖在還原作業期間過期、作業可能會失敗。
 - 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 說明文件"](#)。
 - 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS 文件"](#)。

步驟

1. 使用 Trident Protect CLI 外掛程式驗證 AppVault CR 是否存在於目標叢集上：

```
tridentctl-protect get appvault --context <destination_cluster_name>
```



如果目標叢集上不存在 AppVault CR，請按照 ["使用 Trident Protect AppVault 物件來管理儲存桶"](#) 中的步驟建立它。

2. 查看目標叢集上可用 AppVault 的備份內容，並記下 `appArchivePath` 要還原的備份：

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

執行此命令將顯示 AppVault 中的可用備份，包括其來源叢集、相應的應用程式名稱、時間戳記和歸檔路徑。

範例輸出：

```
+-----+-----+-----+-----+
+-----+-----+-----+
| CLUSTER | APP | TYPE | NAME | TIMESTAMP |
| PATH |
+-----+-----+-----+-----+
+-----+-----+
| production1 | wordpress | backup | wordpress-bkup-1 | 2024-10-30
08:37:40 (UTC) | backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2 | 2024-10-30
08:37:40 (UTC) | backuppath2 |
+-----+-----+-----+-----+
```

+-----+-----+

3. 使用 AppVault 名稱和歸檔路徑將應用程式還原到目標叢集：



使用 CR 時，請確保用於應用程式還原的命名空間存在於目的地叢集上。

使用 CR

1. 建立自訂資源 (CR) 檔案並將其命名為 `trident-protect-backup-restore-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：(必填) 此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appVaultRef**：(必填) 儲存備份內容的 AppVault 名稱。
 - **spec.appArchivePath**：(必填) AppVault 內儲存備份內容的路徑。使用步驟 2 中的指令查看備份內容，並找到 `appArchivePath` 要還原的備份。
 - **spec.destinationApplicationName**：(選用) 還原應用程式的名稱。如果提供、還原的應用程式會使用此名稱。如果未提供、還原的應用程式會使用來源應用程式名稱。
 - **spec.namespaceMapping**：復原作業的來源命名空間到目標命名空間的對應。請將 `my-source-namespace` 和 `my-destination-namespace` 替換為您環境中的資訊。

例如：

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  destinationApplicationName: my-new-app-name
  namespaceMapping: [{"source": "my-source-namespace", "
destination": "my-destination-namespace"}]
```

3. 在 `trident-protect-backup-restore-cr.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

使用 CLI

1. 使用以下命令恢復應用程式，並將方括號中的值替換為您環境中的資訊。命名空間映射參數使用冒號分隔的命名空間，將來源命名空間對應到正確的目標命名空間，格式為 `source1:dest1,source2:dest2`。
例如：

```
tridentctl-protect create backuprestore <restore_name> \
--namespace-mapping <source_to_destination_namespace_mapping> \
--appvault <appvault_name> \
--path <backup_path> \
--destination-app-name <custom_app_name> \
--context <destination_cluster_name> \
-n <application_namespace>
```

從快照還原到不同的命名空間

您可以使用自訂資源（CR）檔案從快照還原資料，還原到不同的命名空間或原始來源命名空間。當您使用 SnapshotRestore CR 將快照還原到不同的命名空間時，Trident Protect 會在新的命名空間中還原應用程式，並為還原的應用程式建立一個應用程式 CR。若要保護還原的應用程式，您可以建立隨需備份或快照，或建立保護排程。



- SnapshotRestore 支援 `spec.storageClassMapping` 屬性，但僅當來源儲存類別和目標儲存類別使用相同的儲存後端時才支援。如果嘗試還原到使用不同儲存後端的 `StorageClass`，則還原操作將會失敗。
- 使用 CR 還原到新命名空間時，必須先手動建立目標命名空間，然後再套用 CR。Trident Protect 僅在使用 CLI 時才會自動建立命名空間。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期、作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 說明文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 說明文件"](#)。

使用 CR

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `trident-protect-snapshot-restore-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appVaultRef**：（必填）儲存快照內容的 AppVault 名稱。
 - **spec.appArchivePath**：AppVault 內儲存快照內容的路徑。您可以使用以下命令來尋找此路徑：

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
jsonpath='{.status.appArchivePath}'
```

- **spec.destinationApplicationName**：（選用）還原應用程式的名稱。如果提供、還原的應用程式會使用此名稱。如果未提供、還原的應用程式會使用來源應用程式名稱。

- **spec.namespaceMapping**：復原作業的來源命名空間到目標命名空間的對應。請將 `my-source-namespace` 和 `my-destination-namespace` 替換為您環境中的資訊。

```
---
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
  namespaceMapping: [{"source": "my-source-namespace",
"destination": "my-destination-namespace"}]
```

3. (可選) 如果您只需要選擇應用程式的某些資源進行恢復，請新增篩選條件，以包含或排除帶有特定標籤的資源：



Trident Protect 會自動選擇一些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持續性磁碟區宣告資源，且該資源關聯了一個 Pod，則 Trident Protect 也會還原該關聯 Pod。

- **resourceFilter.resourceSelectionCriteria**：(篩選必需) 使用 `Include` 或 `Exclude` 來包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：

- **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，它們之間將按 OR 運算匹配，每個元素內的欄位 (group、kind、version) 之間將按 AND 運算匹配。

- **resourceMatchers[].group**：(可選) 要篩選的資源群組。
- **resourceMatchers[].kind**：(可選) 要篩選的資源類型。
- **resourceMatchers[].version**：(可選) 要篩選的資源版本。
- **resourceMatchers[].names**：(可選) 要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。
- **resourceMatchers[].namespaces**：(可選) 要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。
- **resourceMatchers[].labelSelectors**：(可選) 資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如：
"trident.netapp.io/os=linux"。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
```

```
resourceMatchers:
- group: my-resource-group-1
  kind: my-resource-kind-1
  version: my-resource-version-1
  names: ["my-resource-names"]
  namespaces: ["my-resource-namespaces"]
  labelSelectors: ["trident.netapp.io/os=linux"]
- group: my-resource-group-2
  kind: my-resource-kind-2
  version: my-resource-version-2
  names: ["my-resource-names"]
  namespaces: ["my-resource-namespaces"]
  labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 `trident-protect-snapshot-restore-cr.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

使用 CLI

步驟

1. 將快照還原到不同的命名空間，並將括號中的值替換為您環境中的資訊。

- `snapshot`` 引數使用命名空間和快照名稱，格式為 ``<namespace>/<name>``。
- `namespace-mapping`` 引數使用冒號分隔的命名空間，將來源命名空間對應到正確的目標命名空間，格式為 ``source1:dest1,source2:dest2``。

例如：

```
tridentctl-protect create snapshotrestore <my_restore_name> \
--snapshot <namespace/snapshot_to_restore> \
--namespace-mapping <source_to_destination_namespace_mapping> \
--destination-app-name <custom_app_name> \
-n <application_namespace>
```

從快照還原到原始命名空間

您可以隨時將快照還原到原始命名空間。執行就地還原時，Trident Protect 會自動管理保護排程和進行中的作業，以防止無效的還原點：

- 在還原開始之前，應用程式的所有已啟用保護排程都會停用。這可防止在還原應用程式資源時執行排程的備份或快照。
- 恢復成功完成後，只有恢復前已啟用的排程會重新啟用。先前已停用的排程仍保持停用狀態。
- 任何正在進行的備份或快照操作都會在還原開始前取消。如果操作在 5 分鐘內未取消，則還原將繼續進行，並在還原 CR 狀態中記錄警告。

開始之前

請確保 AWS 工作階段權杖的有效期限足以應付任何長時間執行的 s3 還原作業。如果權杖在還原作業期間過期、作業可能會失敗。

- 有關檢查當前會話令牌過期時間的更多資訊，請參閱 ["AWS API 說明文件"](#)。
- 如需 AWS 資源憑證的詳細資訊，請參閱 ["AWS IAM 說明文件"](#)。

使用 CR

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `trident-protect-snapshot-ipr-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appVaultRef**：（必填）儲存快照內容的 AppVault 名稱。
 - **spec.appArchivePath**：AppVault 內儲存快照內容的路徑。您可以使用以下命令來尋找此路徑：

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o  
jsonpath='{.status.appArchivePath}'
```

```
---  
apiVersion: protect.trident.netapp.io/v1  
kind: SnapshotInplaceRestore  
metadata:  
  name: my-cr-name  
  namespace: my-app-namespace  
spec:  
  appVaultRef: appvault-name  
  appArchivePath: my-snapshot-path
```

+ .（可選）如果您只需要選擇應用程式的某些資源進行恢復，請新增篩選條件，以包含或排除帶有特定標籤的資源：

+ 注意：Trident Protect 會自動選擇某些資源，因為它們與您選擇的資源有關聯。例如，如果您選擇了持續性磁碟區宣告資源，且該資源關聯了一個 Pod，則 Trident Protect 也會還原該關聯 Pod。

+ * **resourceFilter.resourceSelectionCriteria**:（過濾必要）使用 `Include`` 或 `Exclude`` 來包含或排除在 `resourceMatchers` 中定義的資源。新增下列 `resourceMatchers` 參數來定義要包含或排除的資源：**resourceFilter.resourceMatchers:resourceMatcher** 物件的陣列。如果在此陣列中定義多個元素，它們之間將按 `OR` 運算匹配，每個元素內的欄位（`group`、`kind`、`version`）之間將按 `AND` 運算匹配。* **resourceMatchers[].group**:（可選）要篩選的資源群組。* **resourceMatchers[].kind**:（可選）要篩選的資源種類。* **resourceMatchers[].version**:（可選）要篩選的資源版本。* **resourceMatchers[].names**:（可選）要篩選的資源的 Kubernetes `metadata.name` 欄位中的名稱。* **resourceMatchers[].namespaces**:（可選）要篩選的資源的 Kubernetes `metadata.name` 欄位中的命名空間。*

resourceMatchers[].labelSelectors: (可選) 資源的 `Kubernetes metadata.name` 欄位中的標籤選擇器字串，如 ["Kubernetes 說明文件"](#)中所定義。例如：

`"trident.netapp.io/os=linux"`。

+ 例如：

+

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

+ 在 `trident-protect-snapshot-ipr-cr.yaml` 檔案中填入正確的值後，套用 CR：

+

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

使用 CLI

步驟

1. 將快照還原到原始命名空間，並將方括號中的值替換為您環境中的資訊。例如：

```
tridentctl-protect create snapshotinplacerestore <my_restore_name> \
--snapshot <namespace/snapshot_to_restore> \
-n <application_namespace>
```

檢查還原作業的狀態

您可以使用命令列來檢查正在進行、已完成或已失敗的還原作業狀態。

步驟

1. 使用以下命令檢索還原作業的狀態，將方括號中的值替換為您環境中的資訊：

```
kubectl get backuprestore -n <namespace_name> <my_restore_cr_name> -o  
jsonpath='{.status}'
```

使用進階 Trident Protect 還原設定

您可以利用註釋、命名空間設定和儲存選項等進階設定來自訂還原作業，以滿足您的特定需求。

還原和容錯移轉作業期間的命名空間註釋和標籤

在還原和容錯移轉作業期間，目的地命名空間中的標籤和註釋會與來源命名空間中的標籤和註釋相符。來源命名空間中存在但目的地命名空間中不存在的標籤或註釋會被新增，而任何已存在的標籤或註釋則會被覆寫以符合來源命名空間中的值。僅存在於目的地命名空間中的標籤或註釋則保持不變。



如果您使用 Red Hat OpenShift，請務必注意命名空間註解在 OpenShift 環境中的關鍵作用。命名空間註解可確保復原的 Pod 遵循 OpenShift 安全上下文約束（SCC）定義的相應權限和安全性配置，並能無權限問題地存取磁碟區。如需詳細資訊，請參閱 ["OpenShift 安全上下文約束文檔"](#)。

您可以透過在執行復原或故障轉移操作之前設定 Kubernetes 環境變數

RESTORE_SKIP_NAMESPACE_ANNOTATIONS，來防止目標命名空間中的特定註解被覆寫。例如：

```
helm upgrade trident-protect -n trident-protect netapp-trident-  
protect/trident-protect \  
  --set-string  
  restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k  
  ey_to_skip_2>}" \  
  --reuse-values
```



執行還原或容錯移轉作業時，restoreSkipNamespaceAnnotations 和 restoreSkipNamespaceLabels 中指定的任何命名空間註釋和標籤都會從還原或容錯移轉作業中排除。請確保在初始 Helm 安裝期間配置這些設定。若要深入瞭解，請參閱 ["設定其他 Trident Protect Helm Chart 設定"](#)。

如果您使用 Helm 並帶有 --create-namespace 標誌安裝了來源應用程式，則會對 name 標籤鍵進行特殊處理。在還原或容錯移轉過程中，Trident Protect 會將此標籤複製到目的地命名空間，但如果來源的值與來源命名空間相符，則會將值更新為目的地命名空間值。如果此值與來源命名空間不相符，則會將其複製到目的地命名空間而不做任何變更。

範例

以下範例展示了來源命名空間和目標命名空間，它們各自具有不同的註解和標籤。您可以查看操作前後目標命名空間的狀態，以及註解和標籤在目標命名空間中是如何組合或覆蓋的。

在還原或容錯移轉作業之前

下表說明了復原或容錯移轉作業之前範例來源命名空間和目標命名空間的狀態：

命名空間	註解	標籤
命名空間 ns-1 （來源）	<ul style="list-style-type: none">• annotation.one/key: 「updatedvalue」• annotation.two/key: 「true」	<ul style="list-style-type: none">• environment=production• 合規性=hipaa• 名稱=ns-1
命名空間 ns-2 （目標）	<ul style="list-style-type: none">• annotation.one/key: 「true」• annotation.three/key: 「false」	<ul style="list-style-type: none">• 角色=資料庫

還原作業後

下表展示了復原或故障轉移作業後範例目標命名空間的狀態。一些鍵已被添加，一些鍵已被覆蓋，並且 name 標籤已更新以匹配目標命名空間：

命名空間	註解	標籤
命名空間 ns-2 （目標）	<ul style="list-style-type: none">• annotation.one/key: 「updatedvalue」• annotation.two/key: 「true」• annotation.three/key: 「false」	<ul style="list-style-type: none">• 名稱=ns-2• 合規性=hipaa• environment=production• 角色=資料庫

支援的欄位

本節說明可用於還原作業的其他欄位。

儲存類別對應

此 `spec.storageClassMapping` 屬性定義了從來源應用程式中的儲存類別到目標叢集上新儲存類別的對應。在將應用程式遷移到具有不同儲存類別的叢集之間，或變更 BackupRestore 操作的儲存後端時，可以使用此屬性。

- 範例：*

```
storageClassMapping:  
- destination: "destinationStorageClass1"  
  source: "sourceStorageClass1"  
- destination: "destinationStorageClass2"  
  source: "sourceStorageClass2"
```

支援的註釋

本節列出了系統中用於設定各種行為的支援註解。如果使用者未明確設定註解，系統將使用預設值。

註解	類型	說明	預設值
protect.trident.netapp.io/data-mover-timeout-sec	字串	資料移動器操作允許停止的最長時間（以秒為單位）。	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	字串	Kopia 內容快取的大小上限（以 MB 為單位）。	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	字串	等待所有新建立的 PersistentVolumeClaims (PVC) 達到 `Bound` 階段的最長時間（以秒為單位），超過此時間操作將會失敗。適用於所有還原 CR 類型（BackupRestore、BackupInplaceRestore、SnapshotRestore、SnapshotInplaceRestore）。如果您的儲存設備後端或叢集通常需要更多時間，請使用更高的值。	"1200"（20 分鐘）

使用自訂資源還原資源時修改資源

資源轉換功能可讓您在復原資源的過程中進行修改。當復原後的版本需要與原始版本有所不同時，此功能非常有用，例如，在將應用程式還原到不同的叢集時，更新 ConfigMap 中的主機名稱。

資源修改的運作方式

The transformations 欄位位於 SnapshotRestore、BackupRestore、AppMirrorRelationship 及其他復原資源中，可讓您在復原過程中修改 Kubernetes 資源。當復原後的應用程式需要與原始應用程式採用不同的組態時，例如變更主機名稱、登錄 URL、資源限制或環境變數，此功能非常實用。

資源轉換使用 "RFC 6902 JSON Patch" 操作和 "RFC 6901 JSON Pointer" 路徑來定位和修改 Kubernetes 資源中的特定欄位。

下面展示了包含資源轉換的還原物件的基本結構：

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-restore
  namespace: target-namespace
spec:
  appVaultRef: my-vault
  appArchivePath: /path/to/snapshot
  namespaceMapping:
    - source: source-ns
      destination: target-ns
  transformations:
    - resource:
        kind: ConfigMap          # Required: resource kind
```

```

    group: ""                # Optional: API group (empty for core
resources)
    version: ""              # Optional: API version
    name: ""                 # Optional: specific resource name
    operations:
      - op: replace           # Operation type
        path: "/data/key"    # JSON Pointer path
        value: "new-value"   # New value (for add/replace/test)

```

支援的資源

您可以將資源轉換套用至符合下列條件的資源：

- **kind** (必填)：Kubernetes 資源類型 (例如，ConfigMap，Deployment，Pod)
- **group** (可選)：API 群組 (例如，apps，route.openshift.io) — 對於核心資源，請省略
- 版本 (可選)：API 版本 (例如，v1，v1beta1)
- 名稱 (可選)：僅套用於指定名稱的資源



目前不支援修改 PersistentVolumeClaims 和命名空間。

支援的作業

您可以使用以下操作來修改資源：add，copy，move，remove，replace，以及 test。

為資源新增值

使用 add 操作可在指定路徑新增欄位或值。您可以為物件或陣列新增資料。

使用 CR

以下範例向 Deployment 資源新增節點選擇器：

```

transformations:
  - resource:
      kind: Deployment
    operations:
      - op: add
        path: "/spec/template/spec/nodeSelector"
        value:
          "topology.kubernetes.io/zone": "us-east-1a"
          disktype: "ssd"

```

使用 CLI

使用以下命令透過命令列執行此轉換：

```
tridentctl-protect create snapshotrestore <restore_name> \
  --snapshot <namespace/snapshot-name> \
  --namespace-mapping <source-ns>:<dest-ns> \
  --transformation
'apps,v1,Deployment:add{"path":"/spec/template/spec/nodeSelector","value":{"topology.kubernetes.io/zone":"us-east-1a","disktype":"ssd"}}'
```

複製資源中的值

使用 `copy` 操作可將相同資源內的值從一個路徑複製到另一個路徑。來源值不會改變。

使用 CR

以下範例複製 ConfigMap 物件的資料鍵：

```
transformations:
- resource:
  kind: ConfigMap
  operations:
  - op: copy
    from: "/data/source-key"
    path: "/data/backup-key"
```

使用 CLI

使用以下命令透過命令列執行此轉換：

```
tridentctl-protect create snapshotrestore <restore_name> \
  --snapshot <namespace/snapshot-name> \
  --namespace-mapping <source-ns>:<dest-ns> \
  --transformation ',v1,ConfigMap:copy{"from":"/data/source-key","path":"/data/backup-key"}'
```

在資源內移動值

使用 `move` 操作可將相同資源中的值從一個路徑移至另一個路徑。來源路徑將被移除，值將被放置在目標路徑中。

使用 CR

以下範例重新命名 ConfigMap 物件的資料鍵：

```
transformations:
```

```
- resource:
  kind: ConfigMap
  operations:
    - op: move
      from: "/data/OLD_KEY"
      path: "/data/NEW_KEY"
```

使用 CLI

使用以下命令透過命令列執行此轉換：

```
tridentctl-protect create snapshotrestore <restore_name> \
--snapshot <namespace/snapshot-name> \
--namespace-mapping <source-ns>:<dest-ns> \
--transformation
',v1,ConfigMap:move{"from":"/data/OLD_KEY","path":"/data/NEW_KEY"}'
```

從資源中移除值

使用 `remove` 操作可刪除指定路徑中的欄位或值。

使用 CR

以下範例從 `ConfigMap` 資源中刪除註解：

```
transformations:
- resource:
  kind: ConfigMap
  operations:
    - op: remove
      path: "/metadata/annotations/kubectl.kubernetes.io~1last-
applied-configuration"
```



在上述範例的路徑中、~1 是 / 的 JSON Pointer 轉義序列。

使用 CLI

使用以下命令透過命令列執行此轉換：

```
tridentctl-protect create snapshotrestore <restore_name> \
--snapshot <namespace/snapshot-name> \
--namespace-mapping <source-ns>:<dest-ns> \
--transformation
',v1,ConfigMap:remove{"path":"/metadata/annotations/kubectl.kubernetes.
```

```
io~1last-applied-configuration"}'
```

取代資源中的值

使用此 `replace` 操作可取代指定路徑下資源中的現有值。JSON 路徑必須已存在。

使用 CR

以下範例變更 Route 物件的主機名稱：

```
transformations:
- resource:
  kind: Route
  group: route.openshift.io
  operations:
  - op: replace
    path: "/spec/host"
    value: "prod.example.com"
```

使用 CLI

使用以下命令透過命令列執行此轉換：

```
tridentctl-protect create snapshotrestore <restore_name> \
--snapshot <namespace/snapshot-name> \
--namespace-mapping <source-ns>:<dest-ns> \
--transformation
'route.openshift.io,v1,Route:replace{"path":"/spec/host","value":"prod.
example.com"}'
```

測試資源修改

使用 test 操作，在執行其他操作之前驗證路徑處的值是否與預期值相符。如果測試失敗，整個修改將會回滾。

使用 CR

以下範例僅在 environment 設定為 staging 時，才會更新 database-host：

```
transformations:
- resource:
  kind: ConfigMap
  operations:
  - op: test
```

```

    path: "/data/environment"
    value: "staging"
- op: replace
  path: "/data/database-host"
  value: "prod-db.example.com"

```

使用 CLI

使用以下命令透過命令列執行此轉換：

```

tridentctl-protect create snapshotrestore <restore_name> \
  --snapshot <namespace/snapshot-name> \
  --namespace-mapping <source-ns>:<dest-ns> \
  --transformation
',v1,ConfigMap:test{"path":"/data/environment","value":"staging"},repla
ce{"path":"/data/database-host","value":"prod-db.example.com"}'

```

使用 NetApp SnapMirror 和 Trident Protect 複製應用程式

使用 Trident Protect，您可以利用 NetApp SnapMirror 技術的非同步複製功能，將資料和應用程式變更從一個儲存後端複製到另一個儲存後端，無論是在同一叢集內還是在不同叢集之間。

還原和容錯移轉作業期間的命名空間註釋和標籤

在還原和容錯移轉作業期間，目的地命名空間中的標籤和註釋會與來源命名空間中的標籤和註釋相符。來源命名空間中存在但目的地命名空間中不存在的標籤或註釋會被新增，而任何已存在的標籤或註釋則會被覆寫以符合來源命名空間中的值。僅存在於目的地命名空間中的標籤或註釋則保持不變。



如果您使用 Red Hat OpenShift，請務必注意命名空間註解在 OpenShift 環境中的關鍵作用。命名空間註解可確保復原的 Pod 遵循 OpenShift 安全上下文約束（SCC）定義的相應權限和安全性配置，並能無權限問題地存取磁碟區。如需詳細資訊，請參閱 ["OpenShift 安全上下文約束文檔"](#)。

您可以透過在執行復原或故障轉移操作之前設定 Kubernetes 環境變數

RESTORE_SKIP_NAMESPACE_ANNOTATIONS，來防止目標命名空間中的特定註解被覆寫。例如：

```

helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values

```



執行還原或容錯移轉作業時，`restoreSkipNamespaceAnnotations` 和 `restoreSkipNamespaceLabels` 中指定的任何命名空間註釋和標籤都會從還原或容錯移轉作業中排除。請確保在初始 Helm 安裝期間配置這些設定。若要深入瞭解，請參閱 ["設定其他 Trident Protect Helm Chart 設定"](#)。

如果您使用 Helm 並帶有 `--create-namespace` 標誌安裝了來源應用程式，則會對 `name` 標籤鍵進行特殊處理。在還原或容錯移轉過程中，Trident Protect 會將此標籤複製到目的地命名空間，但如果來源的值與來源命名空間相符，則會將值更新為目的地命名空間值。如果此值與來源命名空間不相符，則會將其複製到目的地命名空間而不做任何變更。

範例

以下範例展示了來源命名空間和目標命名空間，它們各自具有不同的註解和標籤。您可以查看操作前後目標命名空間的狀態，以及註解和標籤在目標命名空間中是如何組合或覆蓋的。

在還原或容錯移轉作業之前

下表說明了復原或容錯移轉作業之前範例來源命名空間和目標命名空間的狀態：

命名空間	註解	標籤
命名空間 ns-1 (來源)	<ul style="list-style-type: none"> • <code>annotation.one/key</code>: 「updatedvalue」 • <code>annotation.two/key</code>: 「true」 	<ul style="list-style-type: none"> • <code>environment=production</code> • <code>合規性=hipaa</code> • <code>名稱=ns-1</code>
命名空間 ns-2 (目標)	<ul style="list-style-type: none"> • <code>annotation.one/key</code>: 「true」 • <code>annotation.three/key</code>: 「false」 	<ul style="list-style-type: none"> • <code>角色=資料庫</code>

還原作業後

下表展示了復原或故障轉移作業後範例目標命名空間的狀態。一些鍵已被添加，一些鍵已被覆蓋，並且 `name` 標籤已更新以匹配目標命名空間：

命名空間	註解	標籤
命名空間 ns-2 (目標)	<ul style="list-style-type: none"> • <code>annotation.one/key</code>: 「updatedvalue」 • <code>annotation.two/key</code>: 「true」 • <code>annotation.three/key</code>: 「false」 	<ul style="list-style-type: none"> • <code>名稱=ns-2</code> • <code>合規性=hipaa</code> • <code>environment=production</code> • <code>角色=資料庫</code>



您可以設定 Trident Protect 在資料保護作業期間凍結及解除凍結檔案系統。["深入瞭解如何使用 Trident Protect 設定檔案系統凍結"](#)。

故障轉移和反向操作期間的執行掛鉤

使用 AppMirror 關係保護應用程式時，在故障轉移和反向操作期間，您應該注意與執行鉤子相關的特定行為。

- 故障轉移期間，執行鉤子會自動從來源叢集複製到目標叢集。您無需手動重新建立。故障轉移後，執行鉤子將存在於應用程式中，並在執行任何相關操作時運行。

- 在反向同步或反向重同步過程中，應用程式上所有現有的執行鉤子都會被移除。當來源應用程式變為目標應用程式時，這些執行鉤子將失效並被刪除以防止其執行。

若要深入瞭解執行掛鉤，請參閱 ["管理 Trident Protect 執行掛鉤"](#)。

建立複寫關係

建立複寫關係涉及下列項目：

- 選擇 Trident Protect 拍攝應用程式快照的頻率（包括應用程式的 Kubernetes 資源以及應用程式每個磁碟區的磁碟區快照）
- 選擇複寫排程（包括 Kubernetes 資源以及持續性磁碟區資料）
- 設定拍攝 Snapshot 的時間

步驟

1. 在來源叢集上，為來源應用程式建立一個 AppVault。根據您的儲存供應商，修改 ["AppVault 自訂資源"](#) 中的範例以適應您的環境：

使用 CR 建立 AppVault

- a. 建立自訂資源（CR）檔案並將其命名為（例如、trident-protect-appvault-primary-source.yaml）。
- b. 設定下列屬性：
 - **metadata.name**：（必填）AppVault 自訂資源的名稱。請記下您選擇的名稱，因為複寫關係所需的其他 CR 檔案會引用此值。
 - **spec.providerConfig**：（必要）儲存使用指定提供者存取 AppVault 所需的組態。選擇 bucketName 以及提供者所需的任何其他詳細資料。請記下您選擇的值，因為複寫關係所需的其他 CR 檔案會參照這些值。請參閱["AppVault 自訂資源"](#)以取得其他提供者的 AppVault CR 範例。
 - **spec.providerCredentials**：（Required）儲存使用指定提供者存取 AppVault 所需的任何憑證參考。
 - **spec.providerCredentials.valueFromSecret**：（Required）表示憑證值應來自金鑰。
 - **key**: (必填) 要從中選取的有效金鑰。
 - **name**：（必填）包含此欄位值的 secret 名稱。必須位於同一個 namespace 中。
 - **spec.providerCredentials.secretAccessKey**：（必要）用於存取提供者的存取金鑰。name 應與 spec.providerCredentials.valueFromSecret.name 相符。
 - **spec.providerType**：（必填）確定備份服務商；例如，NetApp ONTAP S3、通用 S3、Google Cloud 或 Microsoft Azure。可選值：
 - aws
 - azure
 - gcp
 - generic-s3
 - ontap-s3

- storagegrid-s3

- c. 在 `trident-protect-appvault-primary-source.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-appvault-primary-source.yaml -n
trident-protect
```

使用 CLI 建立 AppVault

- a. 建立 AppVault，並將括號中的值替換為您環境中的資訊：

```
tridentctl-protect create vault Azure <vault-name> --account
<account-name> --bucket <bucket-name> --secret <secret-name> -n
trident-protect
```

2. 在來源叢集上、建立來源應用程式 CR：

使用 CR 建立來源應用程式

- a. 建立自訂資源（CR）檔案並將其命名為（例如、`trident-protect-app-source.yaml`）。
- b. 設定下列屬性：

- **metadata.name**：（必填）應用程式自訂資源的名稱。請記下您選擇的名稱，因為複寫關係所需的其他 CR 檔案會引用此值。
- **spec.includedNamespaces**：（必要）命名空間及其關聯標籤的陣列。使用命名空間名稱，並可選擇性地使用標籤來縮小命名空間的範圍，以指定此處列出的命名空間中存在的資源。應用程式命名空間必須包含在此陣列中。

YAML 範例：

```
---
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: my-app-namespace
      labelSelector: {}
```

- c. 在 `trident-protect-app-source.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-app-source.yaml -n my-app-namespace
```

使用 **CLI** 建立來源應用程式

a. 建立來源應用程式。例如：

```
tridentctl-protect create app <my-app-name> --namespaces  
<namespaces-to-be-included> -n <my-app-namespace>
```

3. (可選) 在來源叢集上，對來源應用程式進行快照。此快照將用作目標叢集上應用程式的基礎。如果跳過此步驟，則需要等待下一次排程快照運行，以便取得最新的快照。若要建立按需快照，請參閱 ["建立隨需快照"](#)。
4. 在來源叢集上、建立複寫排程 CR：

除了下方提供的排程之外，建議建立一個單獨的每日快照排程，並將保留期設定為 7 天，以便在對等 ONTAP 叢集之間維護一個通用的快照。這樣可以確保快照最多可用 7 天，但保留期可以根據使用者需求進行自訂。



如果發生故障轉移，系統可以使用這些快照進行最多 7 天的逆向操作。這種方法可以加快逆向過程並提高效率，因為只會傳輸自上次快照以來所做的變更，而不是所有資料。

如果應用程式的現有排程已符合所需的保留要求，則不需要其他排程。

使用 **CR** 建立複寫排程

a. 為來源應用程式建立複寫排程：

- i. 建立自訂資源 (CR) 檔案並將其命名為 (例如、trident-protect-schedule.yaml)。
- ii. 設定下列屬性：
 - **metadata.name**：(必填) 排程自訂資源的名稱。
 - **spec.appVaultRef**：(必填) 此值必須與來源應用程式的 AppVault metadata.name 欄位相符。
 - **spec.applicationRef**：(必填) 此值必須與來源應用程式 CR 的 metadata.name 欄位相符。
 - **spec.backupRetention**：(必填) 此欄位為必填項，其值必須設為 0。
 - **spec.enabled**：必須設定為 true。
 - **spec.granularity**：必須設定為 Custom。
 - **spec.recurrenceRule**：定義 UTC 時間的開始日期和重複間隔。
 - **spec.snapshotRetention**：必須設定為 2。

YAML 範例：

```

---
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  name: appmirror-schedule
  namespace: my-app-namespace
spec:
  appVaultRef: my-appvault-name
  applicationRef: my-app-name
  backupRetention: "0"
  enabled: true
  granularity: Custom
  recurrenceRule: |-
    DTSTART:20220101T000200Z
    RRULE:FREQ=MINUTELY;INTERVAL=5
  snapshotRetention: "2"

```

- i. 在 trident-protect-schedule.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-schedule.yaml -n my-app-namespace
```

使用 CLI 建立複寫排程

- a. 建立複寫排程，並將括號中的值替換為您環境中的資訊：

```
tridentctl-protect create schedule --name appmirror-schedule
--app <my_app_name> --appvault <my_app_vault> --granularity
Custom --recurrence-rule <rule> --snapshot-retention
<snapshot_retention_count> -n <my_app_namespace>
```

▪ 範例：*

```
tridentctl-protect create schedule --name appmirror-schedule
--app <my_app_name> --appvault <my_app_vault> --granularity
Custom --recurrence-rule "DTSTART:20220101T000200Z
\nRRULE:FREQ=MINUTELY;INTERVAL=5" --snapshot-retention 2 -n
<my_app_namespace>
```

5. 在目標叢集上，建立一個與在來源叢集上應用的 AppVault CR 相同的來源應用程式 AppVault CR，並將其命名為（例如，trident-protect-appvault-primary-destination.yaml）。
6. 套用 CR：

```
kubectl apply -f trident-protect-appvault-primary-destination.yaml -n
trident-protect
```

7. 在目標叢集上為目標應用程式建立目標 AppVault CR。根據您的儲存供應商，修改 ["AppVault 自訂資源"](#) 中的範例以適應您的環境：
 - a. 建立自訂資源 (CR) 檔案並將其命名為 (例如、trident-protect-appvault-secondary-destination.yaml)。
 - b. 設定下列屬性：
 - **metadata.name**：(必填) AppVault 自訂資源的名稱。請記下您選擇的名稱，因為複寫關係所需的其他 CR 檔案會引用此值。
 - **spec.providerConfig**：(必要) 儲存使用指定提供者存取 AppVault 所需的組態。選擇一個 `bucketName` 以及提供者所需的任何其他詳細資訊。請記下您選擇的值，因為複寫關係所需的其他 CR 檔案會參照這些值。請參閱["AppVault 自訂資源"](#)以取得其他提供者的 AppVault CR 範例。
 - **spec.providerCredentials**：(*Required*) 儲存使用指定提供者存取 AppVault 所需的任何憑證參考。
 - **spec.providerCredentials.valueFromSecret**：(*Required*) 表示憑證值應來自金鑰。
 - **key**: (必填) 要從中選取的有效金鑰。
 - **name**：(必填) 包含此欄位值的 secret 名稱。必須位於同一個 namespace 中。
 - **spec.providerCredentials.secretAccessKey**：(必要) 用於存取提供者的存取金鑰。**name** 應與 **spec.providerCredentials.valueFromSecret.name** 相符。
 - **spec.providerType**：(必填) 確定備份服務商；例如，NetApp ONTAP S3、通用 S3、Google Cloud 或 Microsoft Azure。可選值：
 - aws
 - azure
 - gcp
 - generic-s3
 - ontap-s3
 - storagegrid-s3
 - c. 在 trident-protect-appvault-secondary-destination.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-appvault-secondary-destination.yaml
-n trident-protect
```

8. 在目標叢集上、建立 AppMirrorRelationship CR 檔案。



使用 CR 時，請在套用 CR 之前手動建立目的地命名空間。Trident Protect 僅在使用 CLI 時才會自動建立命名空間。

使用 CR 建立 AppMirrorRelationship

- a. 建立自訂資源 (CR) 檔案並將其命名為 (例如、trident-protect-relationship.yaml)。
- b. 設定下列屬性：

- **metadata.name:** (必填) AppMirrorRelationship 自訂資源的名稱。
- **spec.destinationAppVaultRef:** (必填) 此值必須與目標叢集上目標應用程式的 AppVault 名稱相符。
- **spec.namespaceMapping:** (必需) 目標命名空間和來源命名空間必須與對應應用程式 CR 中定義的應用程式命名空間相符。
- **spec.sourceAppVaultRef:** (Required) 此值必須與來源應用程式的 AppVault 名稱相符。
- **spec.sourceApplicationName:** (必需) 此值必須與您在來源應用程式 CR 中定義的來源應用程式名稱相符。
- **spec.sourceApplicationUID:** (必要) 此值必須與您在來源應用程式 CR 中定義的來源應用程式的 UID 相符。
- **spec.storageClassName:** (選用) 選擇叢集上有效儲存類別的名稱。儲存類別必須連結至與來源環境對等的 ONTAP 儲存 VM。如果未提供儲存類別，則預設會使用叢集上的預設儲存類別。
- **spec.storageClassMapping:** (可選) 將同一 AMR 內各個 PVC 的來源儲存類別對應到目標儲存類別。每個條目都需要一個 `source`` 和 ``destination`` 儲存類別名稱。設定後，``storageClassMapping`` 將完全覆蓋 ``storageClassName``；沒有符合來源條目的 PVC 將使用叢集預設儲存類別，而非 `storageClassName`。

在 AppMirrorRelationship CR 中使用 ``storageClassMapping`` 時，請注意以下限制：

- `storageClassMapping` 覆蓋 `storageClassName` 的全部內容。當兩個欄位都設定時，`storageClassName` 將被忽略。
- 來源儲存類別在 `storageClassMapping`` 中沒有相符條目的 PVC 將使用叢集預設儲存類別，而非 ``storageClassName``。
- 每個條目都需要一個 ``source`` 和 ``destination`` 值。
- 更改目標儲存類別可能會強制刪除並重新建立現有的目標 PVC。
- **spec.recurrenceRule:** 定義 UTC 時間的開始日期和重複間隔。

YAML 範例：

```
---
apiVersion: protect.trident.netapp.io/v1
kind: AppMirrorRelationship
metadata:
  name: amr-16061e80-1b05-4e80-9d26-d326dc1953d8
  namespace: my-app-namespace
spec:
  desiredState: Established
```

```

destinationAppVaultRef: generic-s3-trident-protect-dst-bucket-
8fe0b902-f369-4317-93d1-ad7f2edc02b5
namespaceMapping:
  - destination: my-app-namespace
    source: my-app-namespace
recurrenceRule: |-
  DTSTART:20220101T000200Z
  RRULE:FREQ=MINUTELY;INTERVAL=5
sourceAppVaultRef: generic-s3-trident-protect-src-bucket-
b643cc50-0429-4ad5-971f-ac4a83621922
sourceApplicationName: my-app-name
sourceApplicationUID: 7498d32c-328e-4ddd-9029-122540866aeb
storageClassName: sc-vsrm-2

```

- c. 在 trident-protect-relationship.yaml 檔案中填入正確的值後，套用 CR：

```

kubectl apply -f trident-protect-relationship.yaml -n my-app-
namespace

```

使用 CLI 建立 AppMirrorRelationship

- a. 建立並套用 AppMirrorRelationship 物件，將括號中的值替換為您環境中的資訊：

```

tridentctl-protect create appmirrorrelationship
<name_of_appmirrorrelationship> --destination-app-vault
<my_vault_name> --source-app-vault <my_vault_name> --recurrence
-rule <rule> --namespace-mapping <ns_mapping> --source-app-id
<source_app_UID> --source-app <my_source_app_name> --storage
-class <storage_class_name> --storageclass-mapping
<src_class:dst_class> -n <application_namespace>

```



使用 `--storageclass-mapping` 將各個來源儲存類別對應到目標儲存類別。指定一個或多個 ``source:destination`` 以逗號分隔的鍵值對（例如，``"class-a:class-b,class-c:class-d"``）。使用 ``*:destination-class`` 作為萬用字元，可將所有未對應的 PVC 對應到單一目標儲存類別。當 `--storageclass-mapping` 設定後，`--storage-class` 將被忽略。

使用單一目標儲存類別的範例 (`--storage-class`)：

```

tridentctl-protect create appmirrorrelationship my-amr
--destination-app-vault appvault2 --source-app-vault appvault1
--recurrence-rule
"DTSTART:20220101T000200Z\nRRULE:FREQ=MINUTELY;INTERVAL=5"
--source-app my-app --namespace-mapping "my-source-ns1:my-dest-

```

```
ns1,my-source-ns2:my-dest-ns2" --source-app-id 373f24c1-5769-404c-93c3-5538af6ccc36 --storage-class my-storage-class -n my-dest-ns1
```

9. (可選) 在目標叢集上、檢查複寫關係的狀態和狀態：

```
kubectl get amr -n my-app-namespace <relationship name> -o=jsonpath='{.status}' | jq
```

故障轉移至目的地叢集

使用 Trident Protect，您可以將複製的應用程式容錯移轉至目的地叢集。此程序會停止複寫關係，並使應用程式在目的地叢集上線上。如果來源叢集上的應用程式正在運作，Trident Protect 不會停止該應用程式。

步驟

1. 在目標叢集上，編輯 AppMirrorRelationship CR 檔案（例如，trident-protect-relationship.yaml），並將 **spec.desiredState** 的值變更為 Promoted。
2. 儲存 CR 檔案。
3. 套用 CR：

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-namespace
```

4. (可選) 在故障轉移應用程式上建立所需的任何保護排程。
5. (可選) 檢查複寫關係的狀態和狀態：

```
kubectl get amr -n my-app-namespace <relationship name> -o=jsonpath='{.status}' | jq
```

重新同步故障轉移的複寫關係

重新同步作業會重新建立複寫關係。執行重新同步作業後、原始來源應用程式會成為執行中的應用程式、而目的地叢集上執行中應用程式所做的任何變更都會被捨棄。

該過程會在重新建立複寫之前停止目的地叢集上的應用程式。



故障轉移期間寫入目標應用程式的任何資料都會遺失。

步驟

1. 選用：在來源叢集上，建立來源應用程式的快照。這可確保擷取來源叢集的最新變更。
2. 在目標叢集上，編輯 AppMirrorRelationship CR 檔案（例如，trident-protect-relationship.yaml），並將 **spec.desiredState** 的值變更為 Established。

3. 儲存 CR 檔案。

4. 套用 CR：

```
kubectl apply -f trident-protect-relationship.yaml -n my-app-namespace
```

5. 如果您在目的地叢集上建立了任何保護排程來保護故障轉移的應用程式，請將其移除。任何保留的排程都會導致磁碟區快照失敗。

反向重新同步已容錯移轉的複寫關係

當您對故障轉移的複製關係進行反向同步時，目標應用程式將變為來源應用程式，而來源應用程式將變為目標應用程式。故障轉移期間對目標應用程式所做的變更將被保留。

步驟

1. 在原始目標叢集上，刪除 AppMirrorRelationship CR。這將使目標叢集變為來源叢集。如果新目標叢集上仍有任何保護排程，請將其刪除。
2. 透過將最初用於建立關係的 CR 檔案套用到相反的叢集，以建立複寫關係。
3. 確保新目標（原始來源叢集）配置了兩個 AppVault CR。
4. 在相反的叢集上建立複寫關係，並設定反向的值。

反向應用程式複寫方向

當您反轉複製方向時、Trident Protect 會將應用程式移至目的地儲存後端、同時繼續複寫回原始來源儲存後端。Trident Protect 會停止來源應用程式、並在容錯移轉至目的地應用程式之前、將資料複寫至目的地。

在這種情況下，您正在交換來源和目的地。

步驟

1. 在來源叢集上，建立關機快照：

使用 CR 建立關機快照

- a. 停用來源應用程式的保護原則排程。
- b. 建立 ShutdownSnapshot CR 檔案：
 - i. 建立自訂資源（CR）檔案並將其命名為（例如、trident-protect-shutdownsnapshot.yaml）。
 - ii. 設定下列屬性：
 - **metadata.name**：（必填）自訂資源的名稱。
 - **spec.AppVaultRef**：（*Required*）此值必須與來源應用程式的 AppVault metadata.name 欄位相符。
 - **spec.ApplicationRef**：（必填）此值必須與來源應用程式 CR 檔案的 metadata.name 欄位相符。

YAML 範例：

```

---
apiVersion: protect.trident.netapp.io/v1
kind: ShutdownSnapshot
metadata:
  name: replication-shutdown-snapshot-afc4c564-e700-4b72-86c3-
c08a5dbe844e
  namespace: my-app-namespace
spec:
  appVaultRef: generic-s3-trident-protect-src-bucket-04b6b4ec-
46a3-420a-b351-45795e1b5e34
  applicationRef: my-app-name

```

- c. 在 `trident-protect-shutdownsnapshot.yaml` 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-shutdownsnapshot.yaml -n my-app-namespace
```

使用 CLI 建立關機快照

- a. 建立關機快照，並將括號中的值替換為您環境中的資訊。例如：

```
tridentctl-protect create shutdownsnapshot <my_shutdown_snapshot>
--appvault <my_vault> --app <app_to_snapshot> -n
<application_namespace>
```

2. 在來源叢集上，關機 Snapshot 完成後，取得關機 Snapshot 的狀態：

```
kubectl get shutdownsnapshot -n my-app-namespace
<shutdown_snapshot_name> -o yaml
```

3. 在來源叢集上，使用以下命令尋找 `shutdownsnapshot.status.appArchivePath` 的值，並記錄檔案路徑的最後一部分（也稱為基本名稱；這是最後一個斜槓之後的所有內容）：

```
k get shutdownsnapshot -n my-app-namespace <shutdown_snapshot_name> -o
jsonpath='{.status.appArchivePath}'
```

4. 從新的目標叢集到新的來源叢集執行容錯移轉，並進行以下變更：



在故障轉移過程的步驟 2 中，將 `spec.promotedSnapshot` 欄位包含在 `AppMirrorRelationship` CR 檔案中，並將其值設定為您上面的步驟 3 中記錄的基本名稱。

5. 在 [\[反向重新同步已容錯移轉的複寫關係\]](#) 中執行反向重新同步步驟。

6. 在新來源叢集上啟用保護排程。

結果

由於反向複寫，會發生以下動作：

- 對原始來源應用程式的 Kubernetes 資源進行快照。
- 透過刪除應用程式的 Kubernetes 資源（保留 PVC 和 PV），優雅地停止原始來源應用程式的 Pod。
- 在 pod 關閉後，會對應用程式的 Volume 進行快照並進行複寫。
- SnapMirror 關係已中斷，使目的地磁碟區準備好進行讀取 / 寫入。
- 該應用程式的 Kubernetes 資源是從關閉前的快照中還原，使用的是在原始來源應用程式關閉後複寫的磁碟區資料。
- 複寫會以相反的方向重新建立。

將應用程式容錯回復至原始來源叢集

使用 Trident Protect，您可以透過以下步驟在故障轉移作業後實現「故障復原」。在此工作流程中，為了恢復原始複寫方向，Trident Protect 會在反轉複寫方向之前，將所有應用程式變更複寫（重新同步）回原始來源應用程式。

此程序從已完成容錯移轉至目的地的關係開始，並涉及下列步驟：

- 從故障轉移狀態開始。
- 反向重新同步複寫關係。



不要執行正常的重新同步作業，因為這會捨棄在容錯移轉程序期間寫入目的地叢集的資料。

- 反轉複寫方向。

步驟

1. 執行[\[反向重新同步已容錯移轉的複寫關係\]](#)步驟。
2. 執行[\[反向應用程式複寫方向\]](#)步驟。

刪除複寫關係

您可以隨時刪除複寫關係。刪除應用程式複寫關係後，將產生兩個彼此獨立的應用程式，它們之間沒有任何關聯。

步驟

1. 在目前目標叢集上、刪除 AppMirrorRelationship CR：

```
kubectl delete -f trident-protect-relationship.yaml -n my-app-namespace
```

使用 Trident Protect 遷移應用程式

您可以透過還原備份資料，在叢集之間遷移應用程式或將應用程式遷移到不同的儲存類別。



遷移應用程式時，所有為該應用程式配置的執行鉤子都會隨應用程式一起遷移。如果存在復原後執行鉤子，它會在復原操作過程中自動執行。

備份與還原作業

若要針對下列案例執行備份與還原作業，您可以自動執行特定的備份與還原工作。

複製到同一叢集

若要將應用程式複製到同一個叢集、請建立快照或備份、然後將資料還原到同一個叢集。

步驟

1. 執行下列其中一項作業：
 - a. "建立快照"。
 - b. "建立備份"。
2. 在同一叢集上，根據您建立的是快照還是備份，執行下列其中一項：
 - a. "從快照還原資料"。
 - b. "從備份中恢復資料"。

複製到不同的叢集

若要將應用程式複製到另一個叢集（執行跨叢集複製），請在來源叢集上建立備份，然後將備份還原到另一個叢集。請確保目標叢集上已安裝 Trident Protect。



您可以使用 "SnapMirror 複製" 在不同的叢集之間複製應用程式。

步驟

1. "建立備份"。
2. 確保目標叢集上已配置包含備份的物件儲存桶的 AppVault CR。
3. 在目標叢集上，"從備份中恢復資料"。

將應用程式從一個儲存類別遷移到另一個儲存類別

您可以透過將備份還原到目標儲存類別，將應用程式從一個儲存類別遷移到另一個儲存類別。

例如（不包括還原 CR 中的機密）：

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
```

```

name: "${snapshotRestoreCRName}"
spec:
  appArchivePath: "${snapshotArchivePath}"
  appVaultRef: "${appVaultCRName}"
  namespaceMapping:
    - destination: "${destinationNamespace}"
      source: "${sourceNamespace}"
  storageClassMapping:
    - destination: "${destinationStorageClass}"
      source: "${sourceStorageClass}"
  resourceFilter:
    resourceMatchers:
      kind: Secret
      version: v1
    resourceSelectionCriteria: exclude

```

使用 CR 還原快照

步驟

1. 建立自訂資源 (CR) 檔案並將其命名為 `trident-protect-snapshot-restore-cr.yaml`。
2. 在您建立的檔案中、設定以下屬性：
 - **metadata.name**：(必填) 此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.appArchivePath**：AppVault 內儲存快照內容的路徑。您可以使用以下命令來尋找此路徑：

```

kubectl get snapshots <my-snapshot-name> -n trident-protect -o
jsonpath='{.status.appArchivePath}'

```

- **spec.appVaultRef**：(必填) 儲存快照內容的 AppVault 名稱。
- **spec.namespaceMapping**：復原作業的來源命名空間到目標命名空間的對應。請將 ``my-source-namespace`` 和 ``my-destination-namespace`` 替換為您環境中的資訊。

```

---
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: trident-protect
spec:
  appArchivePath: my-snapshot-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace",
"destination": "my-destination-namespace"}]

```

3. (選用) 如果您需要僅選擇要還原的應用程式的某些資源，請新增篩選條件，以包含或排除標記有特定標籤的資源：

- **resourceFilter.resourceSelectionCriteria**：(篩選必需) 使用 `include or exclude` 包含或排除在 resourceMatchers 中定義的資源。新增以下 resourceMatchers 參數以定義要包含或排除的資源：

- **resourceFilter.resourceMatchers**：resourceMatcher 物件的陣列。如果在此陣列中定義多個元素，它們之間將按 OR 運算匹配，每個元素內的欄位 (group、kind、version) 之間將按 AND 運算匹配。

- **resourceMatchers[].group**：(可選) 要篩選的資源群組。

- **resourceMatchers[].kind**：(可選) 要篩選的資源類型。

- **resourceMatchers[].version**：(可選) 要篩選的資源版本。

- **resourceMatchers[].names**：(可選) 要過濾的資源的 Kubernetes metadata.name 欄位中的名稱。

- **resourceMatchers[].namespaces**：(可選) 要篩選的資源的 Kubernetes metadata.name 欄位中的命名空間。

- **resourceMatchers[].labelSelectors**：(可選) 資源在 Kubernetes metadata.name 欄位中定義的標籤選擇器字串 "[Kubernetes 說明文件](#)"。例如：

- "trident.netapp.io/os=linux"。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 在 trident-protect-snapshot-restore-cr.yaml 檔案中填入正確的值後，套用 CR：

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

使用 CLI 還原快照

步驟

1. 將快照還原到不同的命名空間，並將括號中的值替換為您環境中的資訊。

- `snapshot` 引數使用命名空間和快照名稱，格式為 `<namespace>/<name>`。
- `namespace-mapping` 引數使用冒號分隔的命名空間，將來源命名空間對應到正確的目標命名空間，格式為 `<source1:dest1,source2:dest2>`。

例如：

```
tridentctl-protect create snapshotrestore <my_restore_name>
--snapshot <namespace/snapshot_to_restore> --namespace-mapping
<source_to_destination_namespace_mapping>
```

使用 Trident Protect 保護 KubeVirt 虛擬機器

Trident Protect 可讓您備份與還原執行於 OpenShift Virtualization 上的 KubeVirt 虛擬機器 (VM)。您可以同時保護一或多個命名空間中的所有 VM，或使用 `includedVirtualMachines` 欄位依名稱指定特定的 VM。Trident Protect 會在備份期間自動收集所有相依的 VM 資源，而在還原期間，您可以復原整個封存或選擇性地還原個別 VM。

KubeVirt 保護模式

Trident Protect 支援兩種定義要保護的 KubeVirt 虛擬機器的方式。定義應用程式時，請選擇其中一種模式：

模式	欄位	說明
基於命名空間	<code>includedNamespaces</code>	保護一個或多個命名空間中所有符合的資源。在命名空間條目上使用 <code>'labelSelector'</code> 來動態控制包含哪些虛擬機器。
虛擬機器範圍	<code>includedVirtualMachines</code>	依命名空間和名稱保護特定 KubeVirt VM。當 VM 分佈在多個命名空間中，或您不想保護所有命名空間資源時，請使用此模式。

您必須在 `ApplicationSpec` 中指定恰好一個欄位 (`includedNamespaces` 或 `includedVirtualMachines`)。您無法在同一個應用程式中同時使用兩者。

兩種模式均支援額外的篩選功能：

- 使用 `'resourceFilter'` 來包含或排除特定資源。
- 使用 `'includedClusterScopedResources'` 以包含相容的叢集範圍資源，例如 `'StorageClass'` 物件。



Trident Protect 可在資料保護作業期間凍結和解凍 KubeVirt 虛擬機器檔案系統，以確保資料一致性。如需組態詳細資料，請參閱 ["利用 KubeVirt VM 保護資料"](#)。

備份和快照期間收集的資源

當您為包含 KubeVirt VM 的應用程式建立備份或快照時，Trident Protect 會收集選定的 VM 資源並自動探索其相依資源。

收集行為適用於以下兩種情況：

- 使用 VM 範圍的應用程式 `includedVirtualMachines`。
- 基於命名空間且包含 KubeVirt `VirtualMachine` 資源的應用程式。

VM 範圍的收集

對於 VM 範圍的應用程式，Trident Protect 從 `VirtualMachine` 中列出的每個 `includedVirtualMachines` 開始，並探索還原該 VM 所需的相依資源。

資源類型	範圍	探索方式
<code>VirtualMachine</code>	命名空間	從 <code>includedVirtualMachines</code> 清單中直接比對。
<code>VirtualMachineInstance</code>	命名空間	如果虛擬機器正在執行，則使用與虛擬機器相同的命名空間和名稱。
<code>VirtualMachineInstanceType</code>	命名空間	被引用 <code>specinstancetype</code> 時 <code>kind: VirtualMachineInstanceType</code> 。
<code>VirtualMachineClusterInstanceType</code>	叢集	由 <code>specinstancetype</code> 參照，當 <code>kind</code> 未設定或 <code>kind: VirtualMachineClusterInstanceType</code> 時。
<code>VirtualMachinePreference</code>	命名空間	被引用 <code>spec.preference</code> 時 <code>kind: VirtualMachinePreference</code> 。
<code>VirtualMachineClusterPreference</code>	叢集	由 <code>spec.preference</code> 參照，當 <code>kind</code> 未設定或 <code>kind: VirtualMachineClusterPreference</code> 時。
<code>DataVolume</code>	命名空間	被 <code>spec.template.spec.volumes[].dataVolume.name</code> 引用。
<code>PersistentVolumeClaim</code>	命名空間	從 <code>DataVolume</code> 支援的 PVC 中探索，這些 PVC 使用與 <code>DataVolume</code> 相同的名稱；直接 PVC 參照位於 <code>persistentVolumeClaim.claimName</code> ；記憶體傾印 PVC 位於 <code>memoryDump.claimName</code> ；以及暫時性 PVC 位於 <code>ephemeral.persistentVolumeClaim.claimName</code> 。
<code>PersistentVolume</code>	叢集	透過使用 <code>spec.volumeName</code> 從每個收集的 PVC 的備援 PV 中探索。
<code>Secret</code>	命名空間	從磁碟區金鑰 <code>secret.secretName</code> 中探索到； <code>containerDisk</code> 映像提取金鑰； <code>CloudInitNoCloud</code> 和 <code>CloudInitConfigDrive</code> 使用者資料和網路資料金鑰參考； <code>Sysprep</code> 金鑰； <code>KernelBoot</code> 容器映像提取金鑰；以及 <code>AccessCredentials</code> SSH 或密碼金鑰。
<code>ConfigMap</code>	命名空間	從磁碟區 <code>ConfigMaps</code> 中 <code>configMap.name</code> 和 <code>Sysprep ConfigMaps</code> 中探索到。
<code>ServiceAccount</code>	命名空間	從 <code>serviceAccount.serviceAccountName</code> 磁碟區參考中探索到。

資源類型	範圍	探索方式
NetworkAttachmentDefinition	命名空間	當網路名稱不包含 / 時，從 <code>spec.template.spec.networks[].multus.networkName</code> 中的 Multus 網路探索。僅收集相同命名空間的 NetworkAttachmentDefinition 參照。會跳過跨命名空間參照。
Pod	命名空間	透過標籤選擇器為 virt-launcher Pods 探索 <code>kubevirt.io=virt-launcher,vm.kubevirt.io/name=<vmName></code> 。
儲存類別、Trident 磁碟區和 Trident 後端	叢集	收集方式與基於命名空間的應用程式相同，以針對 VM 探索到的 PVC 為基礎。



在收集完所有虛擬機器範圍的命名空間資源後，Trident Protect 會套用標準 `resourceFilter`（如果已設定）。然後，叢集範圍的資源收集將照常進行。

基於命名空間的集合

對於基於命名空間的應用程式，Trident Protect 會掃描選定的命名空間並收集所有相符的資源。如果找到任何 KubeVirt VirtualMachine 物件，Trident Protect 會自動收集其相依資源，包括執行個體類型、偏好設定和 virt-launcher Pod，其方式與處理 VM 範圍應用程式的方式相同。

這意味著即使應用程式已使用 `includedNamespaces` 定義，VM 特定資源也會包含在備份或快照中。

使用基於命名空間的應用程式定義保護虛擬機器

在建立基於命名空間的應用程式時，Trident Protect 會掃描選定的命名空間並收集所有資源，包括所有 KubeVirt 虛擬機器。對於找到的每個虛擬機器，Trident Protect 也會收集備份和還原該虛擬機器所需的相依資源。

基於命名空間的應用程式範例 CR：

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: <application_name>
  namespace: <application_namespace>
spec:
  includedNamespaces:
    - namespace: <vm_namespace>
```

建立應用程式後，請使用標準的 Trident Protect 工作流程進行備份和快照：

- 有關快照 YAML 範例，請參閱["建立隨需快照"](#)。
- 有關備份 YAML 範例，請參閱["建立隨需備份"](#)。

恢復基於命名空間的虛擬機器應用程式的行為

由於基於命名空間的應用程式會從選定的命名空間收集資源，因此備份或快照可能包含 KubeVirt 執行時間物件

和 KubeVirt 管理的中繼資料。其中某些物件不應直接還原，因為它們代表來源叢集的執行時間狀態。

在復原過程中，Trident Protect 會套用 KubeVirt 感知轉換來移除來源叢集元資料並跳過暫存 KubeVirt 資源。這有助於 KubeVirt 在復原的環境中乾淨地重新建立虛擬機器。

資源	轉換
VirtualMachine	移除以 `kubevirt.io/` 開頭的標籤和註釋。
VirtualMachineInstance	移除以 `kubevirt.io/` 開頭的標籤和註釋。
VirtualMachineInstanceMigration	已忽略且未恢復。
VirtualMachineSnapshot	已忽略且未恢復。
VirtualMachineSnapshotContent	已忽略且未恢復。
Pod (virt-launcher)	當 pod 具有 `kubevirt.io=virt-launcher` 標籤時跳過。



Trident Protect 會依照預先定義的順序復原 KubeVirt 資源，以避免相依性問題。CDI DataVolumes (cdi.kubevirt.io) 會優先復原，以確保在建立虛擬機器物件之前，虛擬機器磁碟資料已可供使用。之後，VirtualMachines (kubevirt.io) 會在 VirtualMachineInstances 之前復原。

使用標籤選擇器進行動態虛擬機器保護

如果要動態保護 VM，但又不想列出每個 VM 名稱，請使用基於命名空間的應用程式定義和標籤選擇器。

只有 VirtualMachine CR 需要標籤。相依資源（例如 DataVolumes、PVC、Secrets 和 ConfigMaps）會自動收集。

步驟

1. 使用共用標籤標記虛擬機器 CR：

```
kubectl label virtualmachine <vm_name 1> app=<label_value> -n
<vm_namespace>
kubectl label virtualmachine <vm_name_2> app=<label_value> -n
<vm_namespace>
```

2. 建立含有 includedNamespaces 和 labelSelector 的應用程式 CR：

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: <application_name>
  namespace: <application_namespace>
spec:
  includedNamespaces:
    - namespace: <vm_namespace>
    labelSelector:
```

```
matchLabels:
  app: <label_value>
```

3. 使用標準 Trident Protect 工作流程建立備份和還原。

其他詳細資料：

- 您可以隨時透過變更標籤來新增或移除受保護的虛擬機器：

```
kubectl label virtualmachine <vm_name_to_add> app=<label_value> -n
<vm_namespace>
kubectl label virtualmachine <vm_name_to_remove> app
=<different_label_value> -n <vm_namespace>
```

- 您也可以跨多個命名空間使用標籤選擇器：

```
spec:
  includedNamespaces:
    - namespace: <vm_namespace_1>
      labelSelector:
        matchLabels:
          <label_key>: <label_value>
    - namespace: <vm_namespace_2>
      labelSelector:
        matchLabels:
          <label_key>: <label_value>
```

使用 **includedVirtualMachines** 保護特定虛擬機器

當您想要保護一個或多個命名空間中的一組指定 VirtualMachines，並從歸檔中選擇性地還原特定虛擬機時，請使用 `includedVirtualMachines`。

應用程式和復原 CR 都使用相同的 `includedVirtualMachines` 選擇器格式。

在不同的上下文中使用此選擇器：

- 在應用程式 CR 中，它定義了哪些虛擬機器受到保護。
- 在還原 CR 中，它定義了從備份或快照封存中還原哪些虛擬機器。



在還原 CR 時，此欄 `includedVirtualMachines` 位為選填欄位。如果不包含此欄位，則會還原整個封存。如果指定此欄位，則僅還原列出的虛擬機器及其相依資源。

以下 YAML 程式碼展示了共用選擇器結構：

```
includedVirtualMachines:
  - namespace: <vm_namespace_1>
    names:
      - <vm_name_1>
      - <vm_name_2>
  - namespace: <vm_namespace_2>
    names:
      - <vm_name_3>
```



多個條目位於 `includedVirtualMachines` 中，可以參考不同的命名空間，從而實現多命名空間 VM 感知應用程式定義和還原。

欄位	類型	說明
命名空間	字串	包含目標虛擬機器物件的 Kubernetes 命名空間。
名稱	字串列表	此命名空間中的一個或多個虛擬機器名稱。

基於虛擬機器的應用程式範例：

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: <application_name>
  namespace: <application_namespace>
spec:
  includedVirtualMachines:
    - namespace: <vm_namespace_1>
      names:
        - <vm_name_1>
        - <vm_name_2>
    - namespace: <vm_namespace_2>
      names:
        - <vm_name_3>
  includedClusterScopedResources:
    - group: storage.k8s.io
      kind: StorageClass
```

還原特定 KubeVirt VM

您可以使用 `includedVirtualMachines` 還原 CR，僅從備份、快照或複製快照存檔中還原選定的 KubeVirt 虛擬機器。

當 `includedVirtualMachines` 在還原 CR 上指定時，Trident Protect 僅還原列出的 VirtualMachines 及其相依資源，例如 `VirtualMachineInstance`、`DataVolume`、`PersistentVolumeClaim`、`PersistentVolume`、`Secret`、`ConfigMap`、`ServiceAccount`，以及其他 VM 相關物件。

如果您未在復原 CR 中指定 `includedVirtualMachines`，Trident Protect 將根據復原 CR 設定還原完整的歸檔。

支援的還原 **CR** 和 **CLI** 命令

下表列出了支援的還原 CR `includedVirtualMachines` 及其對應的 CLI 命令。

恢復 CR	CLI 指令	說明
BackupRestore	<code>tridentctl-protect create backuprestore</code>	從備份還原到新的或不同的命名空間映射。支援 <code>namespaceMapping</code> 和 <code>storageClassMapping</code> 。
BackupInplaceRestore	<code>tridentctl-protect create backupinplacerestore</code>	從備份還原到原始命名空間或多個命名空間。
SnapshotRestore	<code>tridentctl-protect create snapshotrestore</code>	從快照還原到新的或不同的命名空間映射。支援 <code>namespaceMapping</code> 和 <code>storageClassMapping</code> 。
SnapshotInplaceRestore	<code>tridentctl-protect create snapshotinplace restore</code>	從快照還原到原始命名空間或多個命名空間。
ReplicateSnapshotRestore	僅支援 YAML 格式，或如果您的環境中支援，也可以使用受支援的 CLI 命令。	從複製的快照還原。支援 <code>namespaceMapping</code> 、 <code>storageClassMapping</code> ，以及使用 <code>inPlaceRestore</code> 旗標進行原地還原。



`tridentctl-protect` CLI 在還原命令上沒有適用於 `includedVirtualMachines` 的旗標。若要還原特定的 VMs，您必須直接使用 `kubectl apply` 套用還原 CR YAML 檔案。您可以從頭撰寫 YAML，或是搭配 `--dry-run --output yaml` 使用 CLI 以產生初始檔案，在 `spec` 下方新增 `includedVirtualMachines` 欄位，然後套用它。

虛擬機器範圍的復原行為

The `includedVirtualMachines` 恢復 CR 中的欄位使用與應用程式 CR 相同的選擇器格式：

```
includedVirtualMachines:
- namespace: <source_vm_namespace>
  names:
    - <vm_name_1>
    - <vm_name_2>
```

對於還原 CR，`includedVirtualMachines` 中的命名空間值指的是備份、快照或複製快照封存中存在的來源命名空間。

如果使用 `namespaceMapping`，Trident Protect 會先從來源歸檔中選擇要求的虛擬機，然後在還原過程中套用

命名空間對應。如果使用 `storageClassMapping`，Trident Protect 會在還原轉換階段套用儲存類別對應。

使用 CLI 產生還原 YAML 檔案

您可以使用 `tridentctl-protect` 來產生基本復原 CR，然後編輯 YAML 以新增 `includedVirtualMachines`。

```
tridentctl-protect create <restore_command> <restore_name> \
  <restore_options> \
  --dry-run --output yaml > <restore_name>.yaml
```

編輯產生的 YAML，並在 `spec` 下方新增 `includedVirtualMachines` 欄位，然後套用該檔案：

```
kubectl apply -f <restore_name>.yaml
```

範例：定義一個基於虛擬機器的應用程式

以下應用程式保護跨兩個命名空間的三個特定虛擬機器。

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  name: production-vms
  namespace: prod
spec:
  includedVirtualMachines:
    - namespace: prod
      names:
        - app-server
        - database-server
    - namespace: monitoring
      names:
        - prometheus-vm
  includedClusterScopedResources:
    - group: storage.k8s.io
      kind: StorageClass
```

範例：建立備份

為基於虛擬機器的應用程式建立備份時，請使用標準備份 CR。備份 CR 中不需要任何虛擬機器特定的欄位。

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
```

```

name: daily-backup
namespace: prod
spec:
  applicationRef: production-vms
  appVaultRef: s3-vault

```

範例：從備份還原單一虛擬機

以下範例僅從備份存檔中還原 database-server。存檔中的其他虛擬機器（例如 app-server 和 prometheus-vm）將被跳過。

```

apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: restore-db-only
  namespace: prod-vms-restore
spec:
  appVaultRef: s3-vault
  appArchivePath: backups/production-vms/2026-03-10T00-00-00Z
  namespaceMapping:
    - source: prod
      destination: prod-dr
  includedVirtualMachines:
    - namespace: prod
      names:
        - database-server

```

```
kubectl apply -f restore-db-only.yaml
```

僅 `database-server` 及其相依資源（例如 DataVolumes、PVCs、PVs、Secrets、ConfigMaps 及相關 KubeVirt 資源）會還原。

範例：從備份中就地還原單一虛擬機

以下範例僅將 `database-server` 從備份存檔還原到其原始命名空間。

```

apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: ipr-db-only
  namespace: prod
spec:
  appVaultRef: s3-vault
  appArchivePath: backups/production-vms/2026-03-10T00-00-00Z

```

```
includedVirtualMachines:
- namespace: prod
  names:
    - database-server
```

```
kubectl apply -f ipr-db-only.yaml
```

範例：從快照還原單一虛擬機

以下範例僅從快照存檔還原 ubuntu-vm-blue-a627be38。

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: blue-vm-snap-restore
  namespace: blue
spec:
  appVaultRef: my-appvault
  appArchivePath: snapshots/protectctl-blue-vm/snap-1
  includedVirtualMachines:
    - namespace: blue
      names:
        - ubuntu-vm-blue-a627be38
```

```
kubectl apply -f blue-vm-snap-restore.yaml
```

將虛擬機器還原與其他過濾器結合使用

您可以在同一個還原 CR 中同時使用 `includedVirtualMachines`、`resourceFilter`、`namespaceMapping` 和 `storageClassMapping` 來微調要還原的內容。

新增 `resourceFilter` 時，Trident Protect 首先會選擇 `includedVirtualMachines` 中列出的 VM 及其相依資源。然後套用資源篩選器，進一步縮小這些結果中包含或排除的項目範圍。

```
spec:
  includedVirtualMachines:
    - namespace: <vm_namespace>
      names:
        - <vm_name>
  resourceFilter:
    resourceSelectionCriteria: Include
    resourceMatchers:
      - kinds: ["PersistentVolumeClaim"]
```

```
names: ["<pvc_name>"]
```

對於 BackupRestore、SnapshotRestore 和 ReplicateSnapshotRestore，namespaceMapping 和 storageClassMapping 協同工作 includedVirtualMachines。includedVirtualMachines 中的命名空間參考對應於歸檔中出現的來源命名空間。命名空間和儲存類別映射在過濾完成後，於復原轉換階段套用。

有關還原行為的詳細資訊，請參閱 ["使用 Trident Protect 恢復應用程式"](#)。

使用 CLI 建立虛擬機器範圍的應用程式

使用 `--virtual-machines` 標誌可將應用程式的範圍限定於特定的 KubeVirt VM，而不是整個命名空間。`--virtual-machines` 標誌與 `--namespaces` 互斥。

步驟

1. 運行以下命令之一以建立應用程式，並將括號中的值替換為您的環境資訊。`--virtual-machines` 標誌的格式為 <namespace>(<vm_name>)。對於多個 VM，請在括號內使用逗號分隔的名稱：

- 命名空間中的單一虛擬機器：

```
tridentctl-protect create application <application_name> \
  -n <application_namespace> \
  --virtual-machines "<vm_namespace>(<vm_name>)"
```

- 跨命名空間的多台虛擬機器：

```
tridentctl-protect create application <application_name> \
  -n <application_namespace> \
  --virtual-machines "<vm_namespace_1>(<vm_name_1>,<vm_name_2>
),<vm_namespace_2>(<vm_name_3>)"
```

相關資訊

- ["定義管理應用程式"](#)
- ["保護應用程式"](#)
- ["使用 Trident Protect 恢復應用程式"](#)
- ["使用進階還原設定"](#)
- ["安裝 Trident Protect CLI 外掛程式"](#)
- ["使用 AppVault 物件來管理儲存桶"](#)

管理 Trident Protect 執行掛鉤

執行鉤子是一種自訂操作，您可以將其配置為與託管應用程式的資料保護操作一起運行。例如，如果您有一個資料庫應用程式，則可以使用執行鉤子在建立快照之前暫停所有資料庫事務，並在快照完成後恢復事務。這可以確保應用程式快照的一致性。

執行掛鉤的類型

Trident Protect 支援以下幾種執行鉤子類型，取決於它們的執行時機：

- 快照前
- 快照後
- 備份前
- 備份後
- 還原後
- 故障轉移後

執行順序

執行資料保護作業時，執行掛鉤事件會依照以下順序發生：

1. 任何適用的自訂作業前執行掛鉤都會在適當的容器上執行。您可以建立並運行任意數量的自訂預操作鉤子，但這些鉤子在操作之前的執行順序既無法保證也無法配置。
2. 如果適用，檔案系統會凍結。["深入瞭解如何使用 Trident Protect 設定檔案系統凍結"](#)。
3. 執行資料保護作業。
4. 如果適用，則解凍已凍結的檔案系統。
5. 任何適用的自訂後操作執行鉤子都會在相應的容器上運行。您可以建立並運行任意數量的自訂後操作鉤子，但這些鉤子在操作後的執行順序既無法保證也無法配置。

如果您建立多個相同類型的執行鉤子（例如，快照前鉤子），則這些鉤子的執行順序無法保證。但是，不同類型鉤子的執行順序是有保證的。例如，以下是包含所有不同類型鉤子的組態的執行順序：

1. 已執行快照前鉤子
2. 執行快照後掛鉤
3. 執行備份前掛鉤
4. 執行備份後掛鉤



前述順序範例僅適用於執行不使用現有快照的備份時。



在生產環境中啟用執行鉤子腳本之前，請務必先對其進行測試。您可以使用 'kubectl exec' 指令方便地測試這些腳本。在生產環境中啟用執行鉤子後，請測試產生的快照和備份，以確保它們的一致性。您可以將應用程式複製到臨時命名空間，還原快照或備份，然後測試應用程式。



如果快照前執行鉤子新增、變更或刪除 Kubernetes 資源，則這些變更將包含在快照或備份以及任何後續還原作業中。

關於自訂執行掛鉤的重要說明

在規劃應用程式的執行鉤子時，請考慮以下幾點。

- 執行掛鉤必須使用指令碼來執行動作。許多執行掛鉤可以參照同一個指令碼。

- Trident Protect 要求執行鉤子使用的腳本以可執行 shell 腳本的格式編寫。
- 指令碼大小限制為 96KB。
- Trident Protect 使用執行掛鉤設定和任何相符條件來判斷哪些掛鉤適用於快照、備份或還原作業。



由於執行鉤子通常會降低甚至完全停用其所針對應用程式的功能，因此您應該始終盡量縮短自訂執行鉤子的執行時間。如果您啟動了一個帶有關聯執行鉤子的備份或快照操作，但隨後取消了該操作，只要備份或快照操作已經開始，這些鉤子仍然可以執行。這意味著備份後執行鉤子中使用的邏輯不能假定備份已經完成。

執行掛鉤篩選器

當您新增或編輯應用程式的執行鉤子時，您可以為該執行鉤子添加過濾器，以管理鉤子將匹配哪些容器。篩選器適用於在所有 Container 上使用相同 Container 映像，但可能將每個映像用於不同用途的應用程式（例如 Elasticsearch）。篩選器可讓您建立執行掛鉤在部分（但不一定全部）相同 Container 上執行的情境。如果為單一執行掛鉤建立多個篩選器，它們將透過邏輯 AND 運算子進行組合。每個執行掛鉤最多可以有 10 個作用中篩選器。

新增至執行鉤子的每個篩選器都使用正規表示式來比對叢集中的 Container。當鉤子匹配到容器時，它將在該容器上運行其關聯的腳本。篩選器的正規表示式使用正規表示式 2 (RE2) 語法，該語法不支援建立從符合清單中排除 Container 的篩選器。有關 Trident Protect 支援的執行鉤子過濾器正規表示式語法的更多資訊，請參閱 ["Regular Expression 2 \(RE2\) 語法支援"](#)。



如果在還原或複製作業之後執行的執行鉤子中新增命名空間篩選器，且還原或複製來源和目的地位於不同的命名空間中，則命名空間篩選器僅套用於目的地命名空間。

執行掛鉤範例

造訪 ["NetApp Verda GitHub 專案"](#) 下載適用於 Apache Cassandra 和 Elasticsearch 等熱門應用程式的真實執行鉤子。您也可以查看範例，並從中取得建置自訂執行鉤子的想法。



Verda 儲存庫中的腳本按原樣提供，並未獲得 NetApp 的官方支援。NetApp 支援僅涵蓋 Trident Protect 中的執行掛鉤框架。

建立執行掛鉤

您可以使用 Trident Protect 為應用程式建立自訂執行鉤子。您需要擁有 Owner、Admin 或 Member 權限才能建立執行鉤子。

使用 CR

步驟

1. 建立自訂資源 (CR) 檔案並將其命名為 `trident-protect-hook.yaml`。
2. 設定以下屬性以符合您的 Trident Protect 環境和叢集組態：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.applicationRef**：（必填）要執行執行鉤子的應用程式的 Kubernetes 名稱。
 - **spec.stage**：（必需）一個字串，指示執行鉤子應在操作的哪個階段運行。可選值：

- 預先
- 發佈
- **spec.action**：（必要）一個字串，指示執行鉤子將執行的操作，假設符合任何指定的執行鉤子篩選器。可選值：
 - 快照
 - 備份
 - 還原
 - 容錯移轉
- **spec.enabled**：（可選）指示此執行鉤子是否啟用或停用。如果未指定，則預設值為 true。
- **spec.hookSource**：（必填）包含 base64 編碼的 hook 腳本的字串。
- **spec.timeout**：（可選）一個數字，定義執行鉤子允許運行的最長時間（以分鐘為單位）。最小值為 1 分鐘，如果未指定，則預設值為 25 分鐘。
- **spec.arguments**：（可選）您可以為執行掛鉤指定的 YAML 引數清單。
- **spec.matchingCriteria**：（可選）條件鍵值對的可選清單，每個鍵值對構成一個執行鉤子過濾器。每個執行鉤子最多可以新增 10 個過濾器。
- **spec.matchingCriteria.type**：（可選）用於識別執行鉤子過濾器類型的字串。可選值：
 - ContainerImage
 - ContainerName
 - PodName
 - PodLabel
 - NamespaceName
- **spec.matchingCriteria.value**：（可選）識別執行鉤子過濾器值的字串或正規表示式。

YAML 範例：

```
apiVersion: protect.trident.netapp.io/v1
kind: ExecHook
metadata:
  name: example-hook-cr
  namespace: my-app-namespace
  annotations:
    astra.netapp.io/astra-control-hook-source-id:
/account/test/hookSource/id
spec:
  applicationRef: my-app-name
  stage: Pre
  action: Snapshot
  enabled: true
  hookSource: IyEvYmluL2Jhc2gKZWNoYAiZXhhbXBsZSBzY3JpcHQiCg==
  timeout: 10
  arguments:
```

```

- FirstExampleArg
- SecondExampleArg
matchingCriteria:
- type: containerName
  value: mysql
- type: containerImage
  value: bitnami/mysql
- type: podName
  value: mysql
- type: namespaceName
  value: mysql-a
- type: podLabel
  value: app.kubernetes.io/component=primary
- type: podLabel
  value: helm.sh/chart=mysql-10.1.0
- type: podLabel
  value: deployment-type=production

```

3. 在用正確的值填入 CR 檔案後，套用 CR：

```
kubectl apply -f trident-protect-hook.yaml
```

使用 CLI

步驟

1. 建立執行鉤子，並將括號中的值替換為您環境中的資訊。例如：

```

tridentctl-protect create exehook <my_exec_hook_name> --action
<action_type> --app <app_to_use_hook> --stage <pre_or_post_stage>
--source-file <script-file> -n <application_namespace>

```

手動執行執行掛鉤

您可以手動執行 execution hook 以進行測試，或者在失敗後需要手動重新執行 hook。您需要擁有 Owner、Admin 或 Member 權限才能手動執行 execution hook。

手動執行執行掛鉤包含兩個基本步驟：

1. 建立資源備份，該備份會收集資源並建立它們的備份，從而確定鉤子函數的運作位置
2. 針對備份執行執行掛鉤

▼ 步驟 1：建立資源備份

使用 CR

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `trident-protect-resource-backup.yaml`。
2. 設定以下屬性以符合您的 Trident Protect 環境和叢集組態：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.applicationRef**：（必填）要為其建立資源備份的應用程式的 Kubernetes 名稱。
 - **spec.appVaultRef**：（必填）儲存備份內容的 AppVault 名稱。
 - **spec.appArchivePath**：AppVault 內儲存備份內容的路徑。您可以使用以下命令來尋找此路徑：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o  
jsonpath='{.status.appArchivePath}'
```

YAML 範例：

```
---  
apiVersion: protect.trident.netapp.io/v1  
kind: ResourceBackup  
metadata:  
  name: example-resource-backup  
spec:  
  applicationRef: my-app-name  
  appVaultRef: my-appvault-name  
  appArchivePath: example-resource-backup
```

3. 在用正確的值填入 CR 檔案後，套用 CR：

```
kubectl apply -f trident-protect-resource-backup.yaml
```

使用 CLI

步驟

1. 建立備份，並將括號中的值替換為您環境中的資訊。例如：

```
tridentctl protect create resourcebackup <my_backup_name> --app  
<my_app_name> --appvault <my_appvault_name> -n <my_app_namespace>  
--app-archive-path <app_archive_path>
```

2. 檢視備份狀態。您可以重複使用此範例命令，直到作業完成：

```
tridentctl protect get resourcebackup -n <my_app_namespace>
<my_backup_name>
```

3. 確認備份是否成功：

```
kubectl describe resourcebackup <my_backup_name>
```

▼ 步驟 2：執行 **execution hook**

使用 **CR**

步驟

1. 建立自訂資源（CR）檔案並將其命名為 `trident-protect-hook-run.yaml`。
2. 設定以下屬性以符合您的 Trident Protect 環境和叢集組態：
 - **metadata.name**：（必填）此自訂資源的名稱；請為您的環境選擇一個唯一且有意義的名稱。
 - **spec.applicationRef**：（必填）確保此值與您在步驟 1 中建立的 ResourceBackup CR 中的應用程式名稱相符。
 - **spec.appVaultRef**：（必填）請確保此值與您在步驟 1 中建立的 ResourceBackup CR 的 appVaultRef 相符。
 - **spec.appArchivePath**：請確保此值與您在步驟 1 中建立的 ResourceBackup CR 內的 appArchivePath 相符。

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o
jsonpath='{.status.appArchivePath}'
```

- **spec.action**：（必要）一個字串，指示執行鉤子將執行的操作，假設符合任何指定的執行鉤子篩選器。可選值：
 - 快照
 - 備份
 - 還原
 - 容錯移轉
- **spec.stage**：（必需）一個字串，指示執行鉤子應在操作的哪個階段運行。此鉤子運行不會在任何其他階段運行鉤子。可選值：
 - 預先
 - 發佈

YAML 範例：

```
---
```

```

apiVersion: protect.trident.netapp.io/v1
kind: ExecHooksRun
metadata:
  name: example-hook-run
spec:
  applicationRef: my-app-name
  appVaultRef: my-appvault-name
  appArchivePath: example-resource-backup
  stage: Post
  action: Failover

```

3. 在用正確的值填入 CR 檔案後，套用 CR：

```
kubectl apply -f trident-protect-hook-run.yaml
```

使用 CLI

步驟

1. 建立手動執行掛鉤執行請求：

```

tridentctl protect create exehooksruntime <my_exec_hook_run_name> -n
<my_app_namespace> --action snapshot --stage <pre_or_post> --app
<my_app_name> --appvault <my_appvault_name> --path
<my_backup_name>

```

2. 檢查執行掛鉤執行的狀態。您可以重複執行此命令，直到操作完成：

```

tridentctl protect get exehooksruntime -n <my_app_namespace>
<my_exec_hook_run_name>

```

3. 描述 exehooksruntime 物件以查看最終詳細資訊和狀態：

```

kubectl -n <my_app_namespace> describe exehooksruntime
<my_exec_hook_run_name>

```

解除安裝 Trident Protect

如果您要從試用版升級到完整版產品，可能需要移除 Trident Protect 元件。

若要移除 Trident Protect，請執行下列步驟。

步驟

1. 刪除 Trident Protect CR 檔案：



版本 25.06 及更高版本不需要此步驟。

```
helm uninstall -n trident-protect trident-protect-crds
```

2. 移除 Trident Protect：

```
helm uninstall -n trident-protect trident-protect
```

3. 移除 Trident Protect 命名空間：

```
kubectl delete ns trident-protect
```

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。