ホワイトペーパー

コンテンツ取扱
印刷可能 **編集不可**

Hitachi Storage Plug-in for Containers を使用した Red Hat® OpenShift® 環境のストレージ連携バックアップ

Implementation Guide for Veritas NetBackup™ with Container Storage Interface (CSI) using Hitachi storage systems on Red Hat® OpenShift® Container Platform

2023 年 4 月発行

株式会社　日立製作所

目次

【免責事項】

- 本書の内容の一部または全部を無断転載することは禁止されています。
- 本書の内容に関しては将来予定なしに変更することがあります。
- 日立製作所の許可なく複製、改変等を行うことはできません。
- 日立製作所が製品やサービスについて行う保証は、製品添付の保証文章に記載した内容のみに限定され、本書のどの箇所であっても何ら新規の保証を行うものではありません。
- 運用した結果の影響については、責任を負いかねますのでご了承ください。
- 本書に技術的あるいは編集上の誤りや欠陥があったとしても、日立製作所は一切の責任を負わないものとします。

【登録商標、商標】

- Hitachi 及び日立は、株式会社　日立製作所の登録商標または商標です。
- Veritas、Veritas ロゴ、および NetBackup は、米国およびその他の国における Veritas Technologies LLC またはその関連会社の登録商標です。
- Red Hat、Red Hat ロゴ、および OpenShift は、米国およびその他の国における Red Hat, Inc. またはその子会社の登録商標です。
- Kubernetes は、米国およびその他の国における The Linux Foundation の商標または登録商標です。
- その他の会社名、製品名は各社の登録商標または商標です。

要約

Red Hat OpenShift Container Platform の container 用に日立ストレージプラグインを使用して NetBackup スナップショットとバックアップオペレーションを設定する方法について説明します。

1　はじめに

1.1　本資料について

本資料では、Hitachi Storage Plug-in for Containers で Red Hat OpenShift Container Platform とストレージを連携させ、Veritas NetBackup 10 でバックアップ/リストアする方法について説明します。

本資料の作業順に従って Hitachi Storage Plug-in for Containers のインストール および NetBackup によるバックアップの準備 を行うことにより、Veritas NetBackup 10 での container アプリケーションの Persistent volume や関連する Kubernetes リソースのバックアップ/リストア操作 が可能となります。

下記は本資料に含まれません。実施方法については各製品ドキュメントを参照してください。
- Red Hat OpenShift Container Platform の構築
- Veritas NetBackup 10 環境の構築
- NetBackup Kubernetes Operator および NetBackup Kubernetes datamover のインストール

本資料はオンラインのベアメタル環境を前提としています。インターネット接続が無い場合や仮想環境の場合、追加の作業が必要となる場合があります。

1.1.1　マルチパス構成のサポート

本資料で用いている Veritas NetBackup 10.0 では、ストレージのパス構成はシングルパス構成のみがサポートされていましたが、Veritas NetBackup 10.1.1 でマルチパス構成がサポートされました。
ストレージ接続がマルチパス構成である Red Hat OpenShift Container Platform をバックアップ/リストアする場合は、本資料の説明内容が一部変更になります。
変更点については、A1 付録 を参照してください。

1.1.2　Veritas NetBackup 10.1.1 について

Veritas NetBackup 10.1.1 の詳細については、製品ドキュメントを参照してください。
ストレージ接続のパス構成に関わらず Veritas NetBackup 10.1.1 を用いる場合は、本資料の説明内容が一部変更になります。
変更点については、A1 付録 の A1.4 注意事項 を参照してください。

1.2　文書規則

本資料は次の文書規則を使用します。

Convention	Description

Bold	ウィンドウタイトル、メニュー、メニューオプション、ボタン、フィールド、ラベルを含むウィンドウ内のテキスト 例： **OK** をクリックする リスト項目の強調する言葉
Italic	ドキュメントタイトルやテキスト内の強調する言葉
`Monospace`	スクリーン上に表示されたテキストまたはユーザーによって入力されるテキスト 例：`oc get pvc`

1.3 対象読者

本資料の対象読者は、Hitachi storage system の管理者および構築者、Red Hat OpenShift Container Platform において Veritas NetBackup 10 を導入する IT プロフェッショナルです。
対象読者は以下の知識と経験を必要とします。
・SAN の基本的な知識
・サーバの基本的な知識
・ネットワークの基本的な知識
・Hitachi storage system の管理知識
・Veritas NetBackup の管理経験
・Red Hat OpenShift Container Platform の管理経験
・Kubernetes の管理経験

1.4 更新履歴

更新内容	更新日付
初版	2023年3月
マルチパス構成のサポート Veritas NetBackup 10.1.1対応	2023年4月

1.5 製品のダウンロード

Hitachi Storage Plug-in for Containers のダウンロードは Hitachi Vantara サポートウェブサイト https://support.hitachivantara.com/から利用できます。

製品リリース後のアップデートを含む最新のダウンロードのアクセスは、ログイン後、製品ダウンロードを選択してください。

本資料が前提とする Red Hat OpenShift Container Platform における Hitachi Storage Plug-in for Containers のダウンロードは、OpenShift web UI の OperatorHub から利用できます。詳細な手順については 4 章を参照してください。

2　本ソリューションの概要

Hitachi Storage Plug-in for Containers は、Container Storage Interface(CSI)を使用して OpenShift Container Platform を Hitachi storage system と統合します。バックアップソフトウェアの Veritas NetBackup 10 と Hitachi Storage Plug-in for Containers を連携すると、Hitachi storage system の機能を使用して、OpenShift Container Platform でのデータ損失からの保護を実現します。

Hitachi Storage Plug-in for Containers と連携することにより、高性能・高信頼な Persistent volume を使用できます。また、この Persistent volume に対するアレイベースでのスナップショットにより、バックアップウィンドウを短縮できます。

2.1　システム構成

以下に、Hitachi Storage Plug-in for Containers を用いた Red Hat OpenShift Container Platform における Veritas NetBackup 10 のバックアップシステムの構成例を示します。

本システムにおけるバックアップのユースケースは Figure 1 に示す 2 つ(Snapshot storage only と Backup from snapshot)があります。詳細については、次の **2.2 Hitachi Storage Plug-in for Containers を用いたバックアップのユースケース** セクションを参照してください。

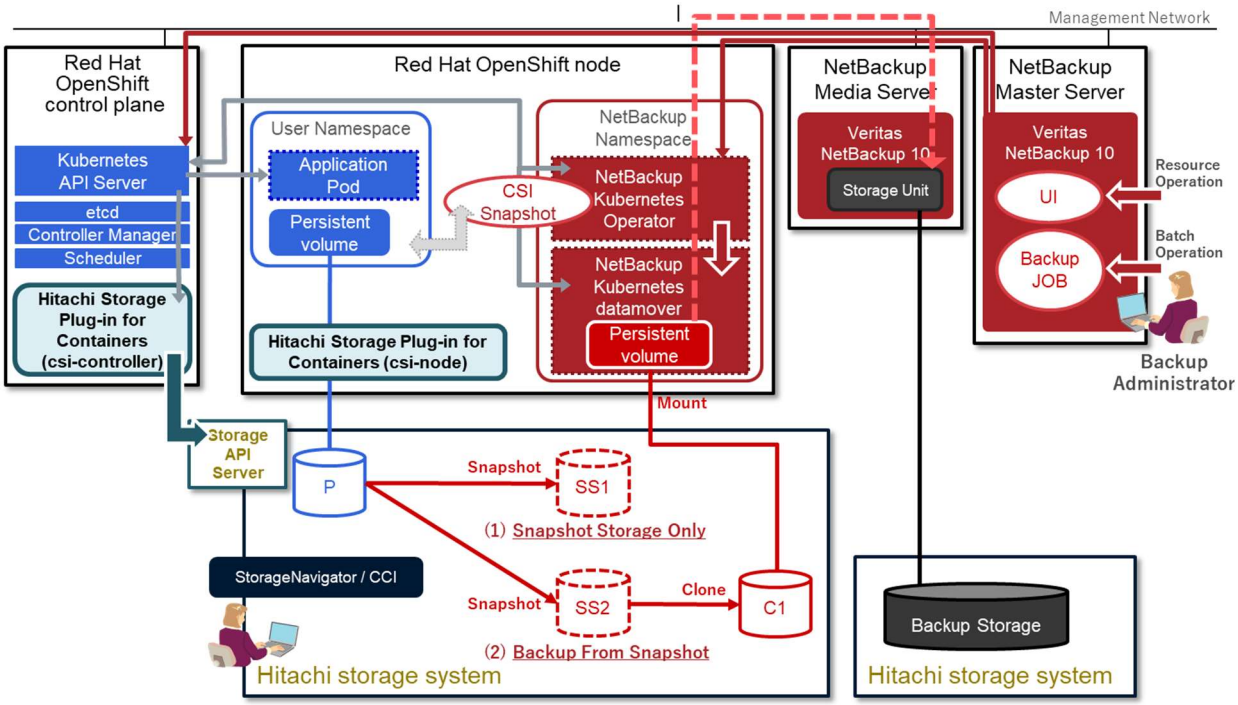

Figure 1. System configuration diagram

Red Hat OpenShift Container Platform

- **Red Hat OpenShift control plane:** OpenShift Container Platform cluster の制御に必要なサービスを実行し、node のワークロードを管理します。

- **Red Hat OpenShift node:** OpenShift Container Platform cluster のユーザーがリクエストした実際のワークロードが実行され、管理されます。
- **Namespace:** 名前空間のスコープを提供し、複数のユーザーの間でクラスタリソースを分割する方法です。
- **Persistent volume:** クラスタ管理者によって静的にプロビジョニングされているか、または StorageClass オブジェクトを使用して動的にプロビジョニングされているクラスタのストレージの一部です。

Hitachi Storage Plug-in

- **Hitachi Storage Plug-in for Containers:** Hitachi storage system から Persistent volume を提供します。これにより、ステートフル アプリケーションは、container のライフ サイクルが終了した後にデータを永続化および保守できます。

  Hitachi Storage Plug-in for Containers は、ステートフル・アプリケーションを実行するために container を作成するために使用できるライブラリー、設定、およびコマンドを含むソフトウェアコンポーネントです。
- **csi-controller:** 主にストレージ操作用の CSI コントローラー・サービスを実装します。これは Deployment としてデプロイされ、control plane 上でのみ実行されます。
- **csi-node:** 主に各 node 上のボリュームを管理する CSI ノード・サービスを実装します。これは DaemonSet としてデプロイされ、すべての node にこのコンポーネントが必要です。

NetBackup System

- **NetBackup Master Server:** NetBackup のバックアップ管理機能を提供します。
- **NetBackup Media Server:** 接続されているストレージデバイスを NetBackup で使用可能とし、バックアップ実行を行います。Master Server が Media Server の役割をする構成も可能です。
- **Storage Unit:** バックアップデータの保存先です。
- **NetBackup Kubernetes Operator:** NetBackup と Kubernetes とのつなぎの役割を担います。バックアップデータの管理情報が格納されます。
- **NetBackup Kubernetes datamover:** NetBackup Kubernetes Operator で取得したバックアップデータを NetBackup Media Server に転送します。

Note: Hitachi Storage Plug-in for Containers を利用するためには、Hitachi storage system の管理者・構築者が pool を作成する等、事前設定を行う必要があります。詳細については、後述する構築手順を参照してください。

2.2 Hitachi Storage Plug-in for Containers を用いたバックアップのユースケース

本システムにおけるバックアップのユースケースは、以下の 2 つがあります。

(1) Snapshot storage only

(2) Backup from snapshot

(1) Snapshot storage only
Hitachi storage system 内へ、スナップショットを保存します。
プロセスの詳細：

1. Hitachi storage system 内でスナップショットを取得する。

(2) Backup from snapshot
NetBackup Media Server に接続された外部ストレージへ、バックアップを保存します。
プロセスの詳細：

1. １次バックアップとして、Hitachi storage system 内でスナップショットを取得する。
2. Hitachi storage system 内でスナップショットからクローンを作成する。
3. ２次バックアップとして、NetBackup Kubernetes datamover を経由してクローンを NetBackup Media Server に接続された外部ストレージへ転送する。

3　システム要件

本章は、Veritas NetBackup 10 と Hitachi Storage Plug-in for Containers を用いた Red Hat OpenShift Container Platform における、バックアップシステムを構築するために必要となるハードウェアおよびソフトウェアコンポーネントについて説明します。

3.1　ハードウェアコンポーネント

本ソリューションに適用できる Hitachi storage system を Table 1、server 構成を Table 2 に示します。

Table 1. Applicable Hitachi storage systems

Hitachi storage systems	Microcode Version
Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H	90-08-01 or later
Hitachi Virtual Storage Platform E1090, E1090H, E990, E790, E790H, E590, E590H	93-06-01 or later

Table 2. Required server configuration

System	Server purpose	Server type
Backup System	NetBackup Master Server	Bare metal server (Note 1)
	NetBackup Media Server	Bare metal server (Note 1)
Production System	OpenShift control plane	Bare metal server (Note 2)
	OpenShift node	Bare metal server (Note 2) (Note 3)

Notes:

1. Veritas NetBackup 10 のシステム要件に従った OS および NetBackup Server Software のインストールが完了していること。詳細については Veritas 社 Veritas サポートの NetBackup™ Installation Guide を参照してください。

   Veritas 社ドキュメント検索ページ： https://sort.veritas.com/documents/

2. Hitachi Storage Plug-in for Containers のシステム要件に従った Red Hat OpenShift Container Platform で構築済みであること。詳細については Hitachi Storage Plug-in for Containers Release Notes を参照してください。

   Hitachi Storage Plug-in for Containers ドキュメントページ： https://knowledge.hitachivantara.com/Documents/Adapters_and_Drivers/Storage_Adapters_and_Drivers/Containers/Storage_Plug-in_for_Containers

3. Veritas NetBackup 10 のシステム要件に従った NetBackup Kubernetes Operator および NetBackup Kubernetes datamover のインストールが完了していること。詳細については Veritas 社 Veritas サポートの NetBackup™ Web UI Kubernetes Administrator's Guide を参照してください。

   Veritas 社ドキュメント検索ページ： https://sort.veritas.com/documents/

3.2 ソフトウェアコンポーネント

本ソリューションで必要となるソフトウェアコンポーネントを Table 3 に示します。

Table 3. Required software components

	Software	Version
Hitachi	Hitachi Storage Virtualization Operating System (SVOS) - Hitachi LUN Manager - Hitachi Dynamic Provisioning	90-08-01 or later (*1) 93-06-01 or later (*2)
	Hitachi Local Replication (Hitachi Thin Image)	
	Hitachi Storage Plug-in for Containers	3.9.0
Red Hat	Red Hat OpenShift Container Platform	4.7 - 4.9
	Red Hat Enterprise Linux CoreOS	7.0 - 7.9, 8.2 - 8.4
Veritas	NetBackup	10.0

(*1) : Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H

(*2) : Hitachi Virtual Storage Platform E1090, E1090H, E990, E790, E790H, E590, E590H

4　環境構築

本手順では、Hitachi storage system の事前設定と、Hitachi Storage Plug-in for Containers のインストール手順および初期設定について説明します。

Hitachi Storage Plug-in for Containers がサポートする単一 pool 構成について説明します。

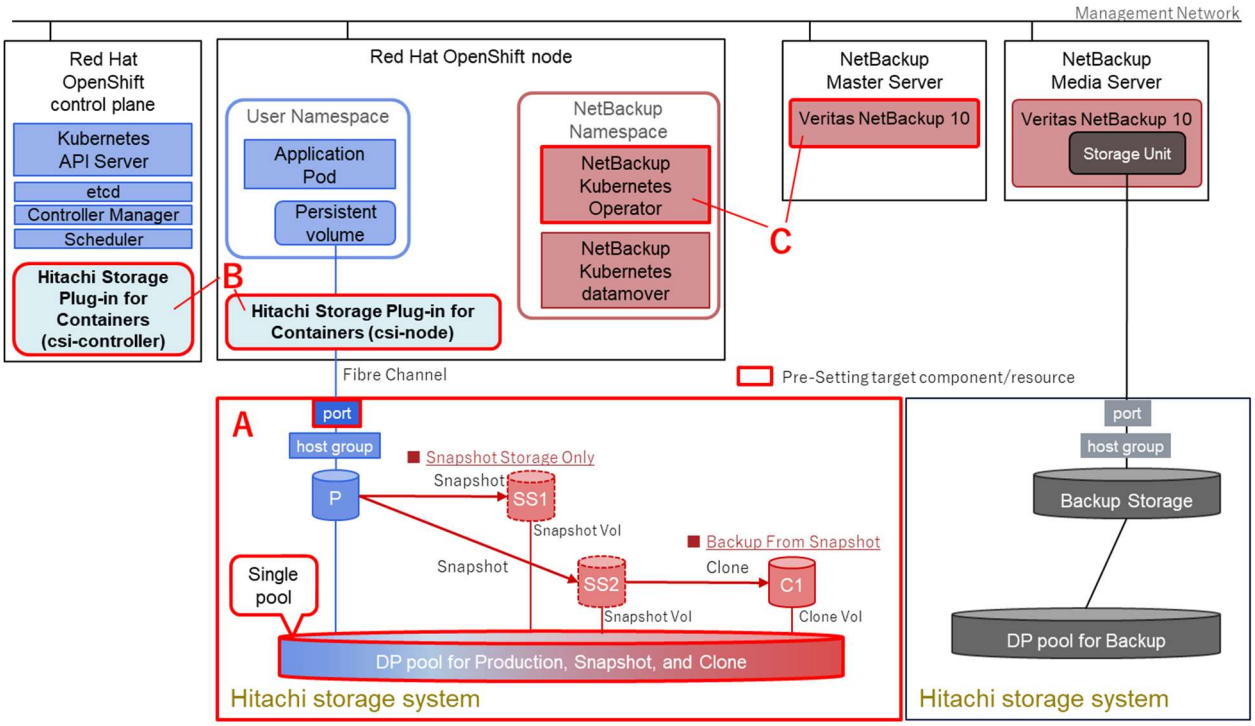

Figure 2. Basic system configuration, components, and resources to be deployed.

A.　Hitachi storage system の設定

（1）Program Products のライセンスの確認

（2）Parity Group の設定

（3）pool の作成

（4）port の設定

B.　Hitachi Storage Plug-in for Containers のインストールと初期設定

（1）Operator のインストール

（2）インスタンスの作成

（3）Secret の設定

（4）StorageClass の設定

C. NetBackup によるバックアップの準備

(1) Kubernetes クラスタの追加

(2) スナップショット操作のための構成設定

(3) バックアップおよびリストア操作のための構成設定

上記の A から C の手順を実施するためには、以下の前提条件を満たしている必要があります。

- 各種 server、および Hitachi storage system の SAN / LAN の物理結線が完了していること
- Hitachi Storage Plug-in for Containers のシステム要件に従った server、Hitachi storage system、および Red Hat OpenShift Container Platform が構築済みであること
- Red Hat OpenShift Container Platform の CLI である oc コマンドを実行できる作業用 server が使用できること

  oc コマンドは Kubernetes API Server に対して発行され、OpenShift Container Platform cluster 内の適切な node で処理されます
- Veritas NetBackup 10 環境が構築済みであり、Red Hat OpenShift Container Platform に NetBackup Kubernetes Operator および NetBackup Kubernetes datamover のインストールが完了していること

4.1 Hitachi storage system の設定

4.1.1 Program Products のライセンスの確認

Hitachi Storage Plug-in for Containers を利用するには、以下のライセンスが必要となります。

1. **Hitachi Storage Virtualization Operating System (SVOS)**
   - Hitachi LUN Manager
   - Hitachi Dynamic Provisioning
2. **Hitachi Local Replication**
   - Hitachi Thin Image

以下に Program Products のライセンス確認方法を示します。

Before you begin

ストレージ管理者として StorageNavigator にログインします。

Procedure

1. [**Administration**] > [**License Keys**]に移動し、必要な各 Program Products のステータスが"**Installed**"であることを確認します。

Program Product Name	Status	Key Type	Licensed Capacity		Term (days)
			Permitted (TB)	Used (TB)	
Compatible PAV	Installed	Permanent	999	0.00	-
Data Retention Utility	Installed	Permanent	999	-	-
Volume Retention Manager	Installed	Permanent	999	-	-
Dynamic Provisioning	Installed	Permanent	999	1.62	-
Open Volume Management	Installed	Permanent	999	-	-
LUN Manager	Installed	Permanent	999	-	-
Performance Monitor	Installed	Permanent	999	-	-
Server Priority Manager	Installed	Permanent	999	-	-
Volume Migration	Installed	Permanent	999	-	-
ShadowImage	Installed	Permanent	999	0.00	-
⟆⟆					
Dynamic Tiering	Installed	Permanent	999	1.57	-
SMI-S Provider	Installed	Permanent	Unlimited	-	-
Dynamic Provisioning for Mainframe	Installed	Permanent	999	0.00	-
Resource Partition Manager	Installed	Permanent	999	-	-
Compatible Software for IBM(R) FlashC...	Installed	Permanent	999	0.00	-
Dynamic Tiering for Mainframe	Installed	Permanent	999	0.00	-
Thin Image	Installed	Permanent	999	0.05	-
nondisruptive migration	Installed	Permanent	999	-	-
global-active device	Installed	Permanent	999	0.00	-
active flash	Installed	Permanent	999	0.00	-
active flash for mainframe	Installed	Permanent	999	0.00	-
dedupe and compression	Installed	Permanent	Unlimited	-	-

Figure 3. License verification

4.1.2 Parity Group の設定

Production Systemとスナップショットデータを格納するParity Groupを用意します。Hitachi Storage Plug-in for Containersを利用するには、Dynamic Provisioning Pool (HDP Pool)構成が必要であるため、このParity Groupからpool VOL を作成します。

Before you begin

ストレージ管理者として StorageNavigator にログインします。

Procedure

1. [**Storage Systems**] > [**Parity Groups**]に移動し、pool VOL を作成します。

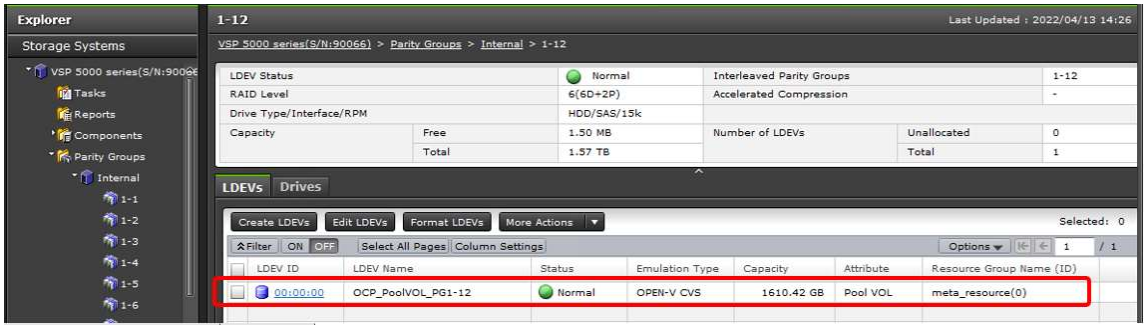

Figure 4. Configuring a Parity Group for storing snapshot image data

4.1.3　pool の作成

Hitachi Storage Plug-in for Containers を利用するには：

- pool は Dynamic Provisioning Pool (HDP Pool)として作成します。
- Production System とスナップショットデータは単一の pool で構成します。

Before you begin

ストレージ管理者として StorageNavigator にログインします。

Procedure

1. [**Storage Systems**] > [**Pools**]に移動し、[**Create Pools**]をクリックして Dynamic Provisioning pool を作成します。

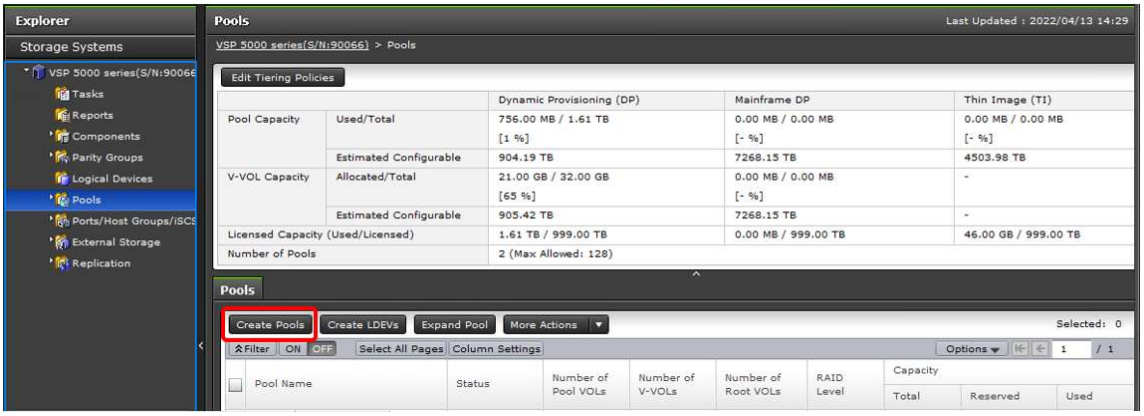

Figure 5. Creating a pool for storing snapshot images

2. 作成した poolVOL を使用して、Dynamic Provisioning pool を作成します。[**Pool Type**]で[**Dynamic Provisioning**]を、[**Multi-Tier Pool**]で[**Disable**]を選択します。

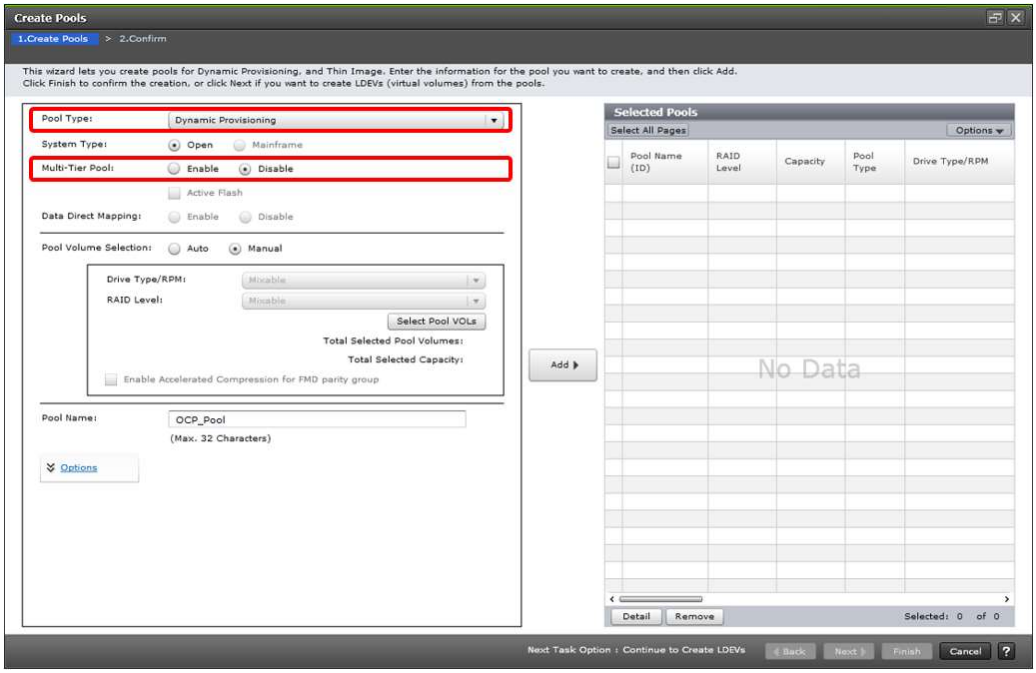

Figure 6. Selecting pool Type for the pool for storing snapshot images

3. Dynamic Provisioning pool の pool タイプが"DP"であることを確認し、pool VOL の正常性を確認します。

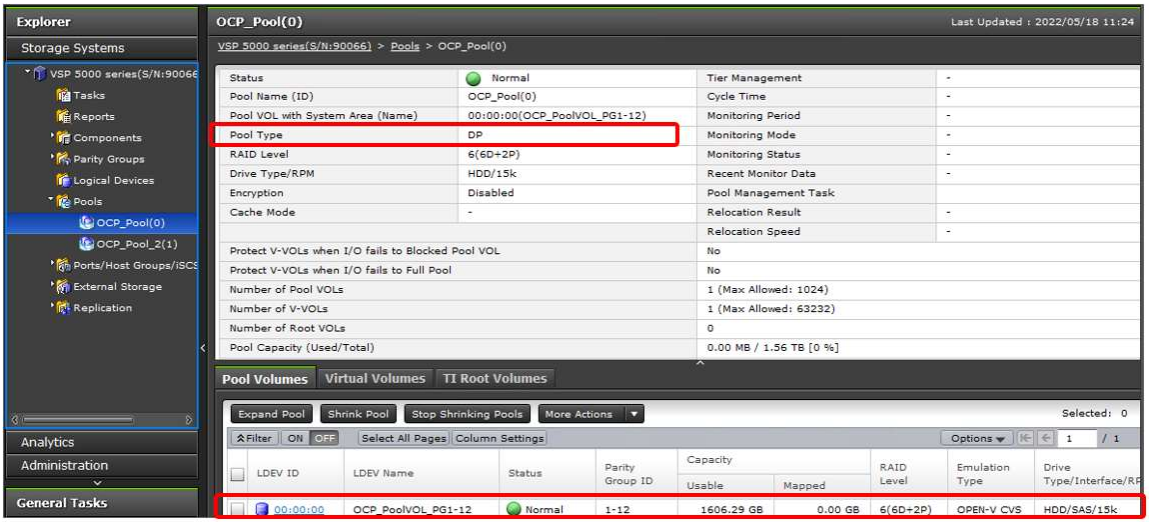

Figure 7. Verifying the pool for storing snapshot images

4.1.4 port の設定

ストレージシステムと server 間の接続インターフェイスとして Fibre Channel 接続を構成するため、ホストグループを作成します。Fibre Channel スイッチは、ストレージと server 間の通信に使用します。StorageNavigator を使用して、ストレージ port に次のパラメータを設定します。

- Port Security: Enable
- Fabric: ON

- Connection Type: P-to-P

Before you begin

ストレージ管理者として StorageNavigator にログインします。

Procedure

1. [**Storage Systems**] > [**Ports/Host Groups/iSCSI Targets**] > [**Ports**]に移動し、使用する port を選択して[**Edit Ports**]をクリックし port を編集します。

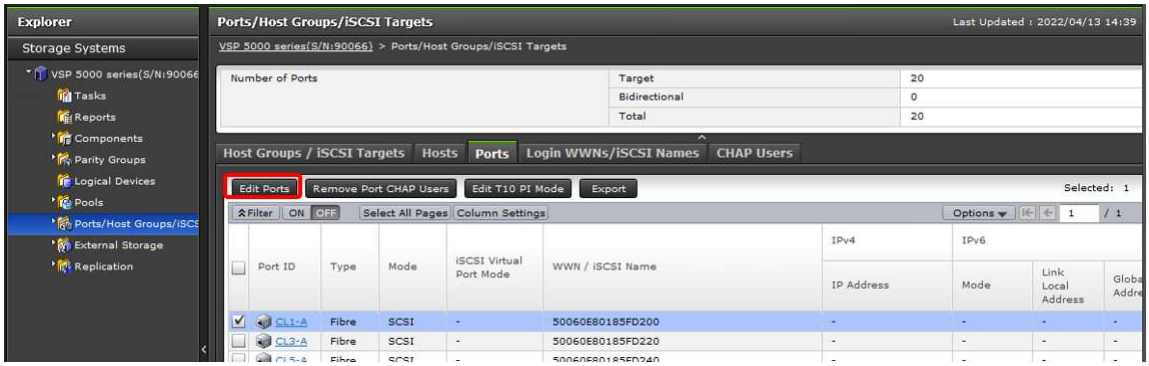

Figure 8. Configure ports and host groups

2. 使用する port に対して、port のプロパティを変更します。

- Port Security: Enable
- Fabric: ON
- Connection Type: P-to-P

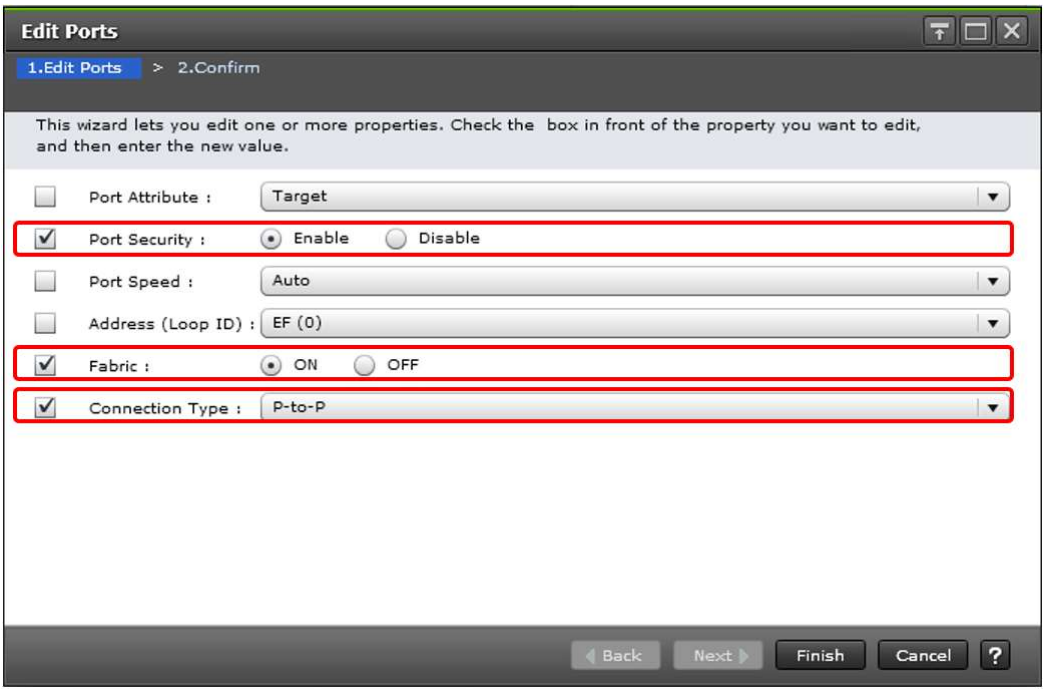

Figure 9. Selecting property for the port

3. 使用する port の Security が"**Enabled**"、Fabric が"**ON** "、Connection Type が"**P-to-P**"であることを確認します。

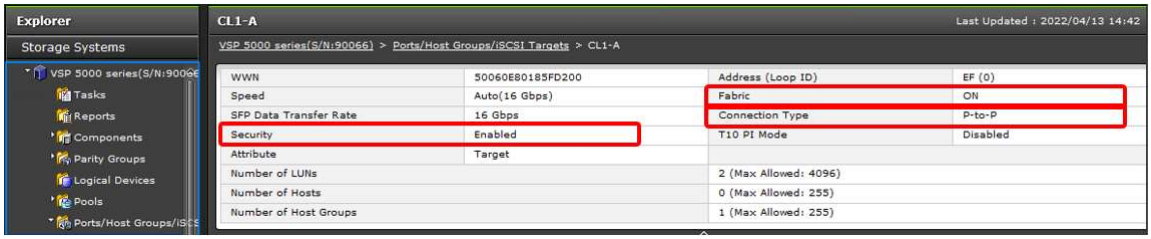

Figure 10. Verifying the port property

以上で Hitachi storage system の構成は終了です。

4.2 Hitachi Storage Plug-in for Containers のインストール

この章では、Hitachi Storage Plug-in for Containers を OpenShift 環境にインストールする方法について説明します。

Hitachi Storage Plug-in for Containers は、OpenShift 環境を操作する OpenShift web UI の OperatorHub から入手します。

4.2.1 Operator のインストール

Hitachi Storage Plug-in for Containers は、OperatorHub からインストールできる Operator を使用して OpenShift にデプロイします。

Before you begin

管理者ユーザーとして OpenShift web UI にログインします。

Procedure

1. [**Operators**] > [**OperatorHub**]に移動し、インストールする Operator を選択します。
   (a) [**All Items**]から"**Hitachi Storage Plug-in for Containers**"を検索します。
   (b) 検索結果に表示された[**Hitachi Storage Plug-in for Containers**]をクリックします。
   (c) Hitachi Storage Plug-in for Containers の情報が表示されるので、[**Install**]をクリックします。

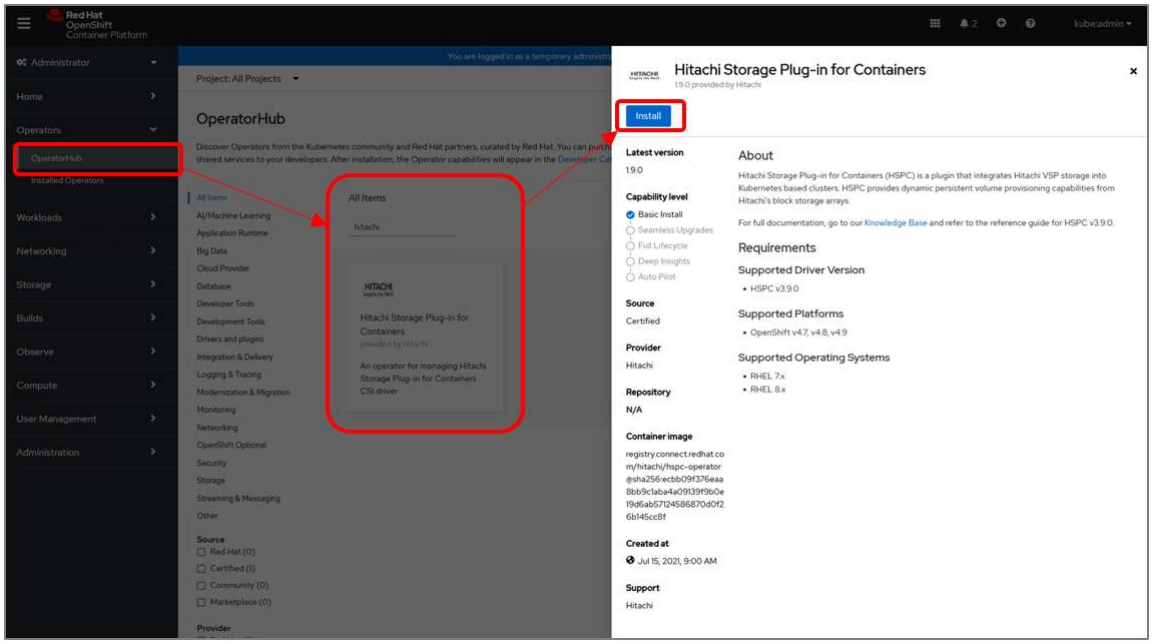

Figure 11. インストールする Operator の選択画面

2. Operator をインストールします。

(a) [**Install Operator**]画面が表示されるので、以下の設定を選択します。

- Installation mode : A specific namespace on the cluster
- Installed Namespace : Hitachi Storage Plug-in for Containers をインストールする namespace
- Update approval : Manual

(b) [**Install**]をクリックします。

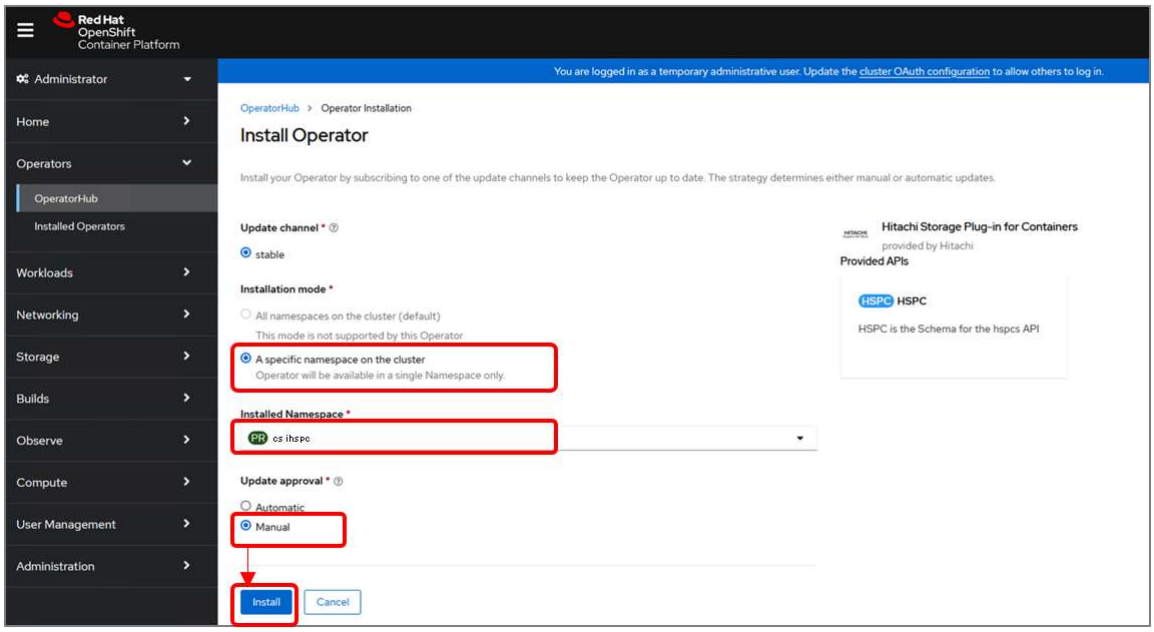

Figure 12. Operator のインストール画面での設定とインストールの実行画面

3. Operator のインストールが完了するまで待ちます。

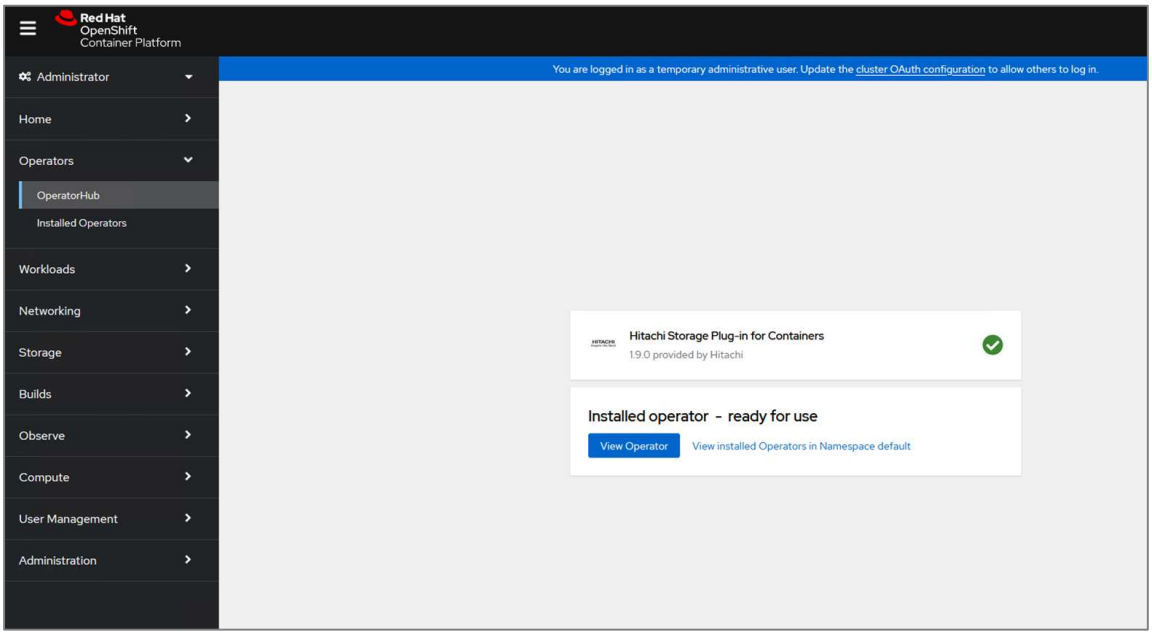

Figure 13. Operator インストールの完了画面

4. [**Operators**] > [**Installed Operators**]に移動し、Hitachi Storage Plug-in for Containers のステータスが "**Succeeded**"であることを確認します。

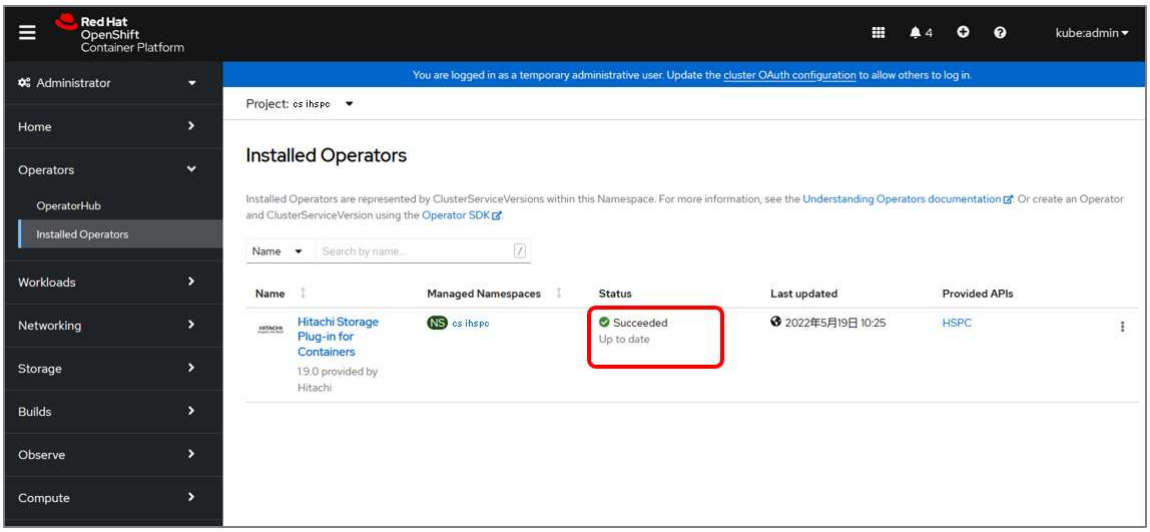

Figure 14. Operator ステータスの確認画面

5. [**Workloads**] > [**Pods**]に移動し、Hitachi Storage Plug-in for Containers の Operator Pod のステータスが "**Running**"であることを確認します。

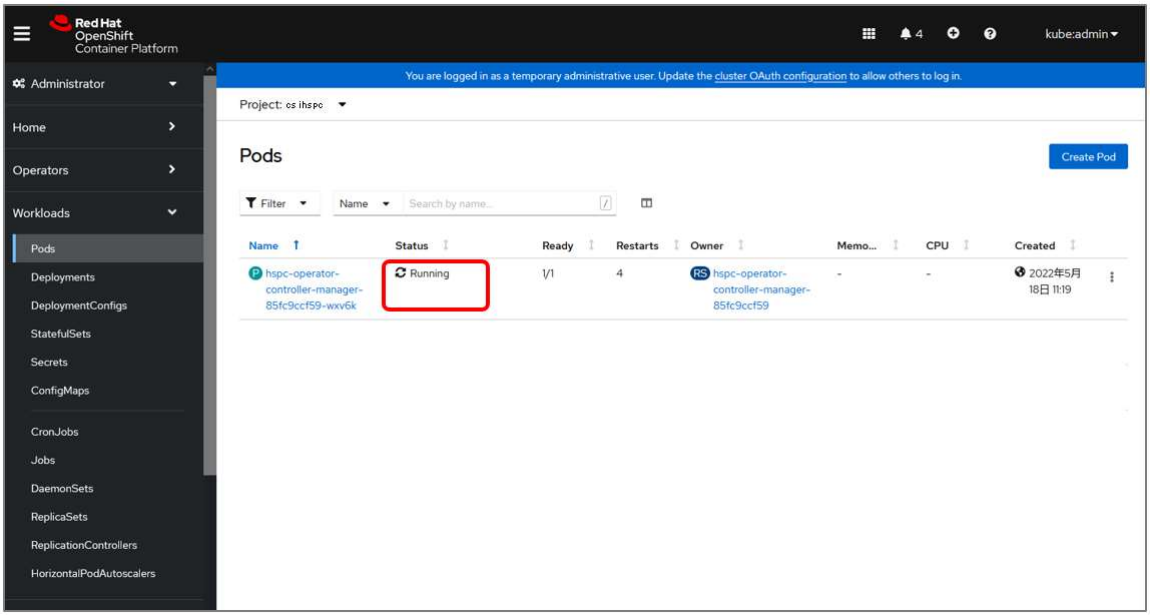

Figure 15. Operator Pod ステータスの確認画面

4.2.2 HSPC インスタンスの作成

Hitachi Storage Plug-in for Containers をインストールするには、次の手順に従ってください。

Before you begin

管理者ユーザーとして OpenShift web UI にログインします。

Procedure

1. インスタンスを作成します。

   (a) [**Operators**] > [**Installed Operators**]に移動し、Hitachi Storage Plug-in for Containers を選択します。

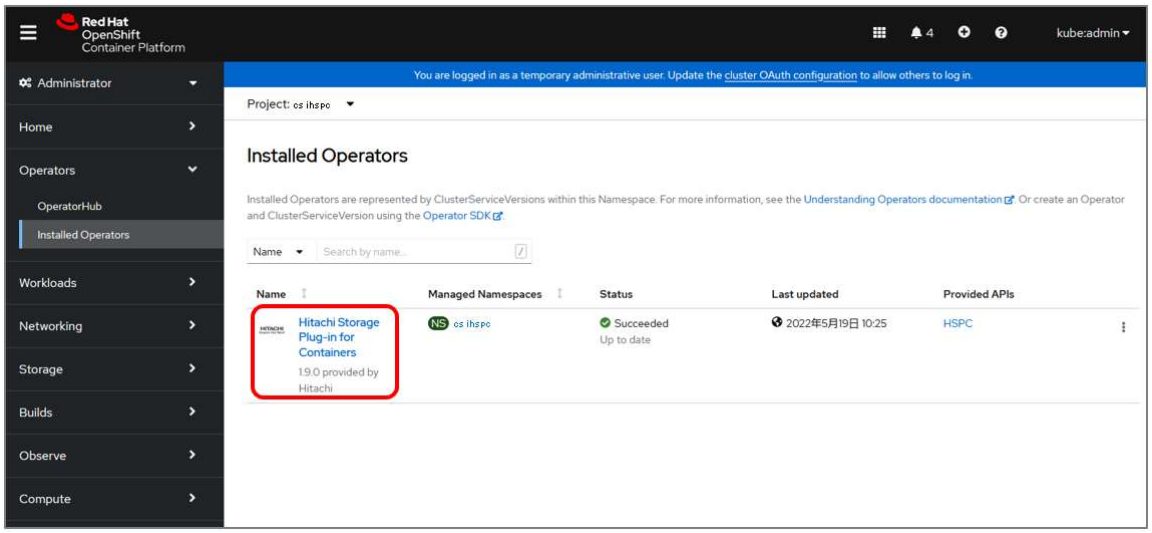

Figure 16. Installed Operator 画面

   (b) [**Operator details**]画面が表示されるので、[**Provided APIs**]の"HSPC"項目にある[**Create instance**]をクリックします。

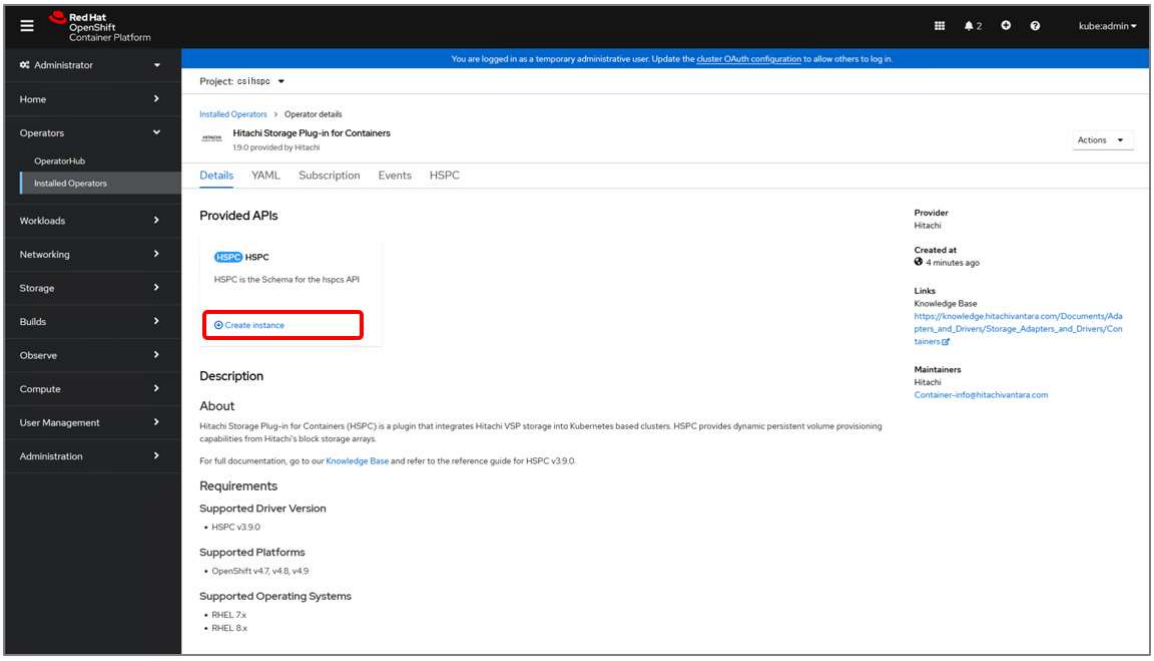

Figure 17. HSPC インスタンスの作成画面

(c) [**Create HSPC**]画面が表示されるので、任意の名前を入力します。

(d) [**Create**]をクリックします。

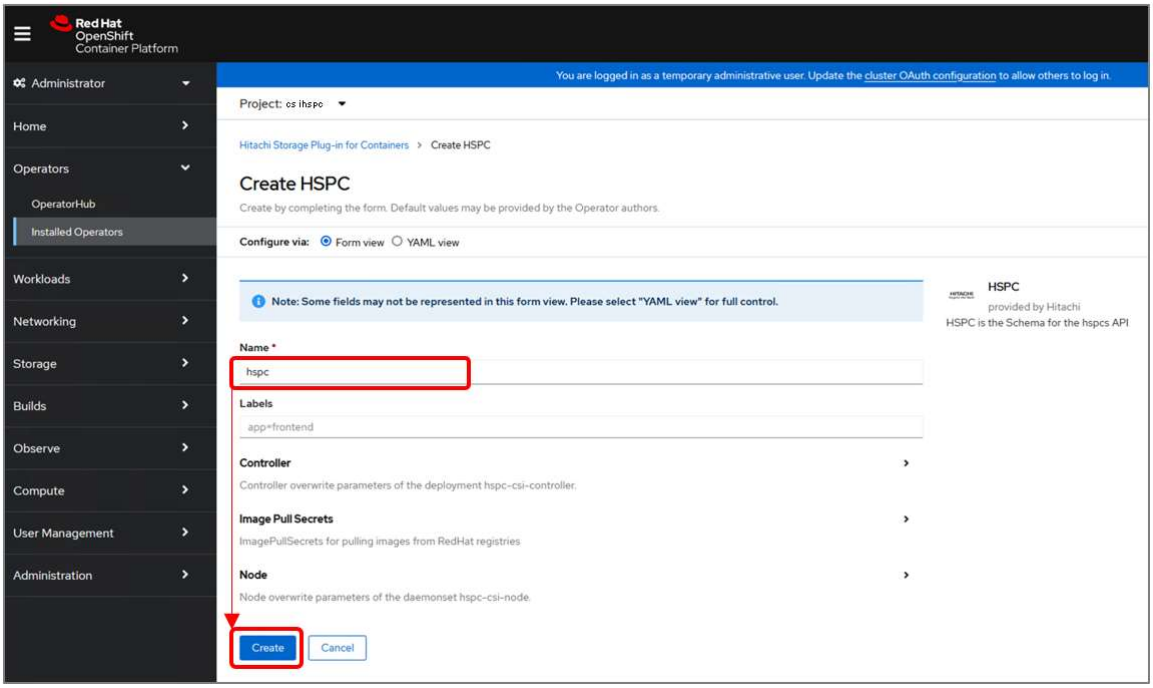

Figure 18. HSPC の作成画面

2. 次のコマンドを使用して、[READY]ステータス が "**true**" であることを確認します。

   [実行例] `# oc get hspc -n csihspc`

```
[root@registry-host ~]# oc get hspc -n csihspc
NAME   READY   AGE
hspc   true    21h
```

Figure 19. コマンド実行例

4.2.3 Secret の設定

Secret ファイルを作成し Secret を設定します。Secret ファイルには、Hitachi Storage Plug-in for Containers が動作するために必要なストレージの URL、ユーザー名、およびパスワード情報を記載します。

Before you begin

Red Hat OpenShift Container Platform の CLI である oc コマンドを実行できる作業用 server に、oc コマンドが実行できるユーザーでログインします。

Procedure

1. 以下のコマンドを使用しシークレット用のストレージ情報を生成します。

   (a) ストレージの URL を base64 でエンコードします。

   本コマンドの実行結果を後の手順で使用しますので、記録しておいてください。

   [実行例] `# echo -n "http://172.16.1.1" | base64`

   (b) ストレージ管理者ユーザー名を base64 でエンコードします。

   本コマンドの実行結果を後の手順で使用しますので、記録しておいてください。

   [実行例] `# echo -n "UserName" | base64`

   (c) ストレージのパスワードを base64 でエンコードします。

   本コマンドの実行結果を後の手順で使用しますので、記録しておいてください。

   [実行例] `# echo -n "Password" | base64`

2. Secret ファイルを作成します。手順 1 で生成されたストレージの URL、ユーザー名、およびパスワード情報を data の各パラメータに記載します。

   以下に Secret の yaml ファイル作成例を示します。ファイル名および metadata.name と metadata.namespace フィールドには任意の名称を入力してください。

```
[root@registry-host HSPC_hitstorage_FC]# cat secret-hitstorage.yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-hitstorage
  namespace: csihspc
type: Opaque

data:
  url: aHROcHM6Ly8xOTIuMTY4LjIxMC4xODg=    ← (a) Storage URL
  user: bWFpbnRlbmFuY2U=                   ← (b) Storage username
  password: cmFpZC1tYWludGVuYW5jZQ==        ← (c) Storage password
[root@registry-host HSPC_hitstorage_FC]#
```

Figure 20. Secret ファイル作成例

3. 以下のコマンドを使用し Secret を作成します。

[実行例] `# oc create -f secret-hitstorage.yaml`

```
[root@registry-host HSPC_hitstorage_FC]# oc create -f secret-hitstorage.yaml
secret/secret-hitstorage created
[root@registry-host HSPC_hitstorage_FC]#
```

Figure 21. Secret 作成例

4.2.4 StorageClass の設定

StorageClass ファイルを作成し StorageClass を設定します。StorageClass ファイルには、Hitachi Storage Plug-in for Containers が Openshift 環境と連携するために必要なストレージ設定情報を記載します。

Before you begin

Red Hat OpenShift Container Platform の CLI である oc コマンドを実行できる作業用 server に、oc コマンドが実行できるユーザーでログインします。

Procedure

1. StorageClass ファイルを作成します。以下のストレージ設定情報を各パラメータに記載します。

    (a) Storage serial number

    (b) HDP pool ID

    (c) Port ID

    (d) Filesystem type. ext4 and xfs are supported. If blank, ext4 is set.

    (e) Secret name

    (f) Secret namespace

    以下に StorageClass の yaml ファイル作成例を示します。ファイル名および metadata.name フィールドには任意の名称を入力してください。

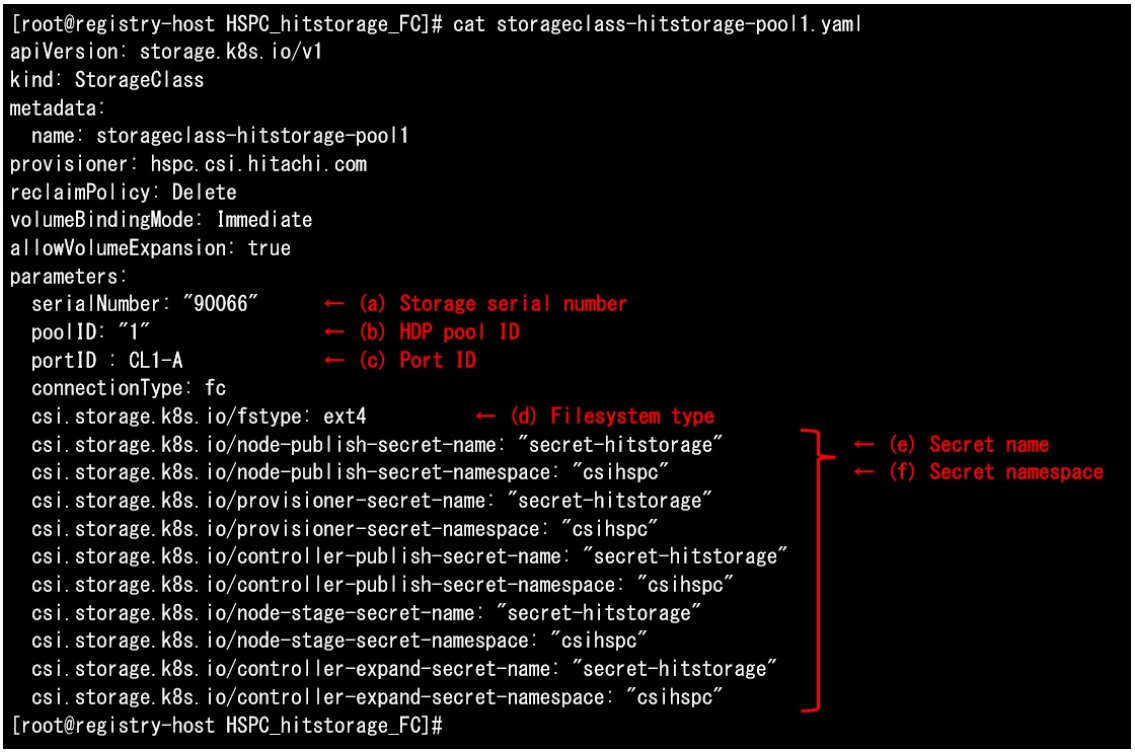

Figure 22. StorageClass ファイル作成例

2. 以下のコマンドを使用し StorageClass を作成します。

[実行例] `# oc create -f storageclass-hitstorage-pool1.yaml`

```
[root@registry-host HSPC_hitstorage_FC]# oc create -f storageclass-hitstorage-pool1.yaml
storageclass.storage.k8s.io/ storageclass-hitstorage-pool1 created
[root@registry-host HSPC_hitstorage_FC]#
```

Figure 23. StorageClass 作成例

以上で Hitachi Storage Plug-in for Containers のインストールは終了です。

4.3 NetBackup によるバックアップの準備

4.3.1 Kubernetes クラスタの追加

Before you begin

Red Hat OpenShift Container Platform に NetBackup Kubernetes Operator および NetBackup Kubernetes datamover のインストールが完了している必要があります。

Red Hat OpenShift Container Platform の CLI である oc コマンドを実行できる作業用 server に、oc コマンドが実行できるユーザーでログインします。

NetBackup web UI にログインします。

Procedure

1. 次のコマンドを作業用 server で実行し「netbackup-backup-server」サービスアカウントの詳細を確認し、使用している token の secret を確認します。

   [実行例] `# oc get serviceaccount netbackup-backup-server -o yaml`

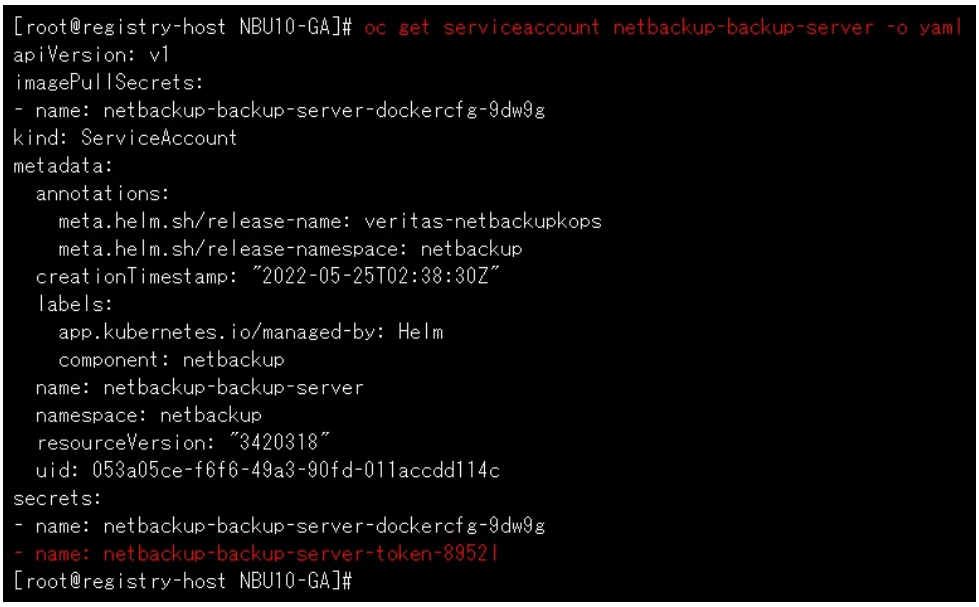

Figure 24. サービスアカウント「netbackup-backup-server」の詳細確認画面

2. 手順 1 で確認した secret 名を指定して次のコマンドを作業用 server で実行し、Secret の詳細出力から CA certificate(ca.crt)と token(token)の値をコピーします。

   [実行例] `# oc get secret netbackup-backup-server-token-89521 -o yaml`

```
[root@registry-host NBU10-GA]# oc get secret netbackup-backup-server-token-8952l -o yaml
apiVersion: v1
data:
  ca.crt: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURNakNDQWhxZ0F3SUJBZ0lJYzIzTnoydlRqR293RFFZSktvWklodmNOQ
  namespace: bmV0YmFja3Vw
  service-ca.crt: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURNakNDQWhxZ0F3SUJBZ0lJYzIzTnoydlRqR293RFFZSktvW
  token: ZXlKaGJHY2lPaUpTVXpJMU5pSXNJbXRwWkNJNklqZDRRV3RKWVRkaVMyMUVNV2QwYkVwSk9VOTFVMDR5Y2todFprbzVSbkpYTU
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: netbackup-backup-server
    kubernetes.io/service-account.uid: 053a05ce-f6f6-49a3-90fd-011accdd114c
  creationTimestamp: "2022-05-25T02:38:30Z"
  name: netbackup-backup-server-token-8952l
  namespace: netbackup
  resourceVersion: "3420290"
  uid: 8ec67938-5621-45cc-a412-ed77ac9368b3
type: kubernetes.io/service-account-token
[root@registry-host NBU10-GA]#
```

Figure25. Secret の詳細画面

3. NetBackup web UI から、Kubernetes クラスタのクレデンシャルを登録します。

   [**Credential management**] の[**Named credentials**]タブで、[**Add**]をクリックします。

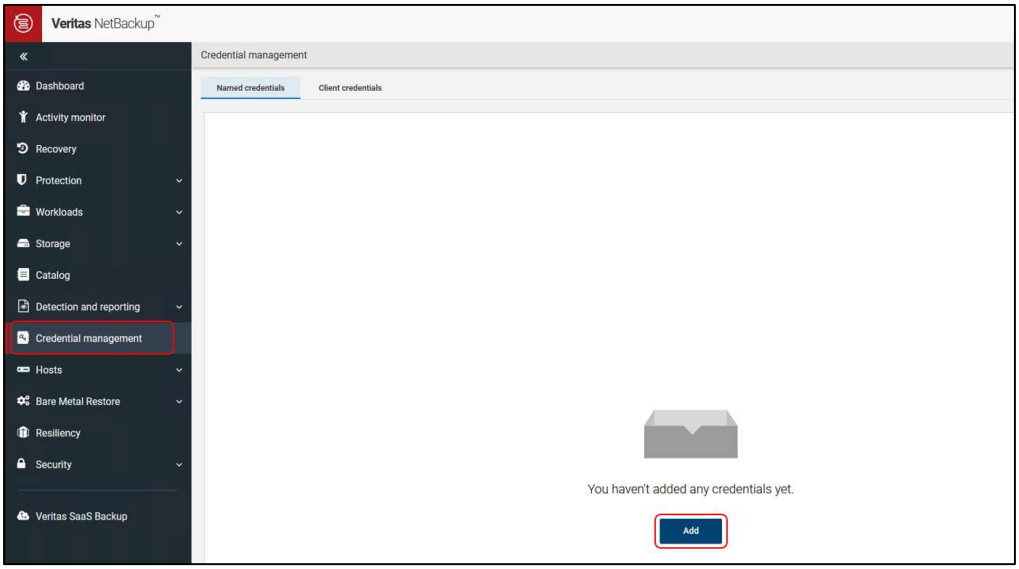

Figure 26. Credential management 画面

4. [**Credential name**]フィールドにクレデンシャル名を入力し、[**Next**]をクリックします。

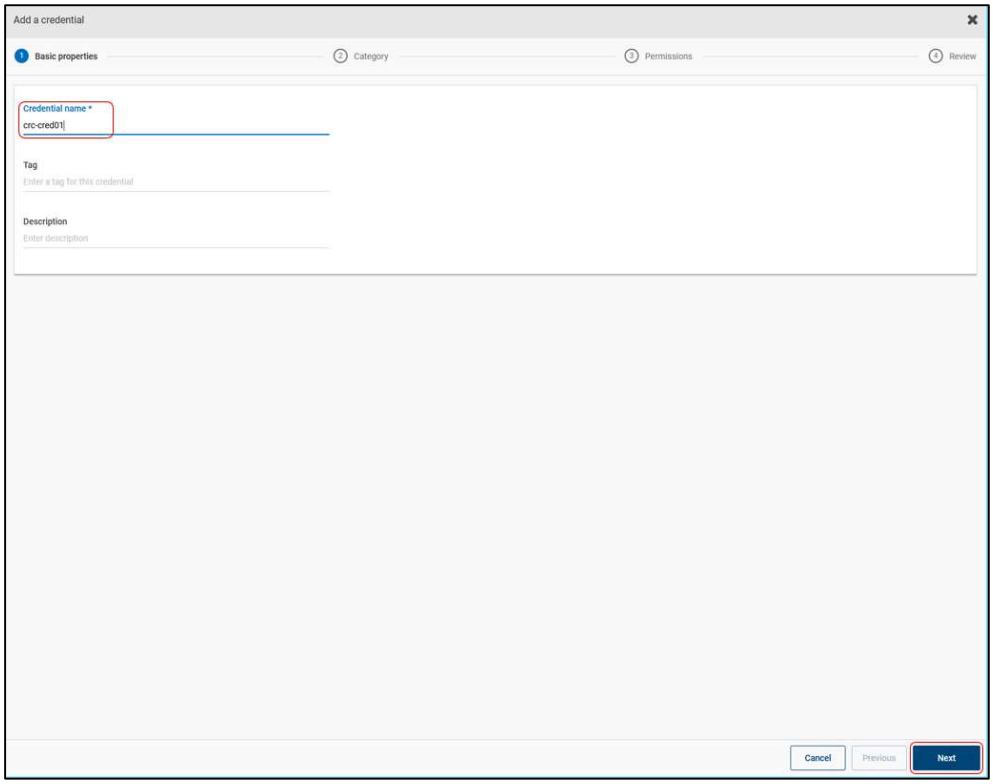

Figure 27. クレデンシャル追加の Basic properties 画面

5. [**Category**]で[**Kubernetes**]を選択し、手順 2 でコピーした token と CA certificate を入力し、[**Next**]をクリックします。

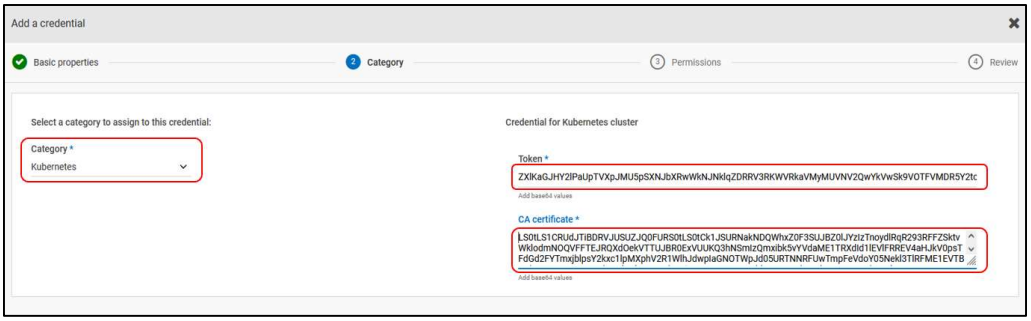

Figure 28. クレデンシャル追加の Basic properties 画面

6. [**Permission**]で必要に応じてロールを選択し、[**Next**]をクリックします。

7. 確認画面で[**Finish**]をクリックします。

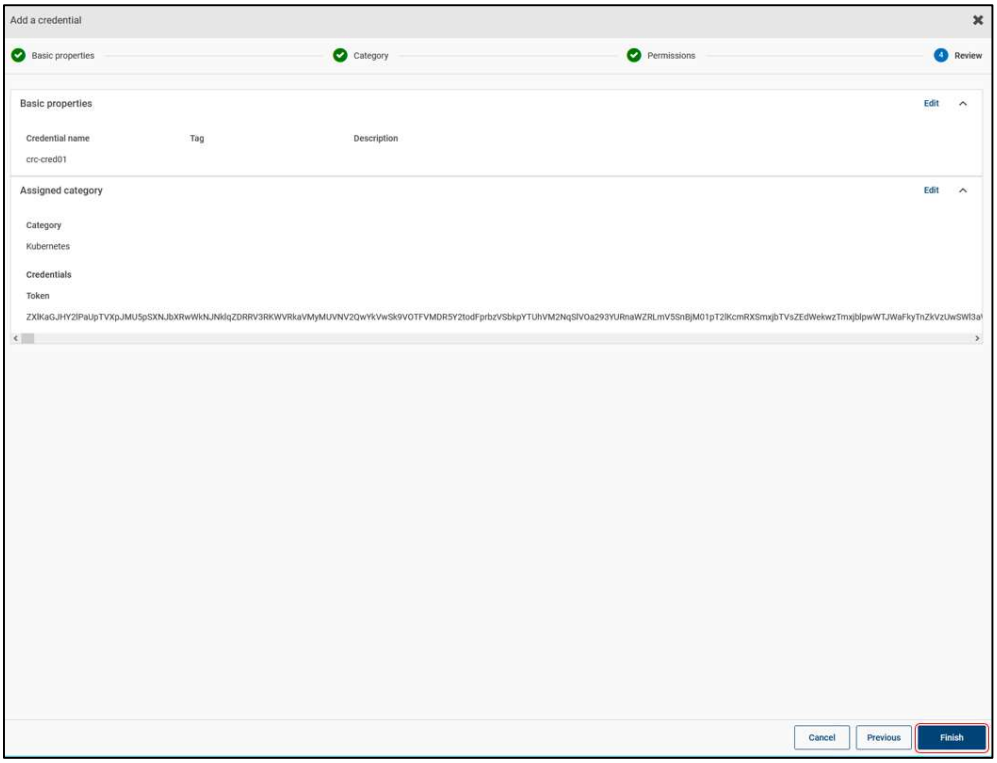

Figure 29. クレデンシャル追加の確認画面

8. クレデンシャルが追加されることを確認します。

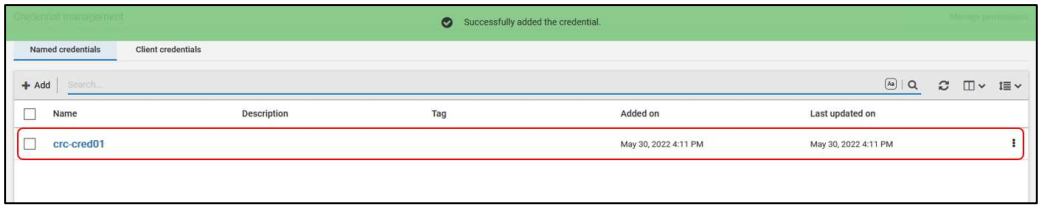

Figure 30. 追加されたクレデンシャル

9. [**Workloads**] > [**Kubernetes**]で[**Kubernetes clusters**]タブを開き、[**+Add**]をクリックして Kubernetes クラスタを追加します。

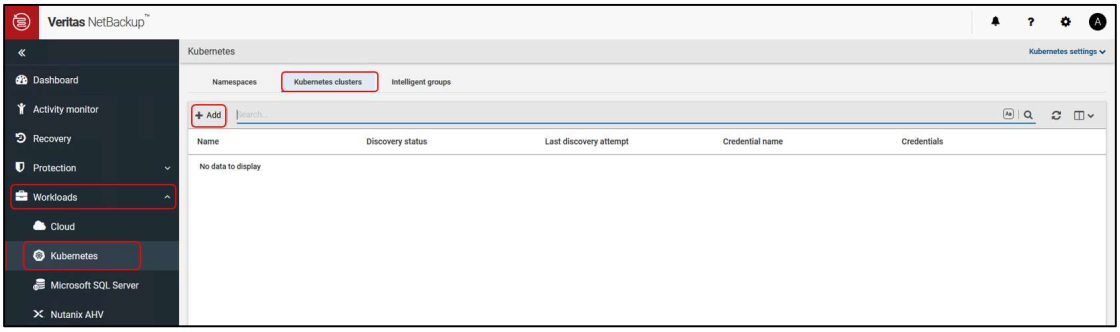

Figure 31. Kubernetes クラスタ画面

10. [**Cluster name**]と[**Controller namespace**]を入力して、[**Next**]をクリックします。

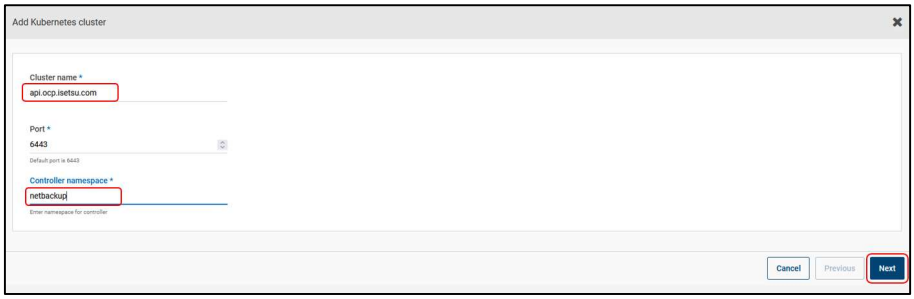

Figure 32. Kubernetes クラスタ追加画面

11. [**Select from existing credentials**]が選択されている状態で[**Next**]をクリックします。

Figure 33. Manage credentials ページ　クレデンシャル追加方法選択画面

12. 手順 8 で追加したクレデンシャルを選択し、[**Next**]をクリックします。

Figure 34. Manage credentials ページ　クレデンシャル選択画面

13. [**Validating credentials**]と表示されることを確認し、[**Close**]をクリックします。

Figure 35. Manage credentials ページ　最終画面

14. [**Workloads**] > [**Kubernetes**]の[**Kubernetes clusters**]タブのクラスター一覧に表示され、[**Discovery status**]が"**Success**"になっていることを確認します。

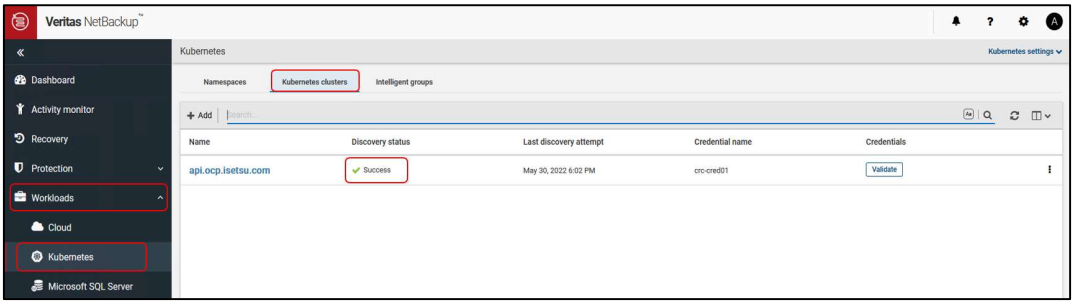

Figure 36. Kubernetes クラスタ追加成功確認画面 (Kubernetes クラスタ画面)

15. [**Workloads**] > [**Kubernetes**]の[**Namespaces**]タブで、クラスタの Namespace が検出されていることを確認します。

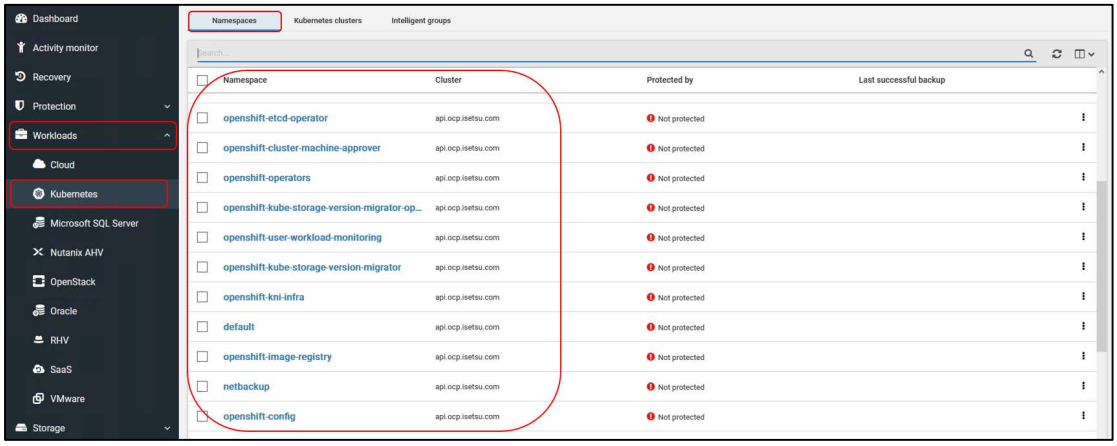

Figure 37. Kubernetes クラスタ追加成功確認画面 (Namespace 画面)

NetBackup に Kubernetes クラスタを追加する手順は以上です。

4.3.2　スナップショット操作のための構成設定

NetBackup のスナップショット操作を実行するため次の構成設定を行います。

VolumeSnapshotClass の作成およびラベルを追加する手順を以下に示します。

Before you begin

Red Hat OpenShift Container Platform の CLI である oc コマンドを実行できる作業用 server に、oc コマンドが実行できるユーザーでログインします。

Procedure

1. VolumeSnapshotClass ファイルを作成します。StorageClass で設定した内容と同一になるよう以下のストレージ情報を各パラメータに設定します。

    (a) HDP pool ID

(b) Secret name

(c) Secret namespace

以下に VolumeSnapshotClass の yaml ファイル作成例を示します。ファイル名および metadata.name フィールドには任意の名称を入力してください。

```
[root@registry-host NBU10-GA]# cat volumesnapshotclass-hitstorage.yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: snapclass-hitstorage
driver: hspc.csi.hitachi.com
deletionPolicy: Delete
parameters:
  poolID: "1"                ← (a) HDP pool ID
  csi.storage.k8s.io/snapshotter-secret-name: "secret-hitstorage"    ← (b) Snapshotter Secret name
  csi.storage.k8s.io/snapshotter-secret-namespace: "csihspc"         ← (c) Snapshotter Secret namespace
[root@registry-host NBU10-GA]#
```

Figure 38. VolumeSnapshotClass yaml ファイル作成例

2. 以下のコマンドを使用し VolumeSnapshotClass を作成します。

[実行例] `# oc create -f volumesnapshotclass-hitstorage.yaml`

```
[root@registry-host NBU10-GA]# oc create -f volumesnapshotclass-hitstorage.yaml
volumesnapshotclass.snapshot.storage.k8s.io/snapclass-hitstorage created
[root@registry-host NBU10-GA]#
```

Figure 39. VolumeSnapshotClass 作成例

3. 以下のコマンドを使用し VolumeSnapshotClass が作成されたことを確認します。

[実行例] `# oc get volumesnapshotclass`

```
[root@registry-host NBU10-GA]# oc get volumesnapshotclass
NAME                  DRIVER                DELETIONPOLICY   AGE
snapclass-hitstorage  hspc.csi.hitachi.com  Delete           6s
[root@registry-host NBU10-GA]#
```

Figure 40. VolumeSnapshotClass 確認例

スナップショット操作のための構成設定は以上です。

4.3.3 バックアップおよびリストア操作のための構成設定

スナップショットからのバックアップとバックアップからのリストア操作を実行するためには次の設定を行います。

- StorageClass および VolumeSnapshotClass にラベルを追加する
- Secret、ConfigMap および BackupServerCert を作成する

StorageClass および VolumeSnapshotClass にラベルを追加する

StorageClass および VolumeSnapshotClass へのラベルを追加する手順を以下に示します。

Before you begin

４章の StorageClass の設定 が完了し、StorageClass が作成できていること。

管理者ユーザーとして OpenShift web UI にログインします。

Procedure

1. OpenShift web UI で[**Storage**] > [**StorageClasses**]を開き、対象の StorageClass に対して[**Labels**]の[**Edit**]をクリックします。

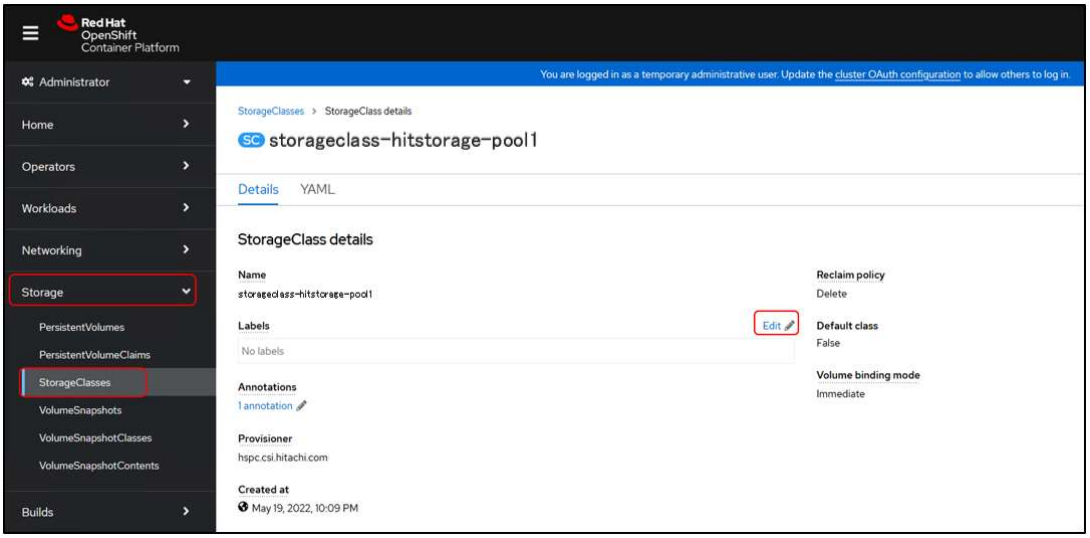

Figure 41. StorageClass 編集画面

2. ラベル編集画面で、以下のラベルを入力し[**Save**]をクリックします。

   netbackup.veritas.com/default-csi-storage-class=true

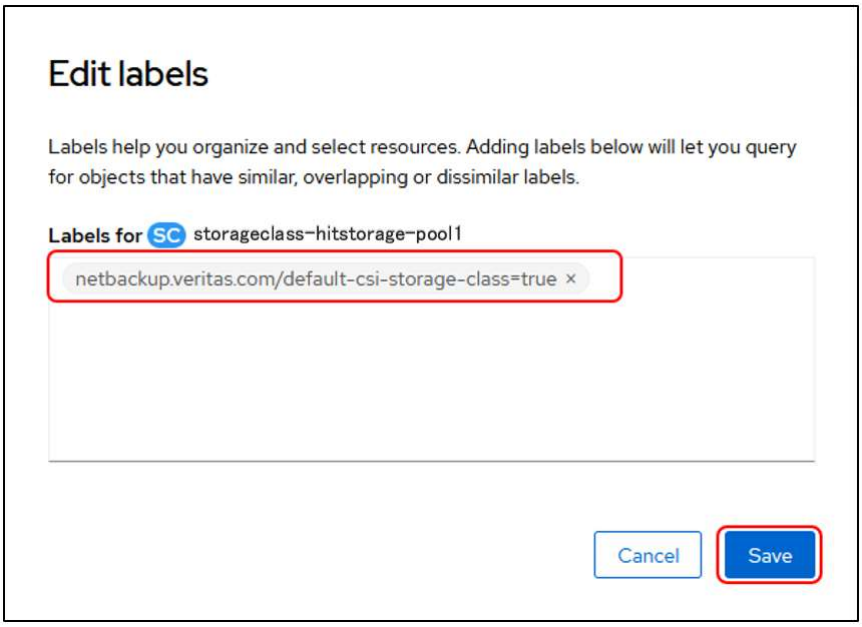

Figure 42. StorageClass のラベル編集画面

3. StorageClass にラベルが設定されていることを確認します。

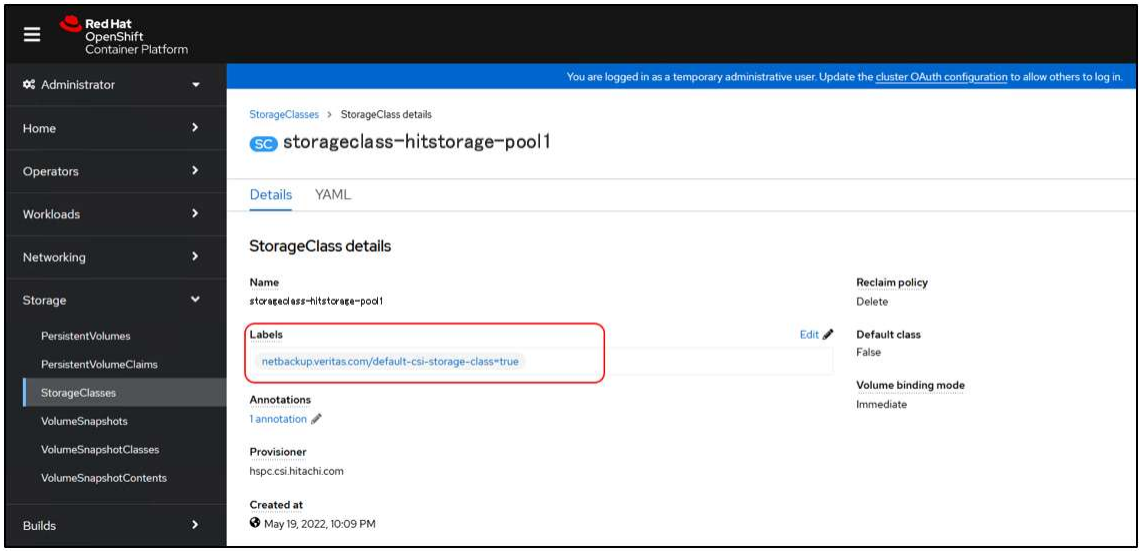

Figure 43. ラベルが設定された StorageClass の画面

4. [**Storage**] > [**VolumeSnapshotClasses**]を開き、対象の VolumeSnapshotClass に対して[**Labels**]の[**Edit**]をクリックします。

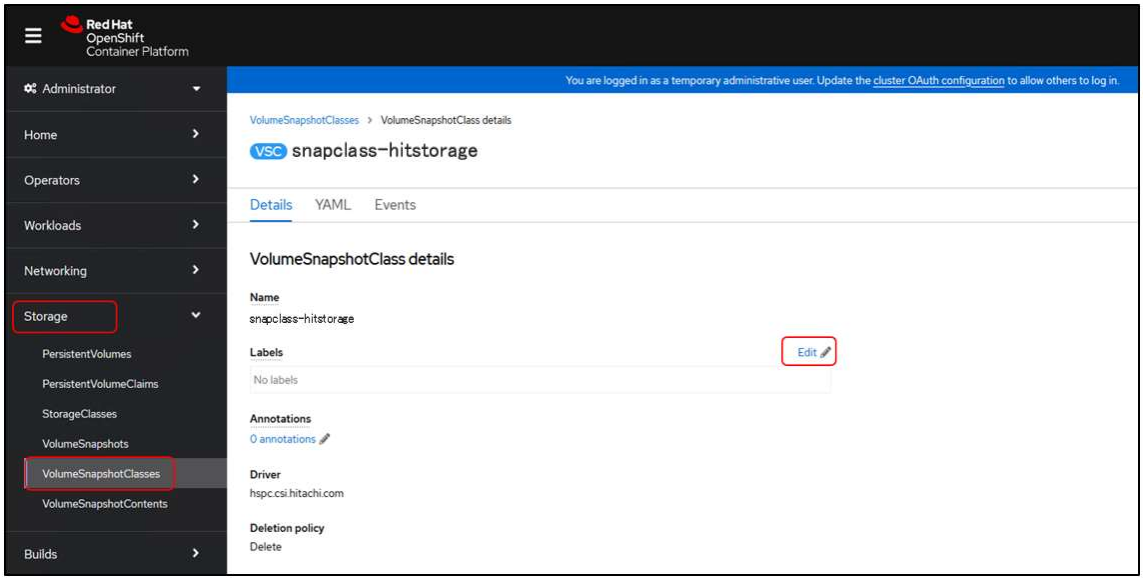

Figure 44. VolumeSnapshotClass 編集画面

5. ラベル編集画面で、以下のラベルを入力し[**Save**]をクリックします。

netbackup.veritas.com/default-csi-volume-snapshot-class=true

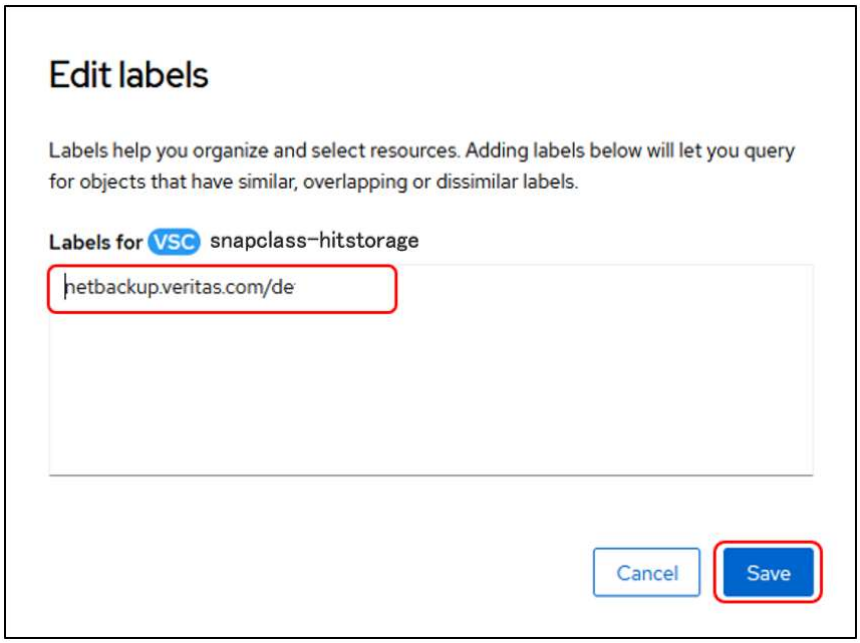

Figure 45. VolumeSnapshotClass のラベル編集画面

4. VolumeSnapshotClass にラベルが設定されていることを確認します。

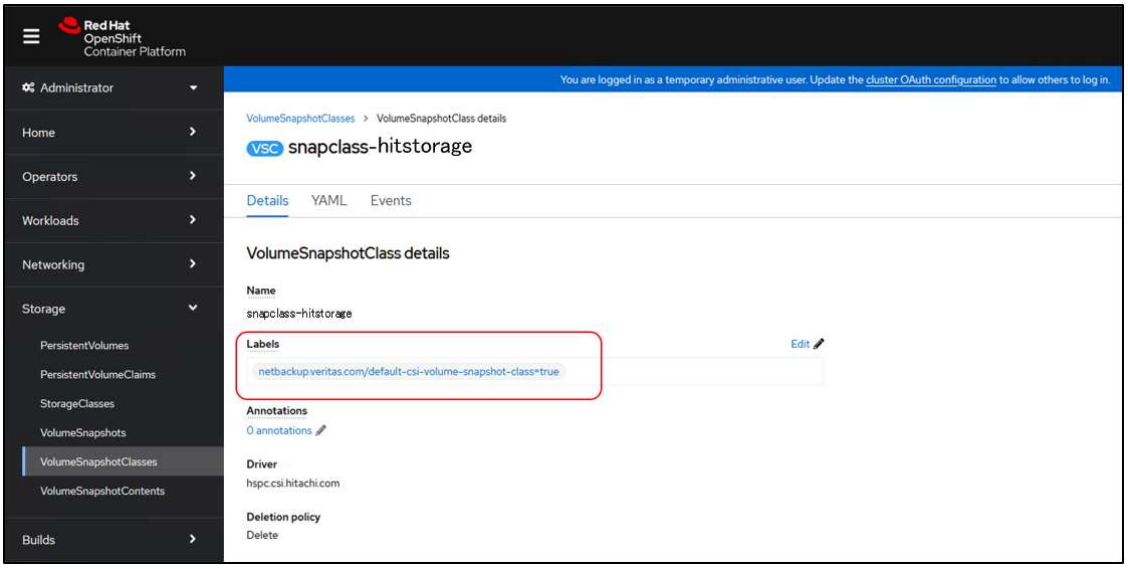

Figure 46. ラベルが設定された VolumeSnapshotClass の画面

Secret、ConfigMap および BackupServerCert を作成する

次に、Secret、ConfigMap および BackupServerCert の 3 つの yaml ファイルを作成し適用します。
手順を以下に示します。

Before you begin

Red Hat OpenShift Container Platform の CLI である oc コマンドを実行できる作業用 server に、oc コマンドが実行できるユーザーでログインします。

NetBackup web UI にログインします。

Procedure

1. 証明書 token とフィンガープリントを取得し、Secret ファイルを作成します。

   (a) 証明書 token を取得します。

   NetBackup Administration Console の[**Security**] > [**Tokens**]画面で token を選択し、[**Show Token**]をクリックします。

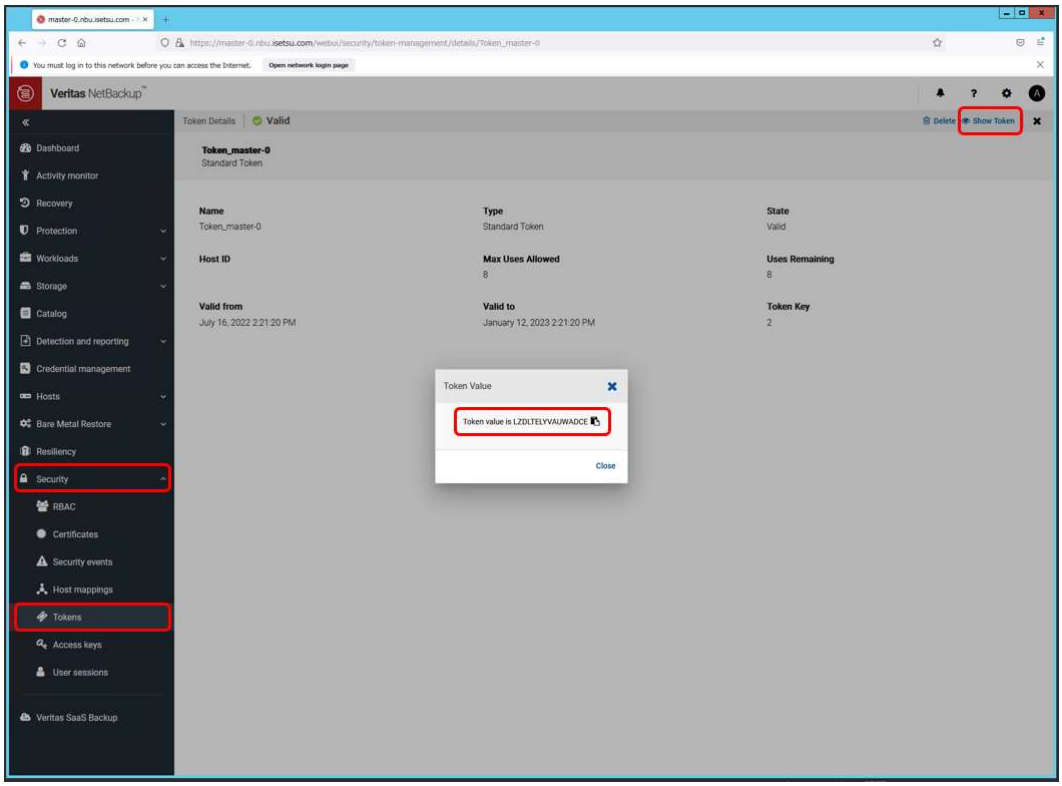

Figure 47. Token 表示画面

(b) NetBackup Master Server で次のコマンドを実行し、"**NBCA モード**"になっていることを確認します。

[実行例] # *install_path*\NetBackup\bin\nbcertcmd -getSecConfig -caUsage

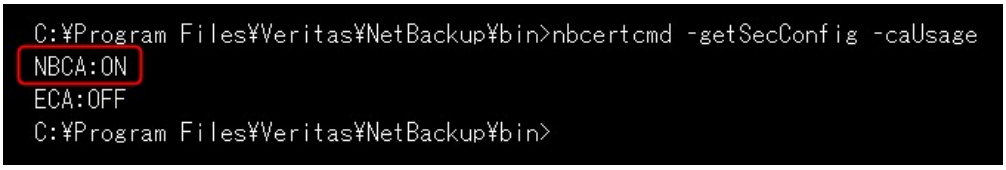

Figure 48. 指定されている認証局の確認画面

(c) フィンガープリントを取得します。

NetBackup Master Server で次のコマンドを実行し、フィンガープリントを取得します。

[実行例] # *install_path*\NetBackup\bin\nbcertcmd -listCACertDetails

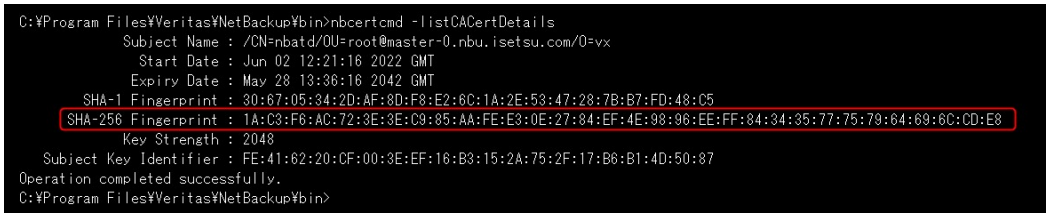

Figure 49. SHA-256 フィンガープリント取得例

(d) Secret ファイルを作業用 server で作成します。以下の設定情報を各パラメータに記載します。

I. Secret name

II. Namespace

III. Token (Issued in the previous step)

IV. SHA-256 fingerprint (Issued in the previous step)

以下に Secret の yaml ファイル作成例を示します。ファイル名には任意の名称を入力してください。

```
[root@registry-host NBU10-GA]# cat NBU_Secret.yaml
apiVersion: v1
kind: Secret
metadata:
        name: master-0.nbu.isetsu.com          ←(Ⅰ) Secret name
        namespace: netbackup                   ←(Ⅱ) Namespace of the NetBackup operator
type: Opaque
stringData:
        token: DREJDCZTRRGZEGPA                ←(Ⅲ) Token issued in the previous step
        fingerprint: 1A:C3:F6:AC:72:3E:3E:C9:85:AA:FE:E3:0E:27:84:EF:4E:98:96:EE:FF:84:34:35:77:75:79:64:69:6C:CD:E8
[root@registry-host NBU10-GA]#                                                  ↑
                                                                                (Ⅳ) SHA-256 fingerprint of the primary server
```

Figure 50. Secret ファイル設定例

2. 作業用 server で以下のコマンドを使用し Secret を適用します。

[実行例] # `oc apply -f NBU_Secret.yaml`

```
[root@registry-host NBU10-GA]# oc apply -f NBU_Secret.yaml
secret/master-0.nbu.isetsu.com created
[root@registry-host NBU10-GA]#
```

Figure 51. Secret 作成例

3. 作業用 server で以下のコマンドを使用し Secret が作成されたことを確認します。

[実行例] `# oc get secret`

```
[root@registry-host NBU10-GA]# oc get secret
NAME                                    TYPE                                  DATA   AGE
builder-dockercfg-r7t86                 kubernetes.io/dockercfg               1      22m
builder-token-hs4c5                     kubernetes.io/service-account-token   4      22m
builder-token-smm6x                     kubernetes.io/service-account-token   4      22m
default-dockercfg-8jqzr                 kubernetes.io/dockercfg               1      22m
default-token-kvpwd                     kubernetes.io/service-account-token   4      22m
default-token-x7p7v                     kubernetes.io/service-account-token   4      22m
deployer-dockercfg-6fdv8                kubernetes.io/dockercfg               1      22m
deployer-token-f6l5j                    kubernetes.io/service-account-token   4      22m
deployer-token-vgpxn                    kubernetes.io/service-account-token   4      22m
netbackup-backup-server-dockercfg-276zv kubernetes.io/dockercfg               1      19m
netbackup-backup-server-token-7zscn     kubernetes.io/service-account-token   4      19m
netbackup-backup-server-token-hcqh4     kubernetes.io/service-account-token   4      19m
netbackup-operator-dockercfg-nqmzz      kubernetes.io/dockercfg               1      19m
netbackup-operator-token-25rlk          kubernetes.io/service-account-token   4      19m
netbackup-operator-token-ttnvf          kubernetes.io/service-account-token   4      19m
master-0.nbu.isetsu.com                 Opaque                                2      8s
sh.helm.release.v1.veritas-netbackupkops.v1 helm.sh/release.v1                1      19m
[root@registry-host NBU10-GA]#
```

Figure 52. Secret 確認例

4. 作業用 server で NetBackup Kubernetes datamover のイメージを配置している場所を指定した ConfigMap ファイルを作成します。以下の設定情報を各パラメータに記載します。

   (a) NetBackup Master Server のホスト名

   (b) NetBackup Kubernetes Operator の namespace

   (c) NetBackup Kubernetes datamover のイメージを配置している場所を指定

以下に ConfigMap の yaml ファイル作成例を示します。ファイル名には任意の名称を入力してください。

```
[root@registry-host NBU10-GA]# ll NBU_ConfigMap.yaml
-rw-r--r-- 1 root root 217  5月 31 15:13 NBU_ConfigMap.yaml
[root@registry-host NBU10-GA]#
[root@registry-host NBU10-GA]# cat NBU_ConfigMap.yaml
apiVersion: v1
kind: ConfigMap
metadata:
        name: master-0.nbu.isetsu.com              ← (a) Host name of the NetBackup Master Server
        namespace: netbackup                       ← (b) Namespace of the NetBackup operator
data:
        version: "1"
        datamover.properties: "image=registry-host.isetsu.com:443/datamover:10.0"  ← (c) datamover image
[root@registry-host NBU10-GA]#
```

Figure 53. ComfigMap のファイル作成例

5. 作業用 server で以下のコマンドを使用し ConfigMap を適用します。

   [実行例] # `oc create -f NBU_ConfigMap.yaml`

```
[root@registry-host NBU10-GA]#
[root@registry-host NBU10-GA]# oc apply -f NBU_ConfigMap.yaml
configmap/master-0.nbu.isetsu.com created
[root@registry-host NBU10-GA]#
```

Figure 54. ConfigMap 作成例

6. 作業用 server で以下のコマンドを使用し ConfigMap が作成されたことを確認します。

   [実行例] # `oc get configmap`

```
[root@registry-host NBU10-GA]# oc get configmap
NAME                                    DATA   AGE
kube-root-ca.crt                        1      22m
master-0.nbu.isetsu.com                 2      18s
netbackup-backup-operator-configuration 15     20m
netbackup-certconfigscript              1      20m
openshift-service-ca.crt                1      22m
[root@registry-host NBU10-GA]#
```

Figure 55. ConfigMap 確認例

7. 作業用 server で BackupServerCert ファイルを作成します。以下の設定情報を各パラメータに記載します。

   I. BackupServerCert 名

   II. NetBackup Kubernetes Operator の namespace

   III. OpenShift のクラスタ名、ドメイン名

   IV. Host name of NetBackup Master Server のホスト名

   V. 証明書 token とフィンガープリントを含んだ Secret 名

   以下に BackupServerCert の yaml ファイル作成例を示します。ファイル名には任意の名称を入力してください。

```
[root@registry-host NBU10-GA]# cat NBU_BackupServerCert.yaml
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
        name: master-0.nbu.isetsu.com                ←(Ⅰ) BackupServerCert name
        namespace: netbackup                         ←(Ⅱ) Namespace of the NetBackup operator
spec:
        clusterName: api.ocp.isetsu.com              ←(Ⅲ) Cluster name or Domain name of the OpenShift
        backupServer: master-0.nbu.isetsu.com        ←(Ⅳ) Host name of the NetBackup Master Server
        certificateOperation: Create
        certificateType: NBCA
        nbcaAttributes:
                nbcaCreateOptions:
                        secretName: master-0.nbu.isetsu.com    ←(Ⅴ) Name of secret containing token and fingerprint
[root@registry-host NBU10-GA]#
```

Figure 56. BackupServerCert ファイル設定例

8. 作業用 server で以下のコマンドを使用し BackupServerCert を適用します。

   [実行例] `# oc apply -f NBU_BackupServerCert.yaml`

```
[root@registry-host NBU10-GA]# oc apply -f NBU_BackupServerCert.yaml
backupservercert.netbackup.veritas.com/master-0.nbu.isetsu.com created
[root@registry-host NBU10-GA]#
```

Figure 57. BackupServerCert 作成例

9. 作業用 server で以下のコマンドを使用し BackupServerCert の作成が成功したことを確認します。

   (a) 以下のコマンドを使用し BackupServerCert が作成されたことを確認します。

   [実行例] `# oc get backupservercert`

```
[root@registry-host NBU10-GA]# oc get backupservercert
NAME                        AGE
master-0.nbu.isetsu.com     11s
[root@registry-host NBU10-GA]#
```

Figure 58. BackupServerCert 作成確認例

(b) 以下のコマンドを使用し BackupServerCert の作成が成功したことを確認します。

[**status:**]の[**phase:**]が"**InProgress**"から"**Success**"になることを確認します。

[実行例] `# oc get backupservercert master-0.nbu.isetsu.com -o yaml`

```
[root@registry-host NBU10-GA]# oc get backupservercert master-0.nbu.isetsu.com -o yaml
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"netbackup.veritas.com/v1","kind":"BackupServerCert","metadata":{"annotations":{},"name
":"master-0.nbu.isetsu.com","namespace":"netbackup"},"spec":{"backupServer":"master-
0.nbu.isetsu.com","certificateOperation":"Create","certificateType":"NBCA","clusterName":"api.ocp.ise
tsu.com","nbcaAttributes":{"nbcaCreateOptions":{"secretName":"master-0.nbu.isetsu.com"}}}}
  creationTimestamp: "2022-07-26T04:42:45Z"
  generation: 1
  name: master-0.nbu.isetsu.com
  namespace: netbackup
  resourceVersion: "37836568"
  uid: d339f246-bfb8-4334-b980-9a90d6816637
spec:
  backupServer: master-0.nbu.isetsu.com
  certificateOperation: Create
  certificateType: NBCA
  clusterName: api.ocp.isetsu.com
  nbcaAttributes:
    nbcaCreateOptions:
      secretName: master-0.nbu.isetsu.com
status:
  phase: Success    ← Confirm that "InProgress" becomes "Success"
[root@registry-host NBU10-GA]#
```

Figure 59. BackupServerCert 作成成功確認例

10. OpenShift クラスタによって token が使用されたことを確認するために、[**Security**] > [**Tokens**]の[**Token Management**]画面で、作成した token の使用数が増えていることを確認します。

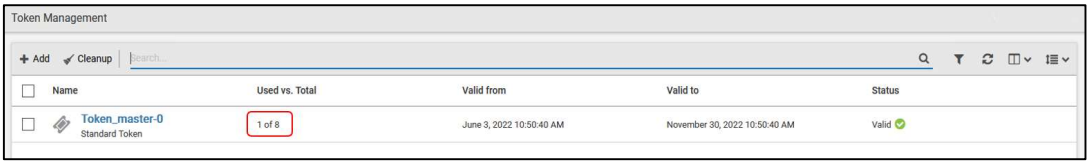

Figure 60. BackupServerCert 適用後の Token Management 画面

11. [**Security**] > [**Host mappings**]の[**Hosts**]タブで、OpenShift クラスタ が"**Secure**"でマッピングされていることを確認します。

Figure 61. BackupServerCert 適用後の Hosts タブ

バックアップおよびリストア操作のための構成設定は以上です。

5　バックアップとリストアの運用手順

この章では、Veritas NetBackup 10.0 でのバックアップとリストアの運用手順を説明します。
Hitachi Storage Plug-in for Containers と連携することにより、Hitachi storage system での Persistent volume に対するアレイベースでのスナップショットを用いて、バックアップウィンドウを短縮することができます。
スナップショットはストレージ筐体内で取得され、バックアップでは NetBackup Media Server へ取得されます。

スナップショットを即時取得し、取得したスナップショットからリストアする場合の手順。

- スナップショットの実行
- スナップショットからのリストア

バックアップを即時取得し、取得したバックアップからリストアする場合の手順。

- バックアップの実行
- バックアップからのリストア

5.1 スナップショットの実行

スナップショットの実行は、Protection planで設定されたスケジュールに沿ったバックアップとBackup now による即時バックアップが実行できます。

5.1.1　Protection Plan の作成

Before you begin

NetBackup web UI にログインします。

Procedure

1. NetBackup web UI で[**Protecition**] > [**Protection Plans**] > [**+Add**]の順にクリックします。

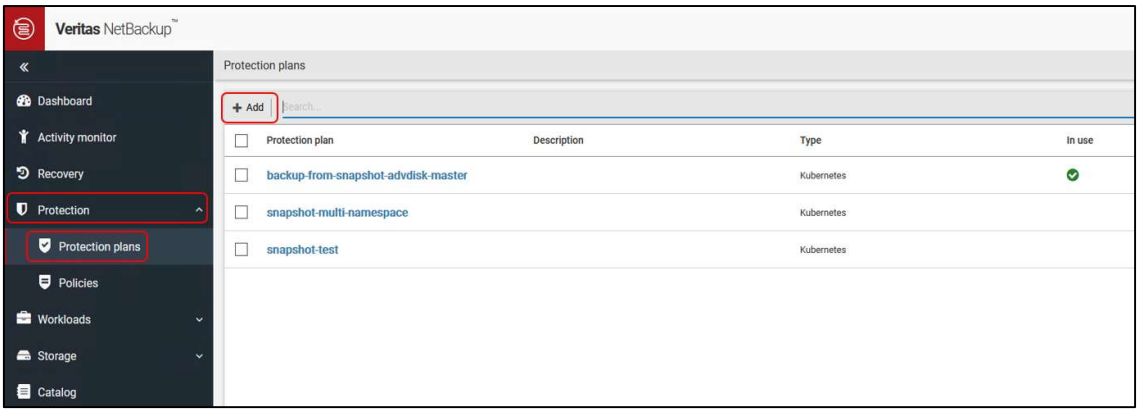

Figure 62. Add a protection plan

2. [Basic properties]でバックアップジョブ名と説明を入力し、[Workload]のドロップダウンリストから"Kubernetes"を選択し、[Next]をクリックします。

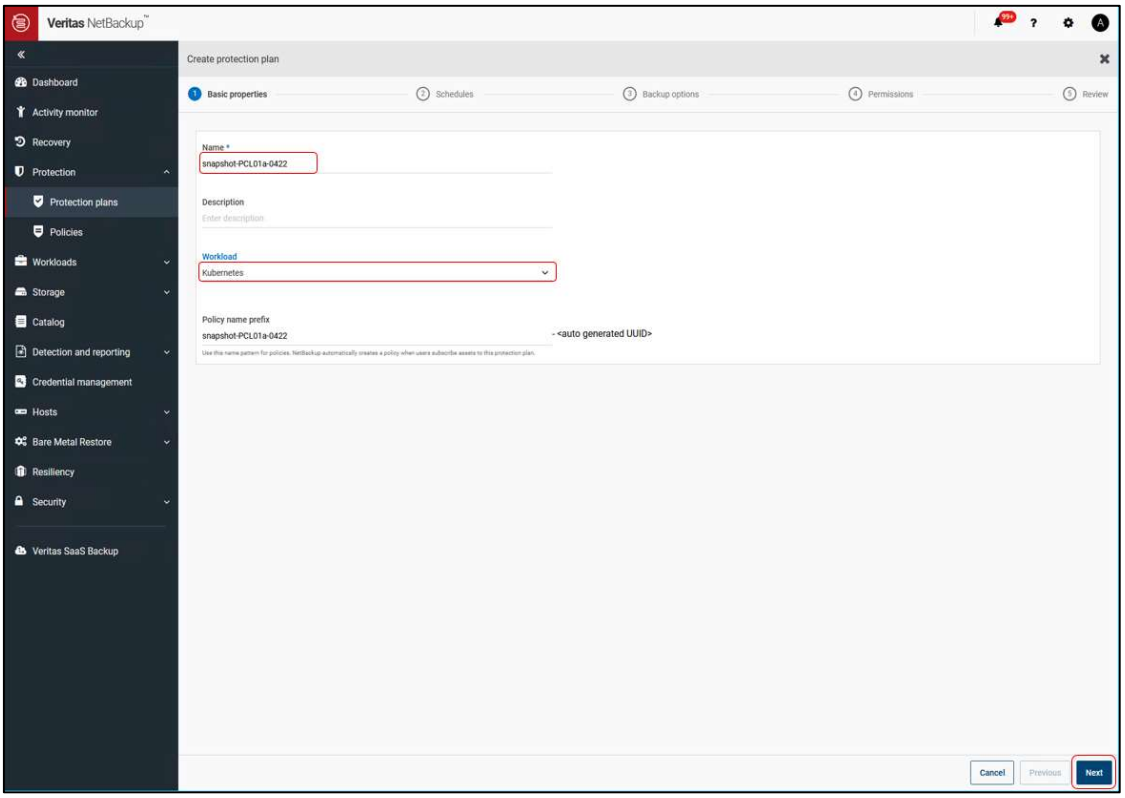

Figure 63. Basic properties

3. [Schedules]で[Add Schedule]をクリックします。

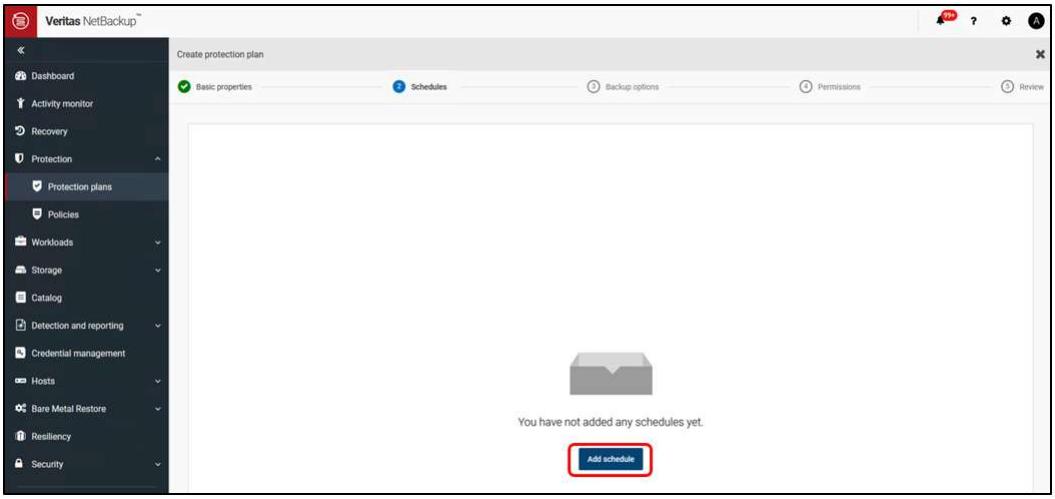

Figure 64. Add schedule

4. [Add backup schedule]の[Attributes]タブで、バックアップタイプの選択やスナップショットの頻度および保持期間など、スナップショットを保持するためのオプションを構成します。

- [Snapshot and backup options]では、[Create backup from snapshot]オプションは設定せずに進みます。

  Create backup from snapshot オプションを設定しないことで、スナップショットだけが実行されるバックアップジョブが設定されるようになります。

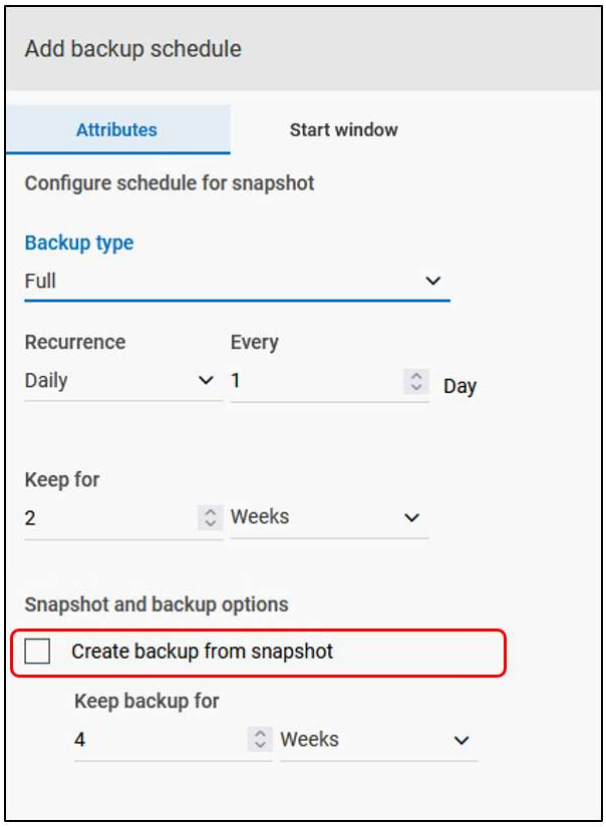

Figure 65. Attributes of Add backup schedule

5. [Start window]タブで開始日時と終了日時を設定し、[Add]をクリックします。

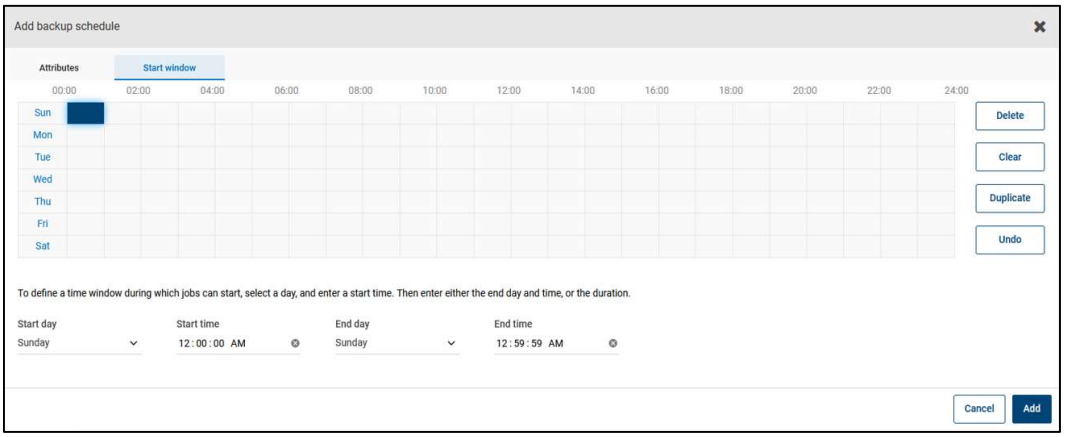

Figure 66. Start window of Add backup schedule

6. スケジュールの確認画面が表示されるので、[Next]をクリックします。

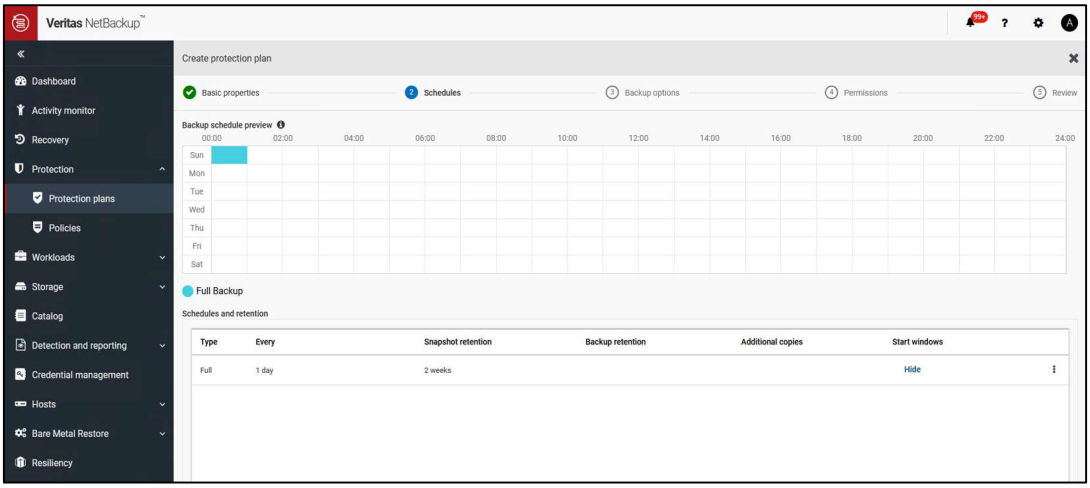

Figure 67. バックアップスケジュール確認画面

7. [**Backup options**]でバックアップオプションを構成するには以下の設定を行います。

   (a) [**Resource kind selection**]セクションで、バックアップするリソースの種類を選択します。デフォルトでは[**Include all resource kinds in the backup**]オプションが選択されており、バックアップジョブのすべてのリソースの種類が含まれます。

   (b) 必要に応じて[**Label selection**]で[**+Add**]を押し、バックアップに関連するリソースをマッピングするためのラベルを追加します。ラベルのプレフィックスとキーを入力し、オペレーターを選択します。

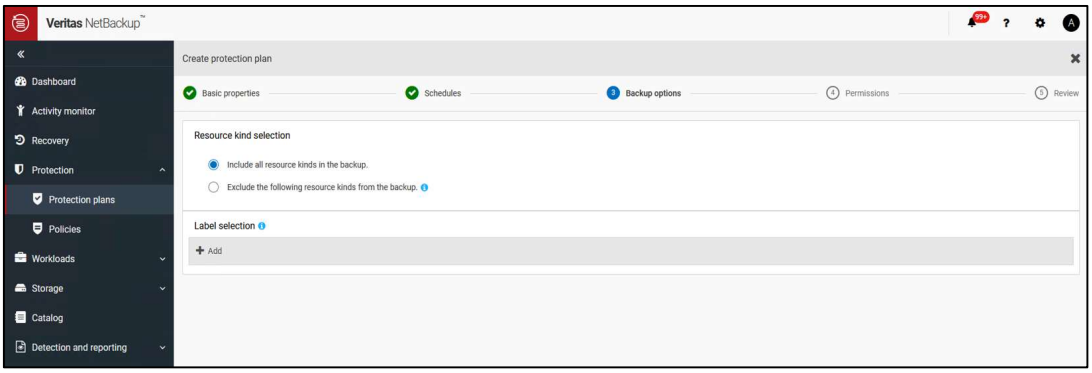

Figure 68. Backup options

8. [**Permissions**]で必要に応じて保護計画にロールを追加し、[**Next**]をクリックします。

Figure 69. Add permissions

9. 内容を確認し[**Finish**]をクリックします。

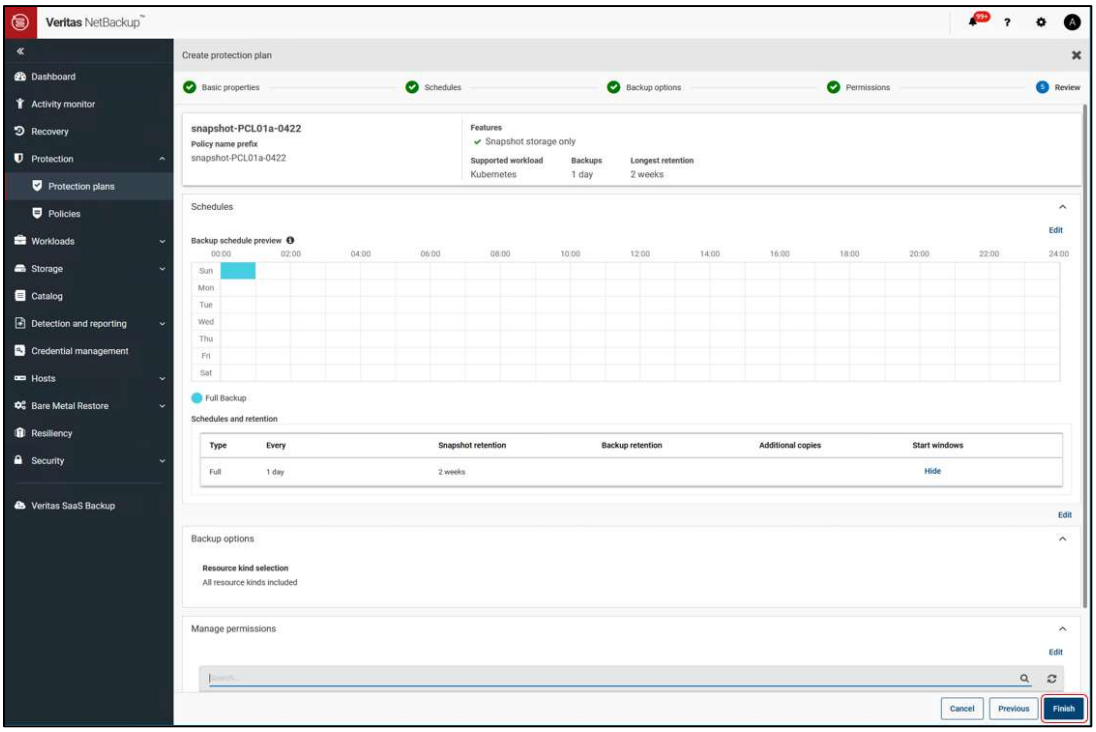

Figure 70. Review

10. Protection Plan が作成されたことを確認します。

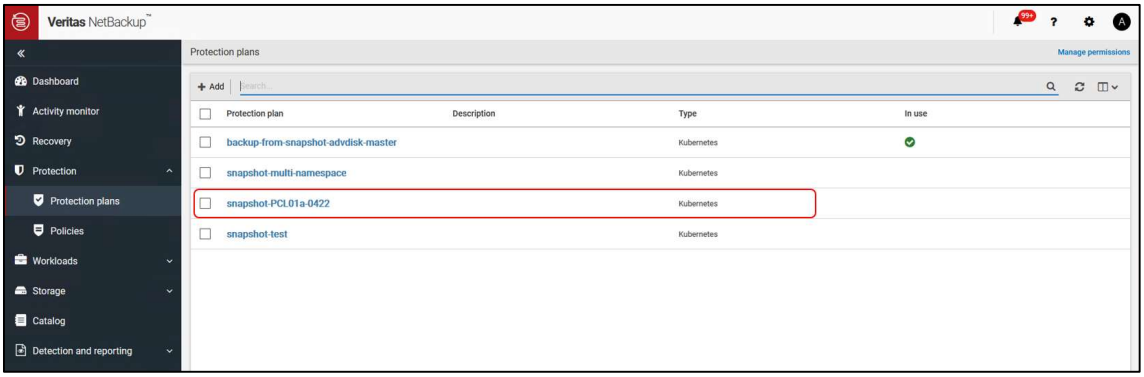

Figure 71. Added a protection plan.

11. [**Workloads**] > [**Kubernetes**]の[**Kubernetes clusters**]タブで、スナップショットを実行するクラスタの[…]をクリックし、"**Discover now**"を選択し、[**Discovery status**]が"**Success**"になることを確認します。

Figure 72. Discover now.

12. [**Namespaces**]タブで Protection Plan を割り当てる namespace をクリックします。

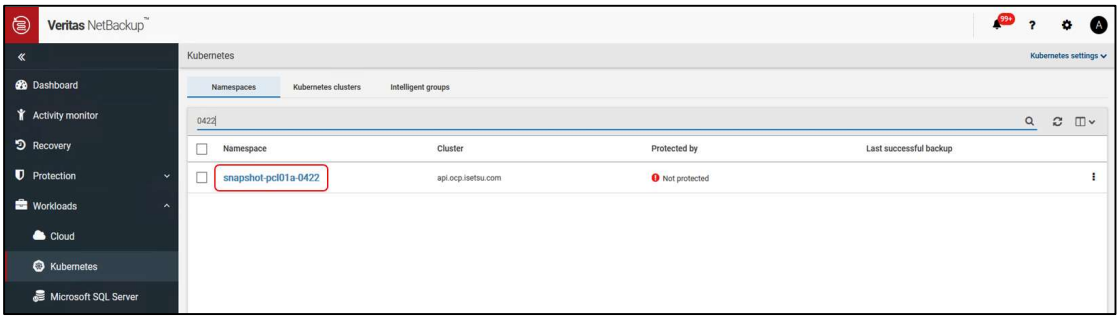

Figure 73. Select the namespace.

13. [**Protection**]タブを開き、[**Add protection**]をクリックします。

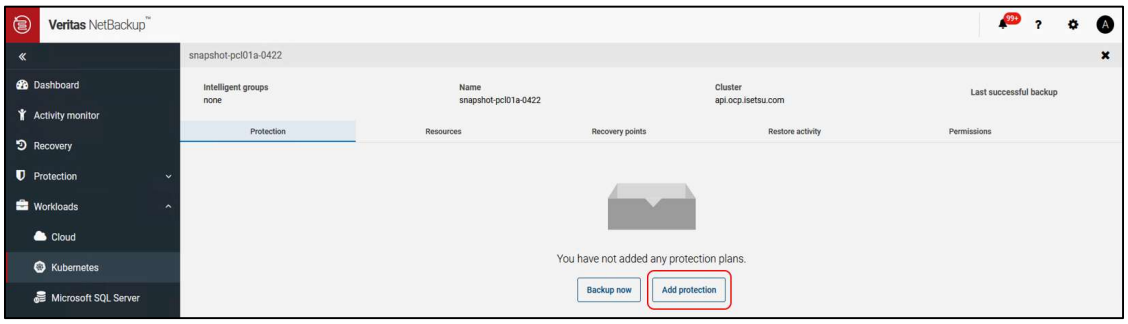

Figure 74. Add protection.

14. Protection plan の一覧から、割り当てる Protection plan を選択し[**Next**]をクリックします。

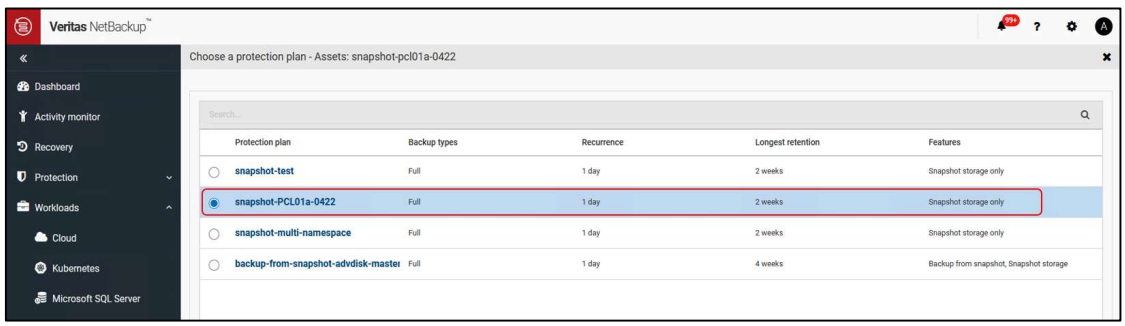

Figure 75. Select the protection plan.

15. Protection plan の情報画面で[**Protect**]をクリックします。

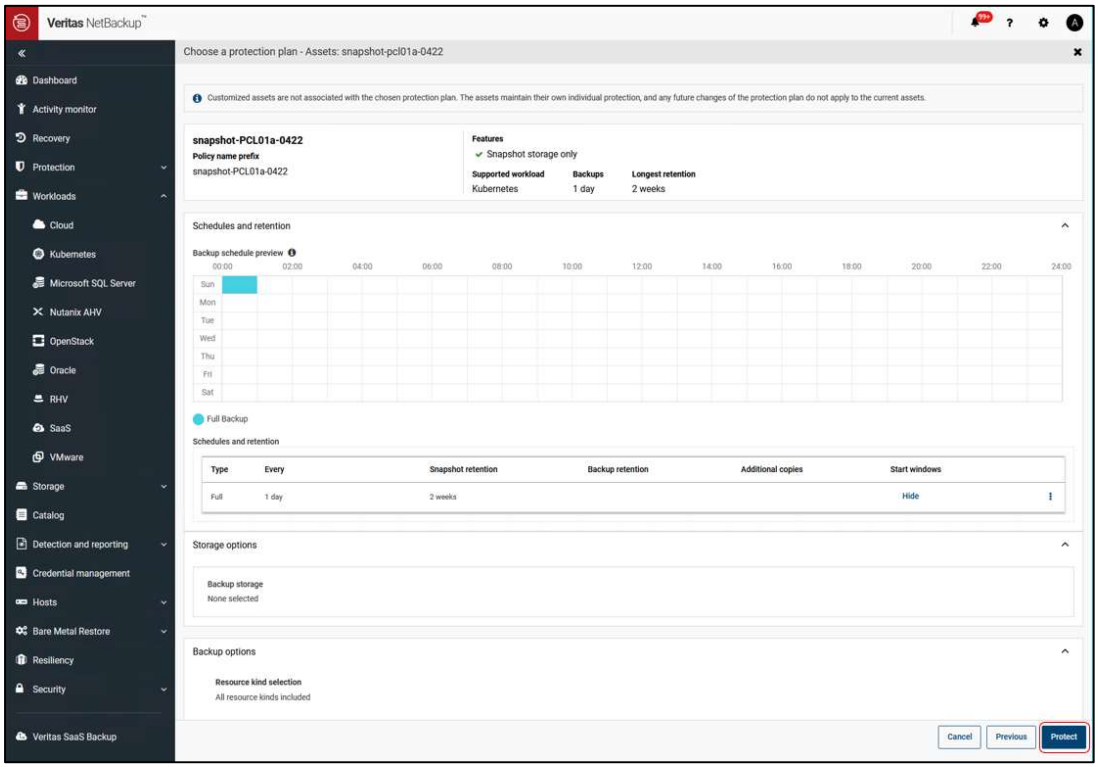

Figure 76. Protect the namespace

16. "**Added to plan**"と表示されることを確認し、[**Close**]をクリックします。

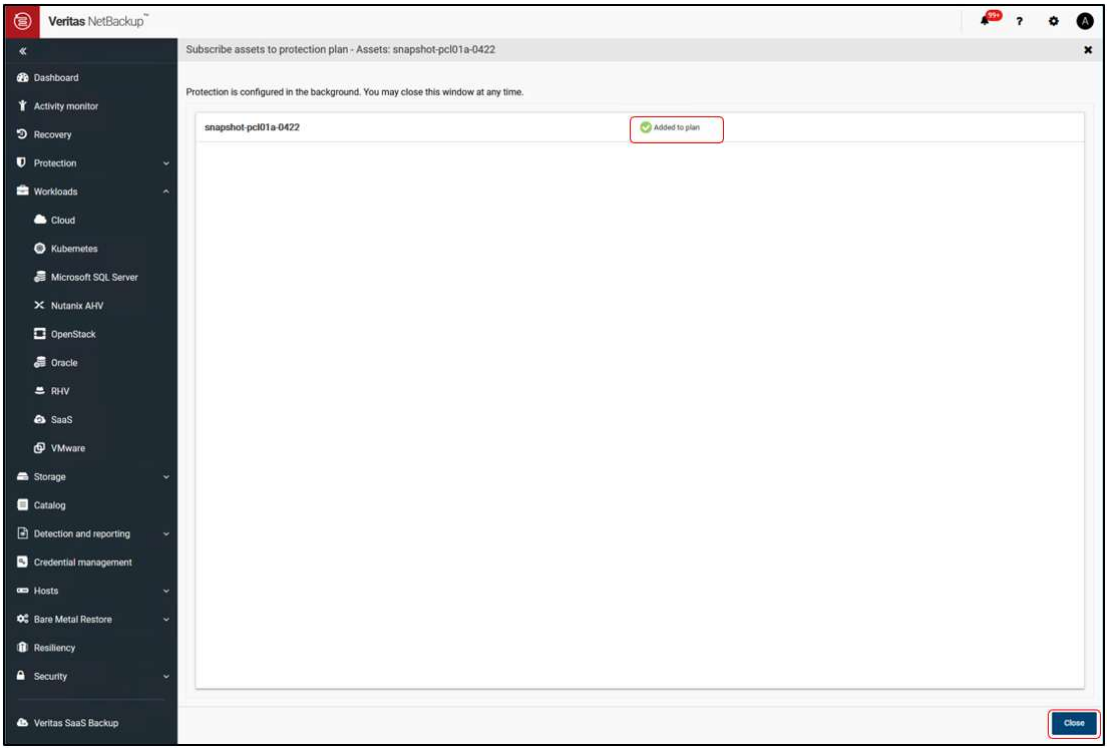

Figure 77. Adding to plan is succeeded.

17. Namespace の Protection に設定した Protection plan が表示されることを確認します。

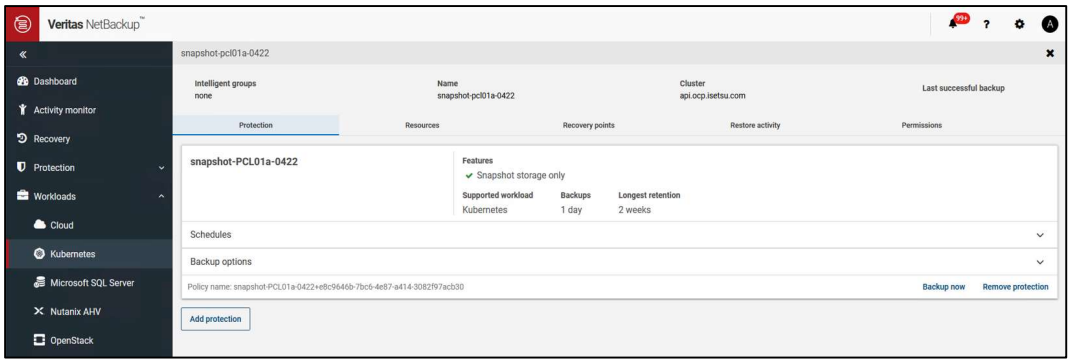

Figure 78. Protection plan of the namespace

以上で Protection Plan の作成は終了です。Protection Plan で設定したスケジュールに従い、割り当てた Namespace に対しスナップショットが取得されます。

5.1.2 Backup now の実行

Backup now により即時バックアップを実行できます。

Prerequisites

事前に Protection plan を作成しておく必要があります。

Before you begin

NetBackup web UI にログインします。

Procedure

1. NetBackup web UI で[**Workloads**] > [**Kubernetes**]の[**Namespaces**]タブでスナップショットを実行する namespace をクリックし、[**Backup now**]をクリックします。

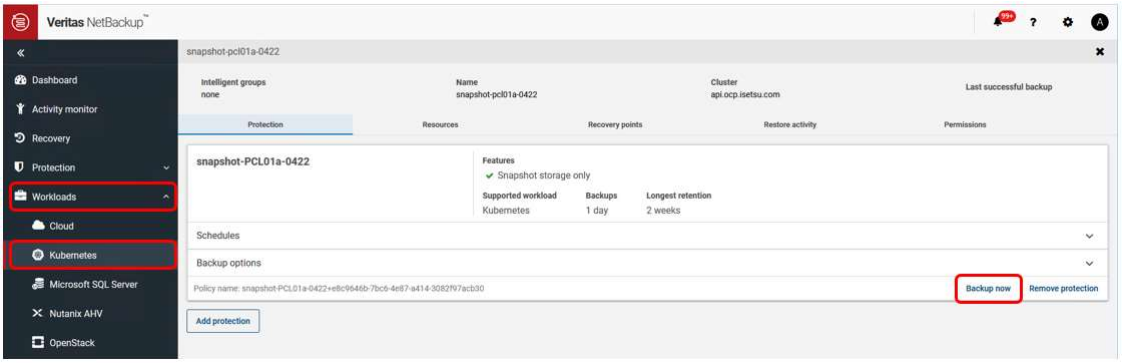

Figure 79. バックアップ実行画面

2. バックアップ実行の確認画面で、[**Start backup**]をクリックします。

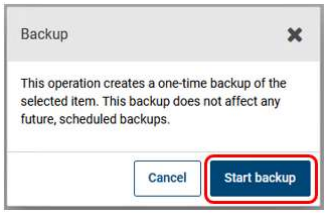

Figure 80. バックアップ実行確認画面

3. [**Activity monitor**]でバックアップジョブの状態を確認し、ジョブが終了するまで待ちます。

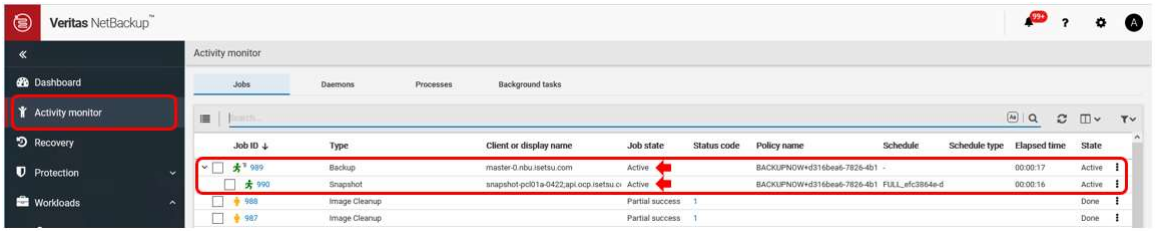

Figure 81. バックアップジョブ確認画面例（ジョブ実行中）

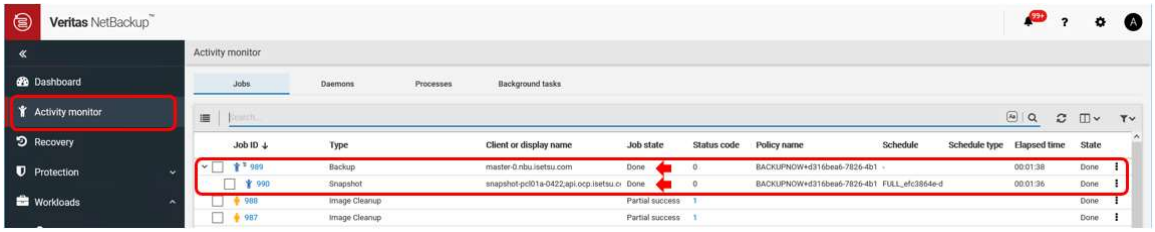

Figure 82. バックアップジョブ確認画面例（ジョブ終了）

4. [**Workloads**] > [**Kubernetes**]の[**Namespaces**]タブでスナップショットを実行した namespace をクリックし、[**Recovery points**]タブをクリックします。

   リカバリポイントが作成されていることを確認します。

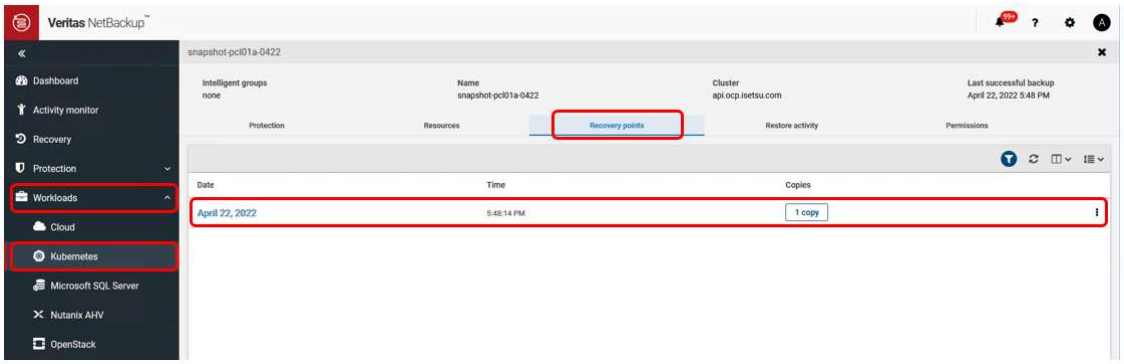

Figure 83. Recovery points 画面例

5. スナップショットが実行できたことを OpenShift クラスタで確認する。

本コマンドは、Red Hat OpenShift Container Platform の CLI である oc コマンドを実行できる作業用 server で実行します。oc コマンドは Kubernetes API Server に対して発行され、OpenShift Container Platform cluster 内の適切な node で処理されます。

(a) スナップショットを取得した Persistent VolumeClaim の VolumeSnapshotContent を確認する。

[実行例] `# oc get volumesnapshot -n snapshot-pcl01a-0824`

Figure 84. VolumeSnapshotContent の確認例

(b) VolumeSnapshotContent でスナップショットのペアを確認する。

[実行例] `# oc describe volumesnapshotcontent snapcontent-9e170547-76c1-45da-b516-8105201a169f`

```
[root@registry-host result_GA_restore-snapshot-PCL01a]# oc describe volumesnapshotcontent snapcontent-9e170547-76c1-45da-b516-
8105201a169f
Name:         snapcontent-9e170547-76c1-45da-b516-8105201a169f
Namespace:
Labels:       <none>
Annotations:  snapshot.storage.kubernetes.io/deletion-secret-name: secret-hitstorage
              snapshot.storage.kubernetes.io/deletion-secret-namespace: csihspc
API Version:  snapshot.storage.k8s.io/v1
Kind:         VolumeSnapshotContent
Metadata:
  Creation Timestamp:  2022-08-24T05:28:00Z
  Finalizers:
    snapshot.storage.kubernetes.io/volumesnapshotcontent-bound-protection
  Generation:  2
  Managed Fields:
    API Version:  snapshot.storage.k8s.io/v1
    Fields Type:  FieldsV1
    fieldsV1:
      f:metadata:
        f:annotations:
          .:
          f:snapshot.storage.kubernetes.io/deletion-secret-name:
          f:snapshot.storage.kubernetes.io/deletion-secret-namespace:
        f:finalizers:
          .:
          v:"snapshot.storage.kubernetes.io/volumesnapshotcontent-bound-protection":
      f:spec:
        .:
        f:driver:
        f:source:
          .:
          f:volumeHandle:
        f:volumeSnapshotClassName:
        f:volumeSnapshotRef:
          .:
          f:apiVersion:
          f:kind:
          f:name:
          f:namespace:
          f:resourceVersion:
          f:uid:
    Manager:      snapshot-controller
    Operation:    Update
    Time:         2022-08-24T05:28:00Z
    API Version:  snapshot.storage.k8s.io/v1
    Fields Type:  FieldsV1
    fieldsV1:
      f:spec:
        f:deletionPolicy:
    Manager:      backup-operator (linux
    Operation:    Update
    Time:         2022-08-24T05:28:20Z
    API Version:  snapshot.storage.k8s.io/v1
    Fields Type:  FieldsV1
    fieldsV1:
      f:status:
        .:
        f:creationTime:
        f:readyToUse:
        f:restoreSize:
        f:snapshotHandle:
    Manager:         csi-snapshotter
    Operation:       Update
    Time:            2022-08-24T05:28:20Z
  Resource Version:  56174842
  UID:               07dc5746-7ca5-4451-9824-268fea2459dc
```

```
Spec:
  Deletion Policy:  Retain
  Driver:           hspc.csi.hitachi.com
  Source:
    Volume Handle:            60060e80120001005040000100000004--spc-c7b8c36223
  Volume Snapshot Class Name:  snapclass-hitstorage              ↑ Nickname of PersistentVolumeClaim that
  Volume Snapshot Ref:                                             obtained snapshot
    API Version:       snapshot.storage.k8s.io/v1
    Kind:              VolumeSnapshot
    Name:              nbu-vs-e6c44cce-d978-4540-a4ac-066db932335c
    Namespace:         snapshot-pcl01a-0824
    Resource Version:  56174685
    UID:               9e170547-76c1-45da-b516-8105201a169f
Status:
  Creation Time:    1661350791000000000
  Ready To Use:     true
  Restore Size:     1374389534720                      ↓ Nickname of snapshot pair
  Snapshot Handle:  60060e80120001005040000100000006--spc-9bf09ed7a7
Events:             <none>
[root@registry-host result_GA_restore-snapshot-PCL01a]#
```

Figure 85. ペアの確認例

6. スナップショットが実行できたことをストレージで確認する。

   (a) ボリュームの一覧で LDEV の状態を確認する。

      手順 5 .(b)で調べた nickname の状態を調べる。

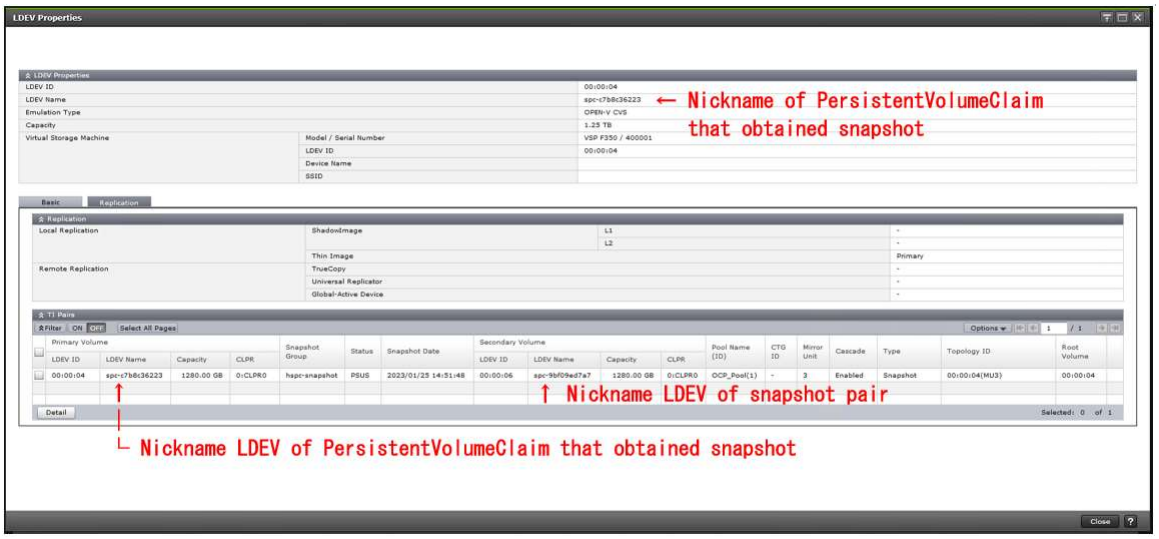

Figure 86. スナップショットを取得した Persistent VolumeClaim の LDEV プロパティ例

Backup now の実行手順は以上です。

5.2 スナップショットからのリストア

スナップショットからのリストアは NetBackup web UI から実行できます。

Before you begin

NetBackup web UI にログインします。

Procedure

1. NetBackup web UI で[**Workloads**] > [**Kubernetes**] > [**Namespaces**]タブを開き、リカバリする namespace をクリックします。

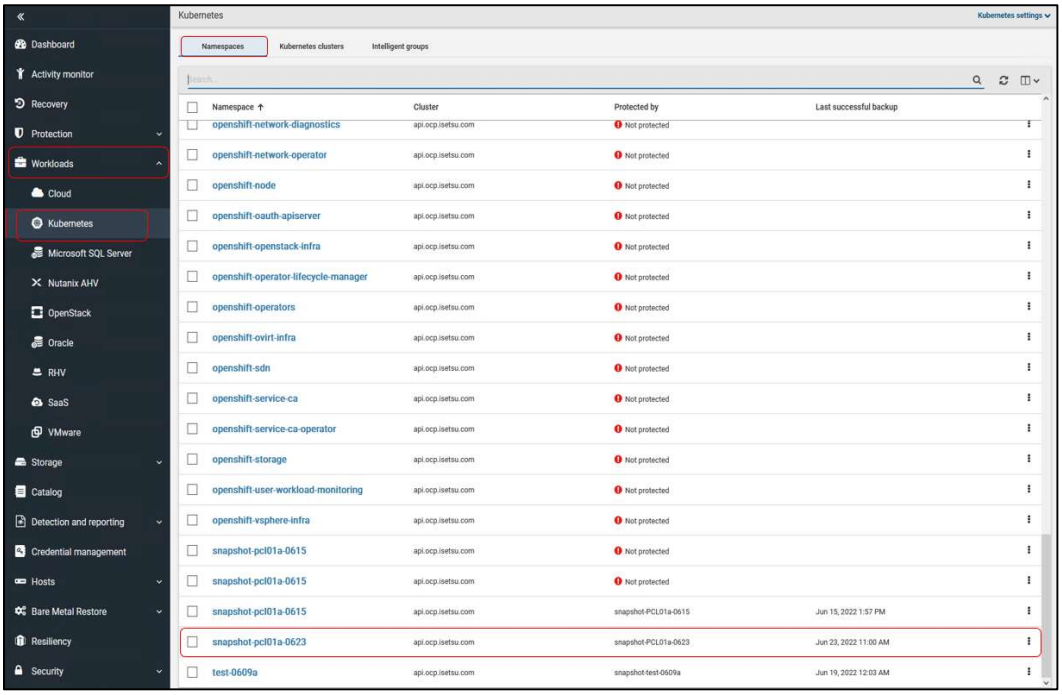

Figure 87. Select a namespace to recovery

2. [**Recovery points**]タブをクリックします。

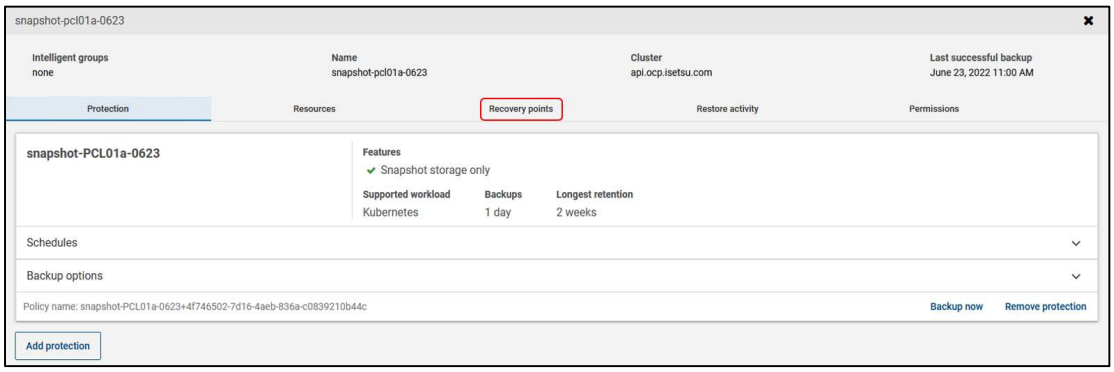

Figure 88. Open the Recovery points tab

3. [**Copies**]の情報をクリックします。Snapshot タイプとリカバリする完全なコピーがあるリカバリポイントの行の省略メニュー（…）をクリックし、[**Restore**]をクリックします。

Figure 89. Copies of the Recovery points

4. [**Recovery target**]ページで以下を選択し[**Next**]をクリックします。

   (a) ターゲットクラスタが自動入力されます。

   (b) [**Specify destination namespace**]でリストアオプションを選択します。

   - Use original namespace： オリジナルの namespace を使用する（デフォルト）
   - Use alternate namespace： 代替の namespace を使用する

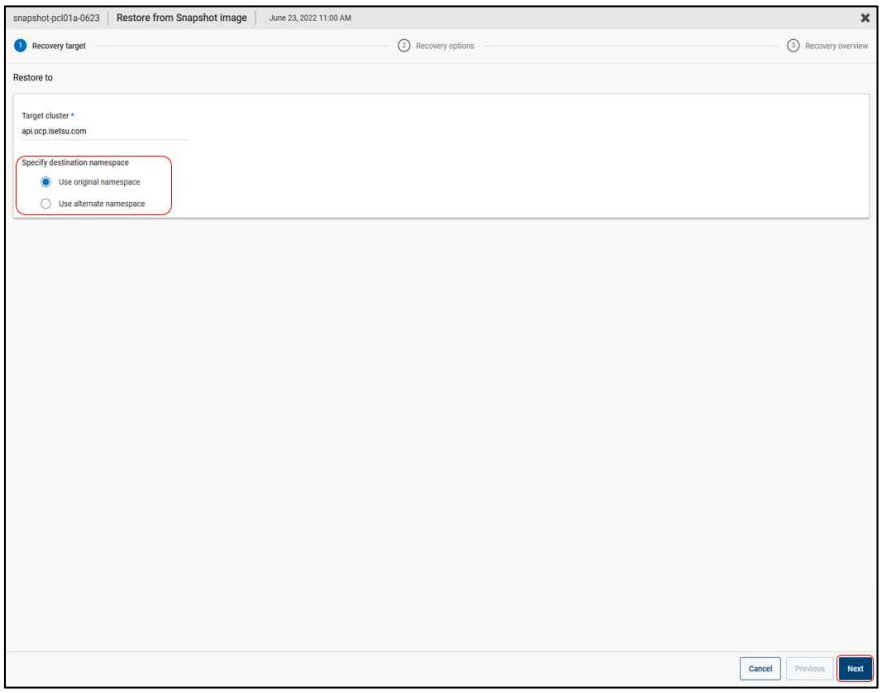

Figure 90. Recovery target

5. [**Recovery options**]ページで以下を選択し[**Next**]をクリックします。

   (a) [**Select resource types to recover**]でリカバリするリソースタイプを選択します。

   - All resource types： すべてのリソースタイプをリカバリします（デフォルト）
   - Recover selected resource types： 選択したリソースタイプをリカバリします

   (b) [**Select Persistent volume claims to recover**]で、すべての Persistent volume claim をリカバリするか、特定の Persistent volume claim をリカバリするか選択します

   - All Persistent volume claims：すべての Persistent volume claim をリカバリします（デフォルト）
   - Recover selected Persistent volume claims: 選択した Persistent volume claim をリカバリします

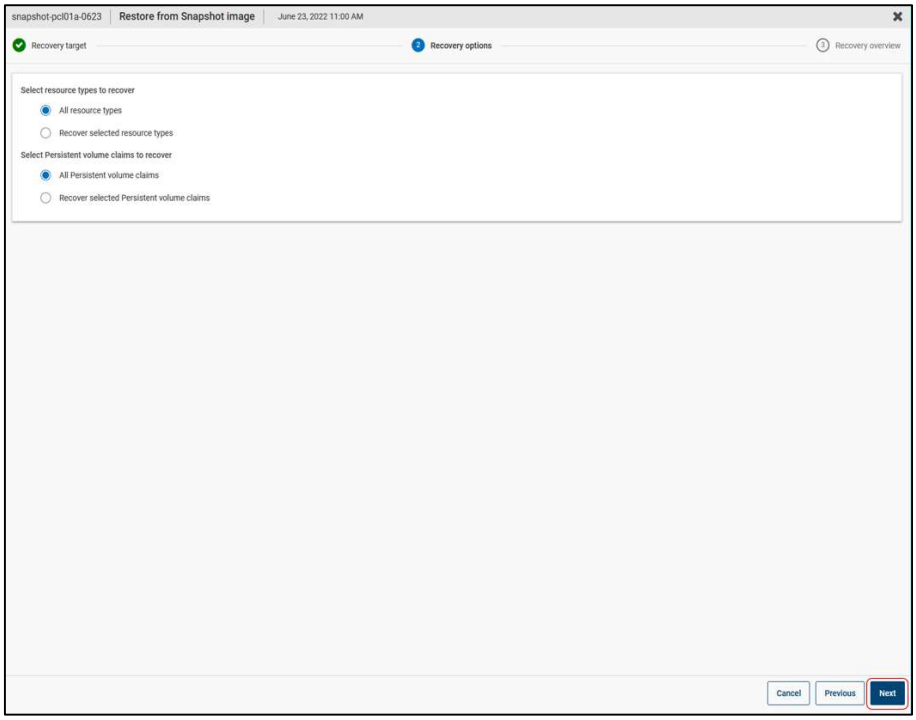

Figure 91. Recovery options

6. [**Recovery overview**]ページで、[**Start recovery**]をクリックしてリカバリエントリをサブミットします。

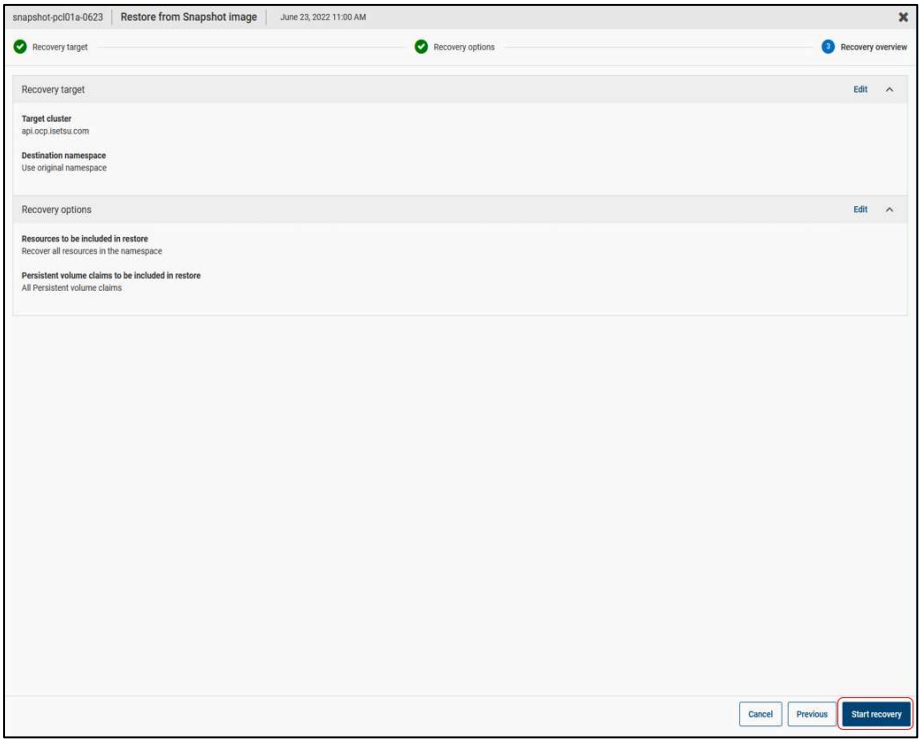

Figure 92. Recovery overview

7. [**Activity Monitor**] > [**Jobs**]タブで Job ID をクリックするとリストアジョブの詳細が表示されます。

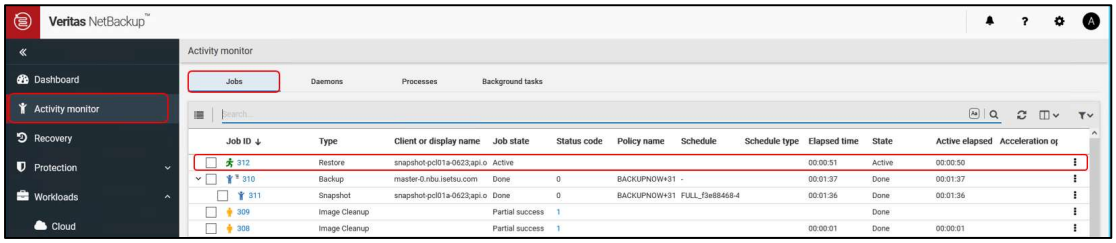

Figure 93. Activity monitor

スナップショットからのリストア手順は以上です。

5.3 バックアップの実行

バックアップの実行 は、Protection plan で設定されたスケジュールに沿ったバックアップと Backup now による即時バックアップが実行できます。バックアップを実行するために、Protection Plan に"Create backup from snapshot"を設定します。

5.3.1 Backup from snapshot の Protection Plan の作成

バックアップの実行は Protection Plan で"Create backup from snapshot"を設定する必要があります。

Before you begin

NetBackup web UI にログインします。

Procedure

1. NetBackup web UI で[**Protection**] > [**Protection Plans**] > [**+Add**]の順にクリックします。

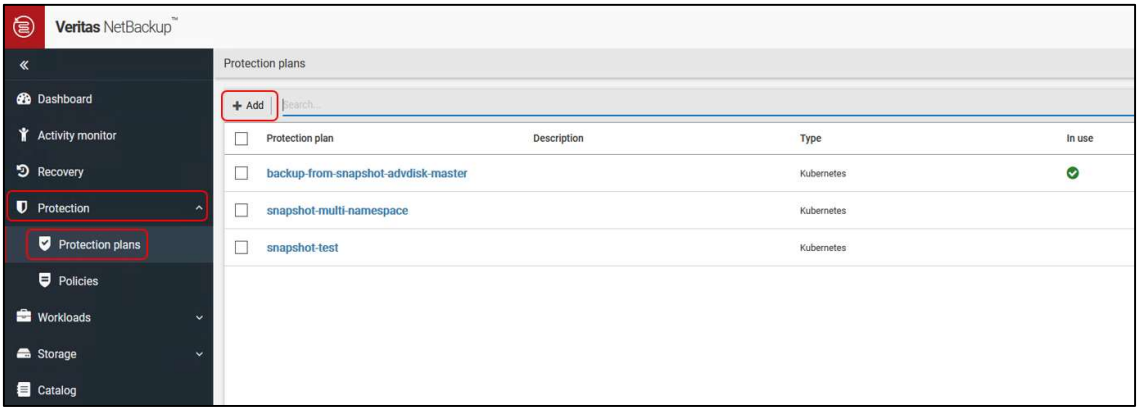

Figure 94. Add a protection plan

2. [**Basic properties**]でバックアップジョブ名と説明を入力し、[**Workload**]のドロップダウンリストから"**Kubernetes**"を選択し、[**Next**]をクリックします。

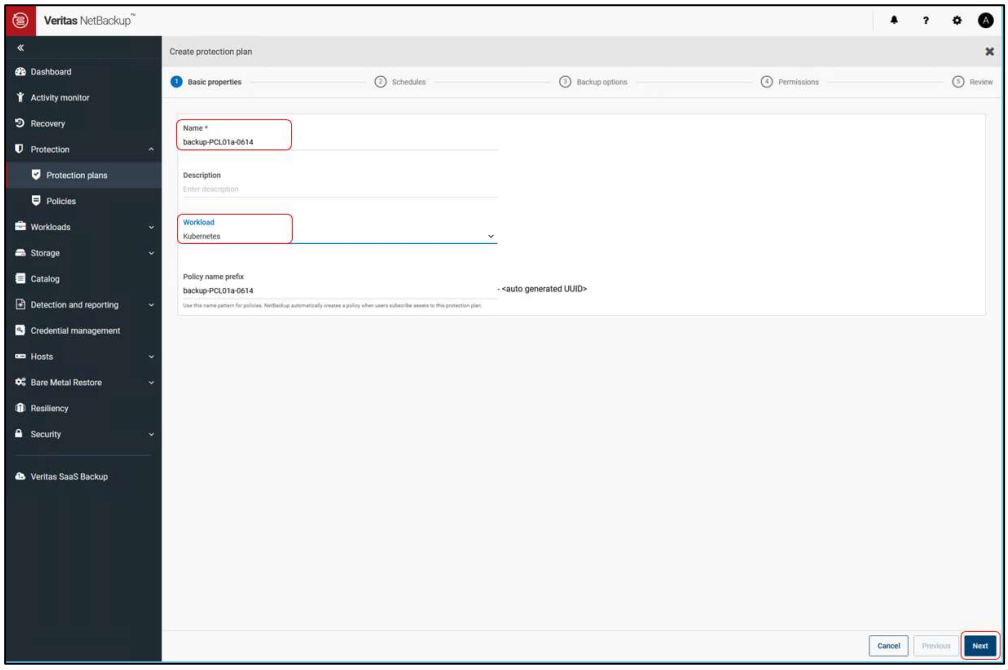

Figure 95. Basic properties

3. [Schedules]で[Add Schedule]をクリックします。

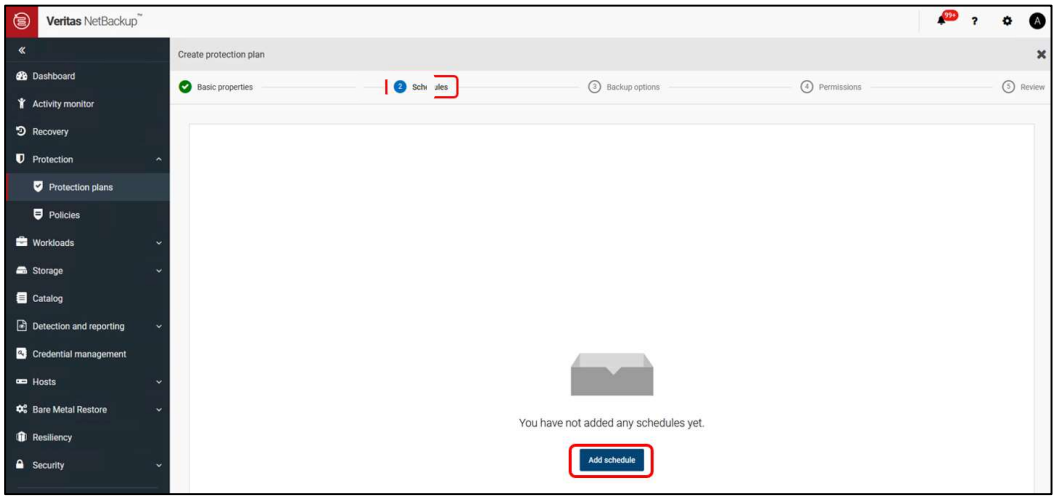

Figure 96. Add schedule

4. [Add backup schedule]の[Attributes]タブで、バックアップタイプの選択やバックアップの頻度および保持期間など、バックアップを保持するためのオプションを構成します。

   - [Snapshot and backup options]では、[Create backup from snapshot]オプションを設定します。

     Create backup from snapshot オプションを設定すると、バックアップジョブが設定されるようになります。

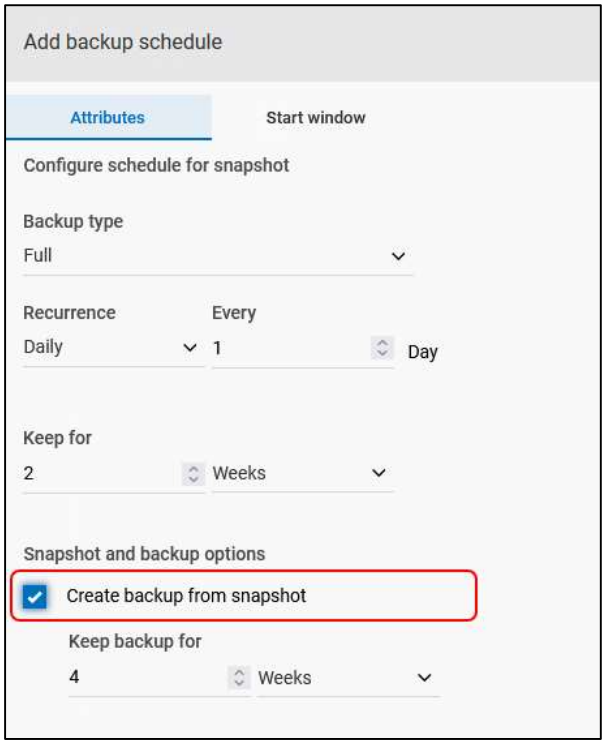

Figure 97. Attributes of Add backup schedule

5. [**Start window**]タブで開始日時と終了日時を設定し、[**Add**]をクリックします。

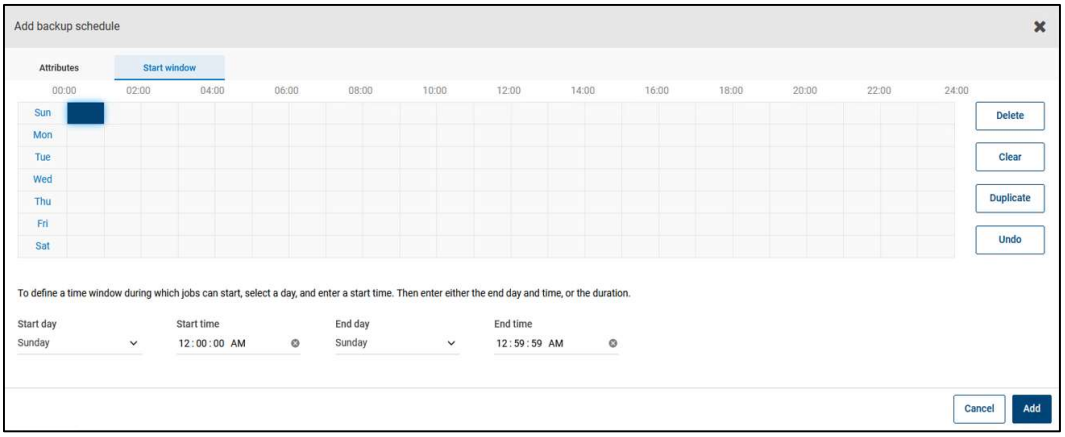

Figure 98. Start window of Add backup schedule

6. スケジュールの確認画面が表示されるので、[**Next**]をクリックします。

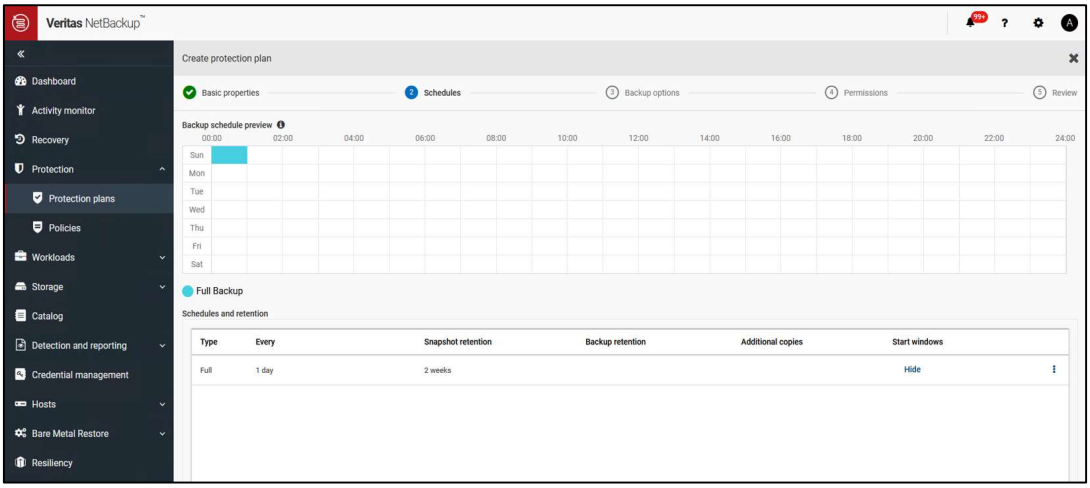

Figure 99. バックアップスケジュール確認画面

7. [**Storage options**]で Backup storage を選択するため、[**Edit**]をクリックします。

Figure 100. Storage options

8. [**Select Backup Storage**]で、メディア server—に作成したストレージユニットを選択し[**Use selected storage**]をクリックします。

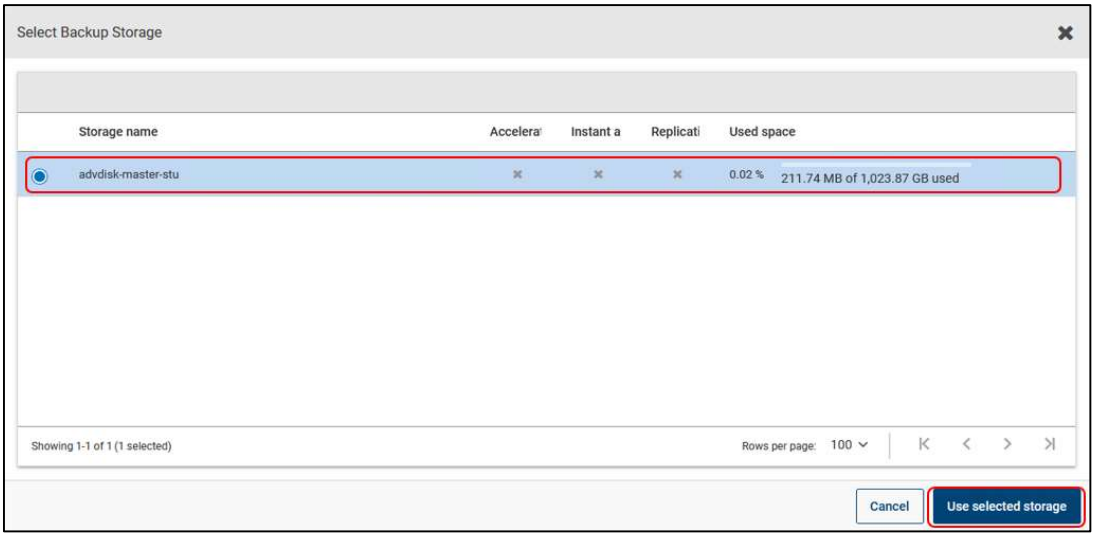

Figure 101. Select Backup Storage

9. Backup storage に指定したストレージユニットが表示されていることを確認し、[**Next**]をクリックします。

Figure 102. Check backup storage

10. [**Backup options**]でバックアップオプションを構成するには以下の設定を行います。

    (a) [**Resource kind selection**]セクションで、バックアップするリソースの種類を選択します。デフォルトでは[**Include all resource kinds in the backup**]オプションが選択されており、バックアップジョブのすべてのリソースの種類が含まれます。

    (b) 必要に応じて[**Label selection**]で[**+Add**]を押し、バックアップに関連するリソースをマッピングするためのラベルを追加します。ラベルのプレフィックスとキーを入力し、オペレーターを選択します。

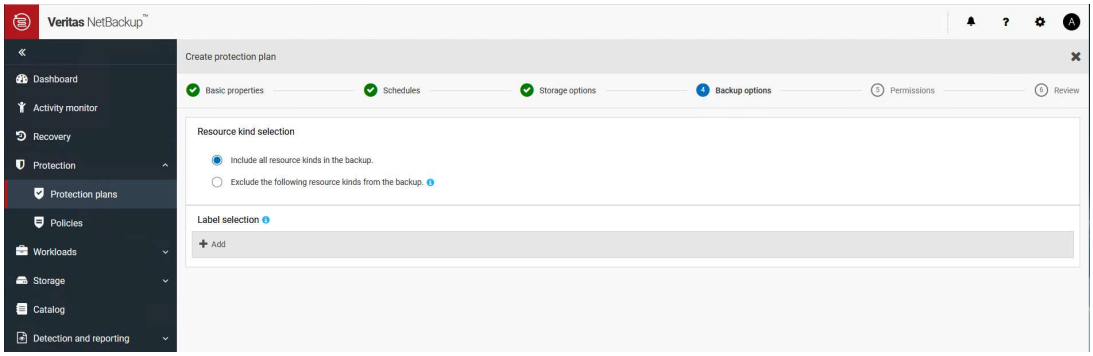

Figure 103. Backup options

11. [**Permissions**]で必要に応じて保護計画にロールを追加し、[**Next**]をクリックします。

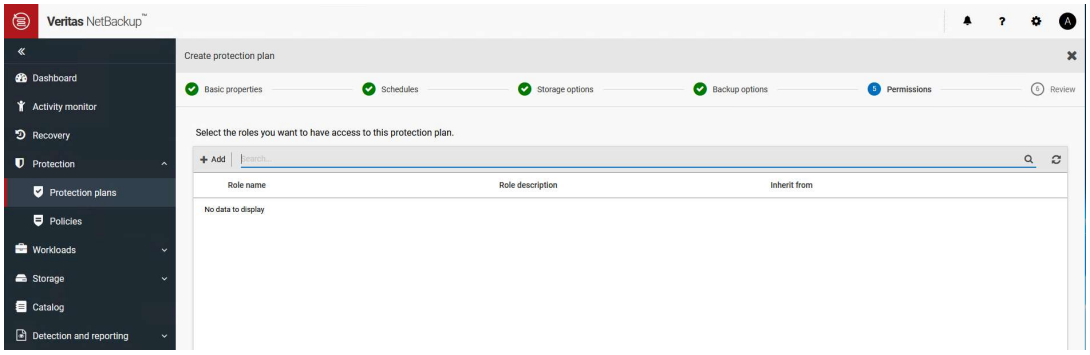

Figure 104. Add permissions

12. 内容を確認し[**Finish**]をクリックします。

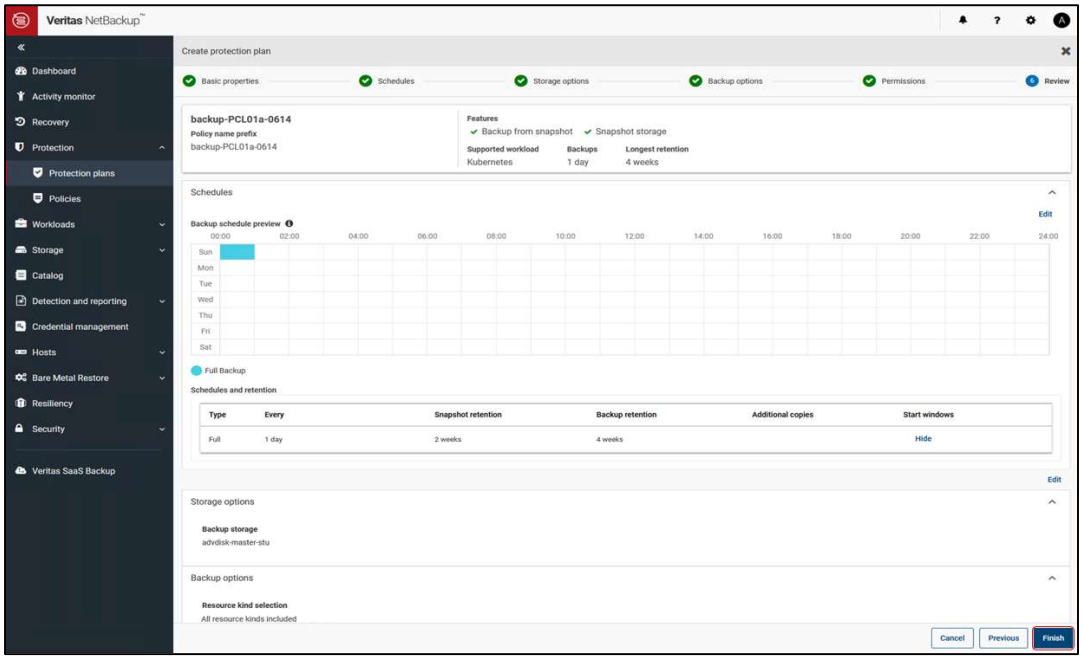

Figure 105. Review

13. Protection Plan が作成されたことを確認します。

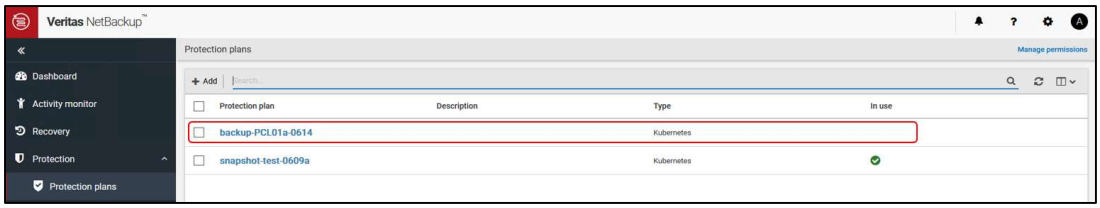

Figure 106. Add permissions

14. [**Workloads**] > [**Kubernetes**]の[**Kubernetes clusters**]タブで、スナップショットからのバックアップを実行するクラスタ の[…]をクリックし、"**Discover now**"を選択し、[**Discovery status**]が"**Success**"になることを確認します。

Figure 107. Discover now.

15. [**Namespaces**]タブで Protection Plan を割り当てる namespace をクリックします。

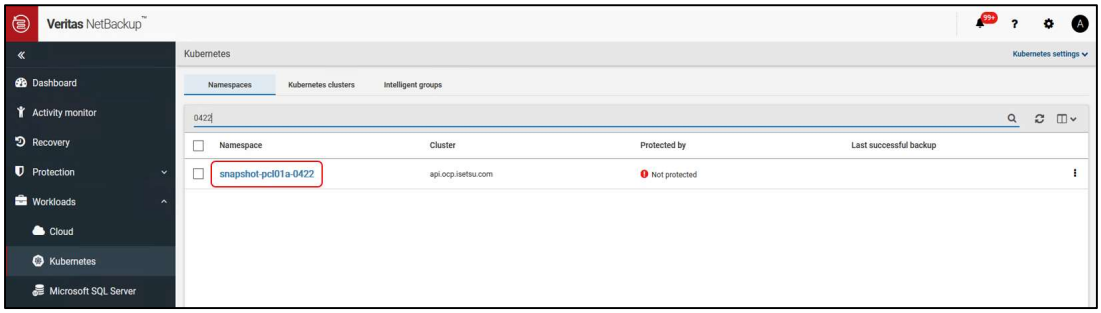

Figure 108. Select the namespace

16. [**Protection**]タブを開き、[**Add protection**]をクリックします。

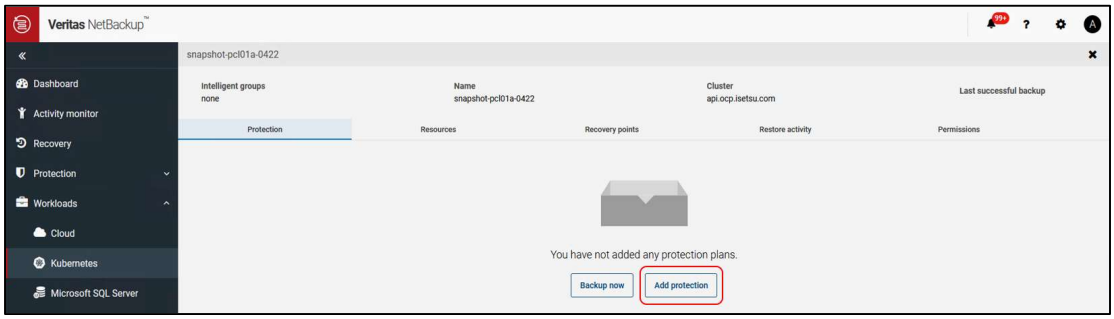

Figure 109. Add protection

17. Protection plan の一覧から、割り当てる Protection plan を選択し[**Next**]をクリックします。

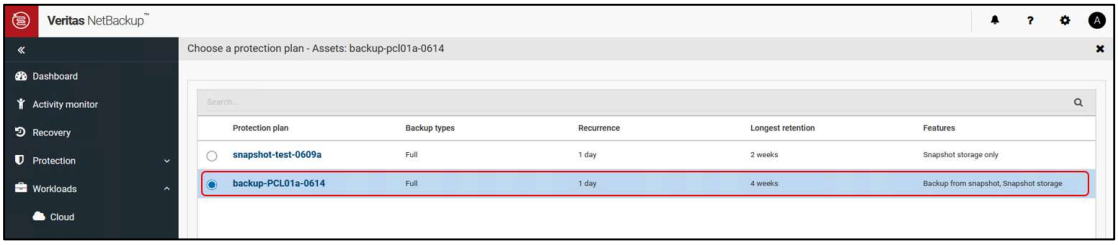

Figure 110. Select the protection plan

18. Protection plan の情報画面で[**Protect**]をクリックします。

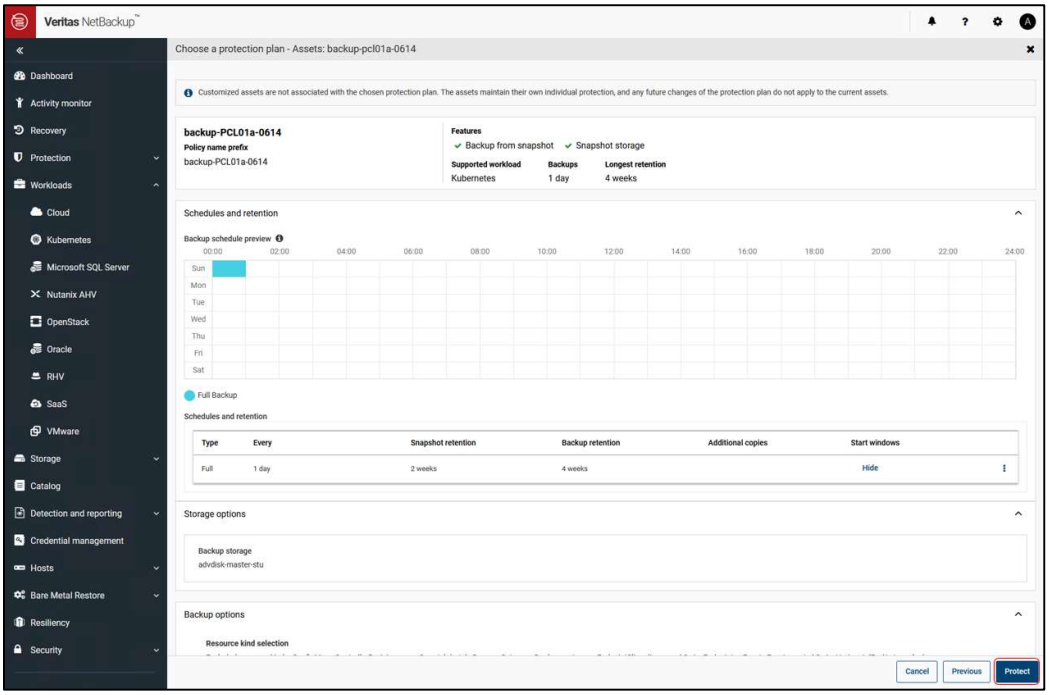

Figure 111. Protect the namespace

19. "**Added to plan**"と表示されることを確認し、[**Close**]をクリックします。

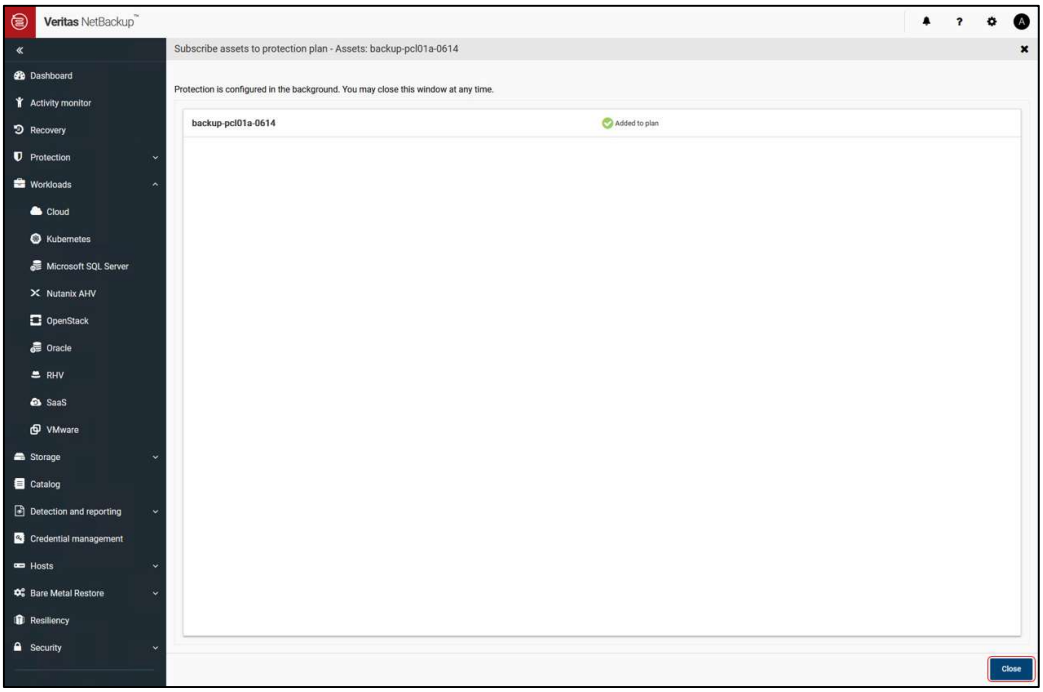

Figure 112. Adding to plan is succeeded

20. Namespace の Protection に設定した Protection plan が表示されることを確認します。

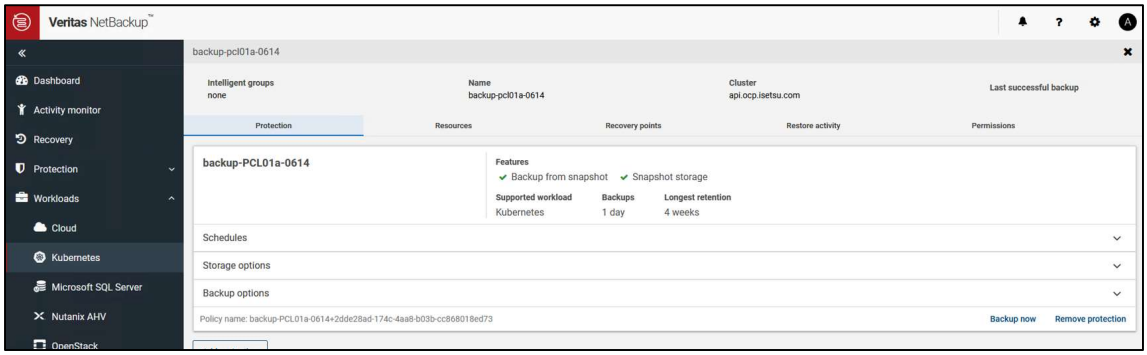

Figure 113. Protection plan of the namespace

以上で Protection Plan の作成は終了です。Protection Plan で設定したスケジュールに従い、割り当てた Namespace に対しバックアップが取得されます。

5.3.2 Backup now の実行

Backup now により即時バックアップを実行できます。
Backup now の手順については、前述のスナップショットの実行の Backup now の実行を参照ください。

5.4 バックアップからのリストア

リストア手順の中で、Backup タイプの Recovery points を選択することでバックアップからのリストアを実行できます。

Before you begin

NetBackup web UI にログインします。

Procedure

1. NetBackup web UI で[**Workloads**] > [**Kubernetes**] > [**Namespaces**]タブを開き、リカバリする namespace をクリックします。

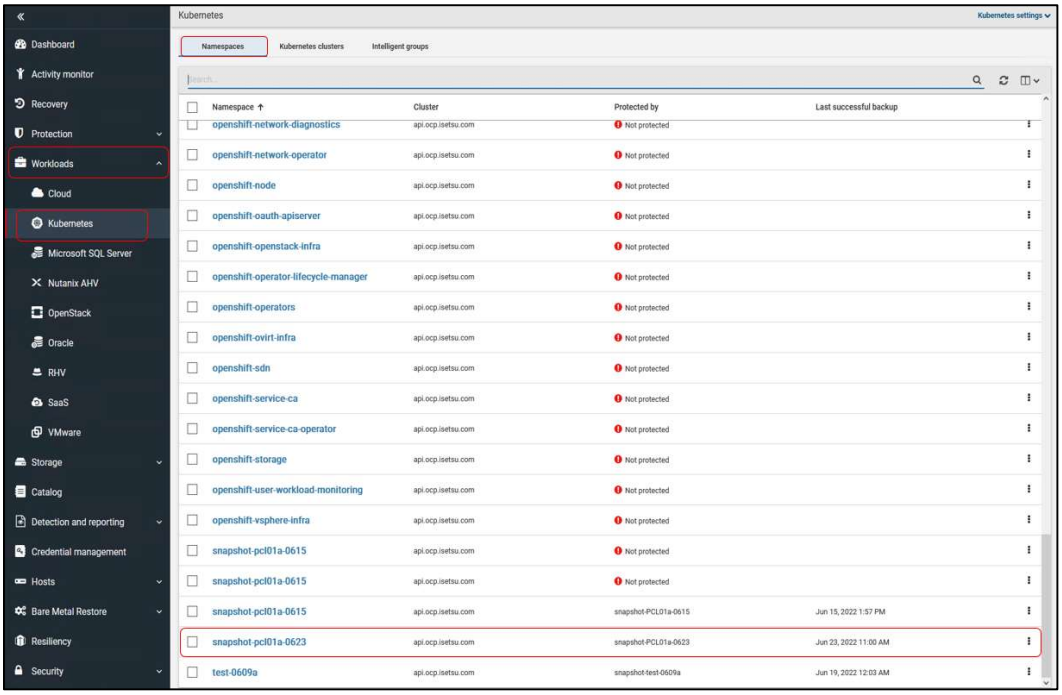

Figure 114. Select a namespace to recovery

2. [**Recovery points**]タブをクリックします。

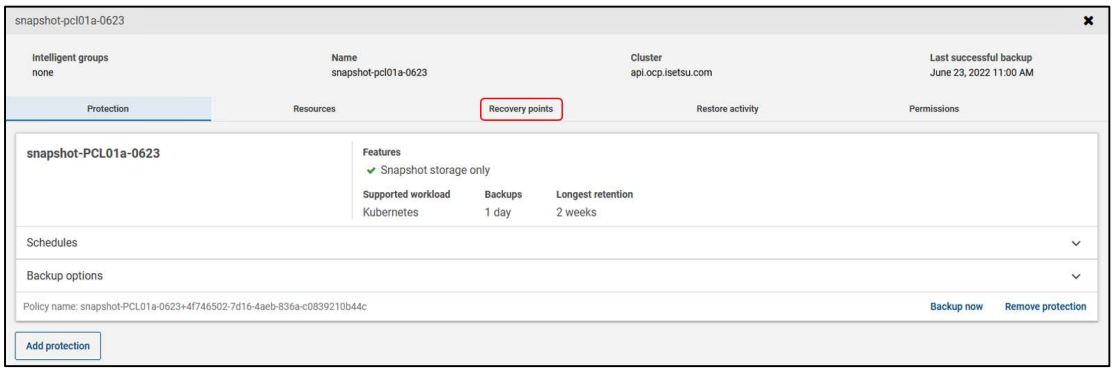

Figure 115. Open the Recovery points tab

3. [**Copies**]の情報をクリックします。Backup タイプとリカバリする完全なコピーがあるリカバリポイントの行の省略メニュー（…）をクリックし、[**Restore**]をクリックします。

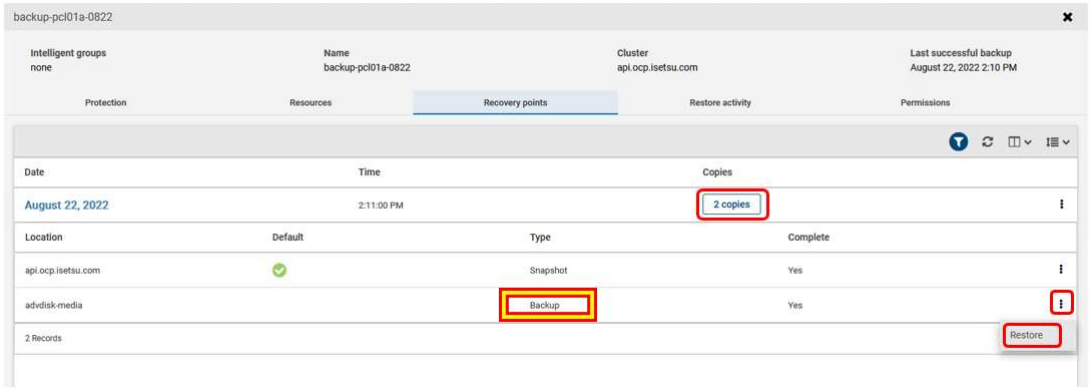

Figure 116. Copies of the Recovery points

4. [**Recovery target**]ページで以下を選択し[**Next**]をクリックします。

   (a) ターゲットクラスタが自動入力されます。

   (b) [**Specify destination namespace**]でリストアオプションを選択します。

   - Use original namespace： オリジナルの namespace を使用する（デフォルト）
   - Use alternate namespace： 代替の namespace を使用する

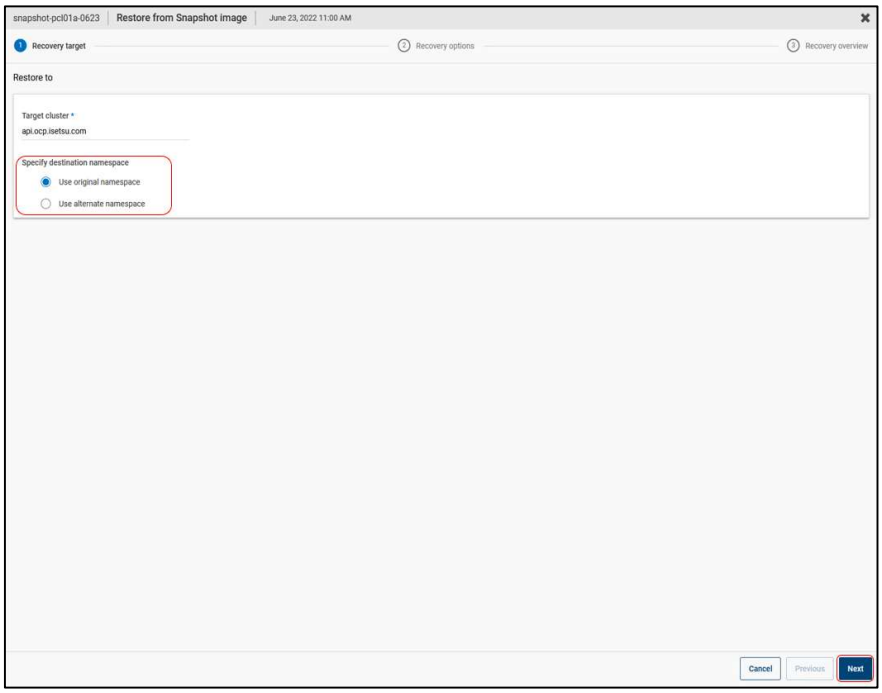

Figure 117. Recovery target

5. [**Recovery options**]ページで以下を選択し[**Next**]をクリックします。

   (a) [**Select resource types to recover**]でリカバリするリソースタイプを選択します。

   - All resource types： すべてのリソースタイプをリカバリします（デフォルト）
   - Recover selected resource types： 選択したリソースタイプをリカバリします

   (b) [**Select Persistent volume claims to recover**]で、すべての Persistent volume claim をリカバリするか、特定の Persistent volume claim をリカバリするか選択します

   - All Persistent volume claims：すべての Persistent volume claim をリカバリします（デフォルト）
   - Recover selected Persistent volume claims: 選択した Persistent volume claim をリカバリします

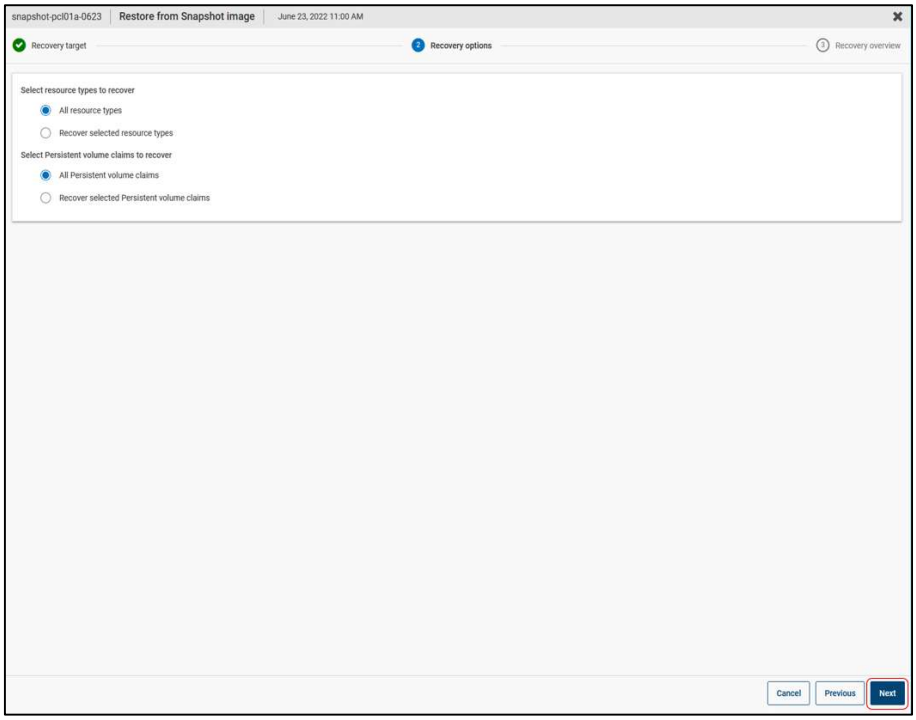

Figure 118. Recovery options

6. [**Recovery overview**]ページで、[**Start recovery**]をクリックしてリカバリエントリをサブミットします。

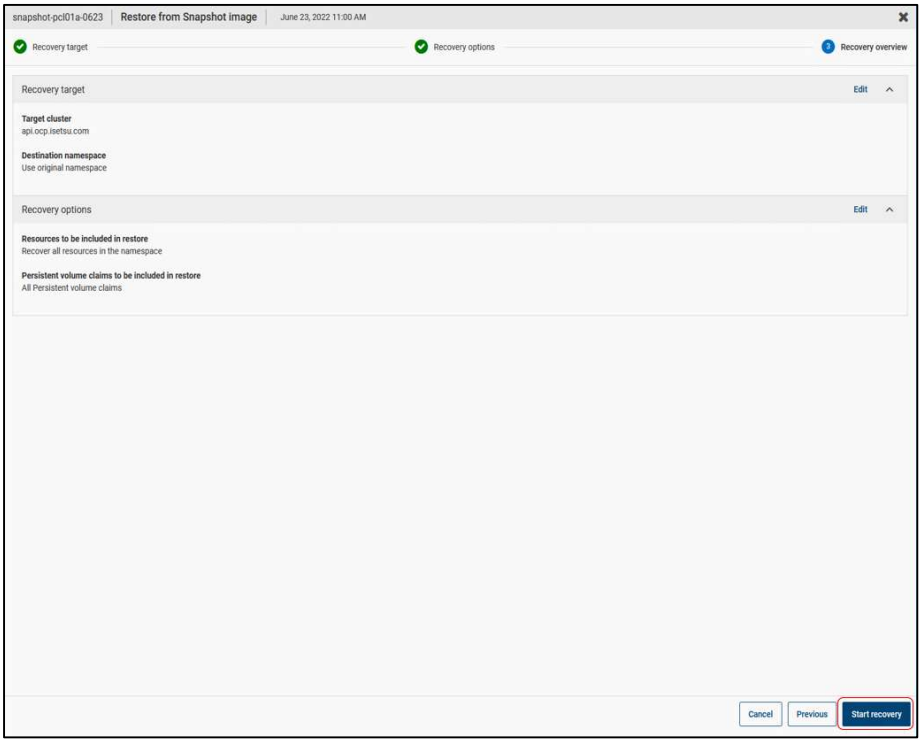

Figure 119. Recovery overview

7. [**Activity Monitor**] > [**Jobs**]タブで Job ID をクリックするとリストアジョブの詳細が表示されます。

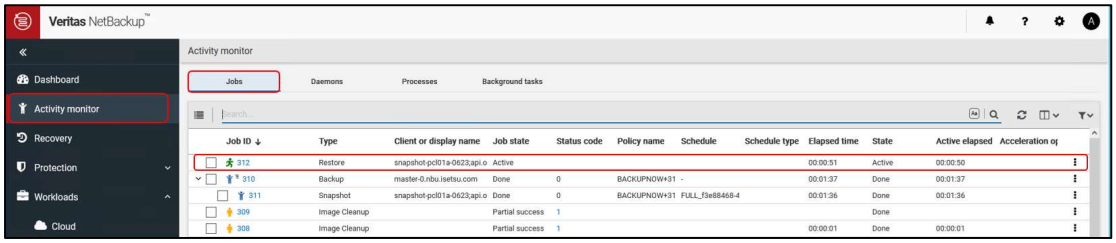

Figure 120. Activity monitor

バックアップからのリストア手順は以上です。

6　注意事項および制限事項

Veritas NetBackup 10、Hitachi Storage Plug-in for Containers、Red Hat OpenShift Container Platform の注意事項および制限事項については、各製品のドキュメントを参照してください。

Veritas NetBackup 10 に関する注意事項および制限事項。

- バックアップコピーからのリストアを行う場合、リストアジョブが"**Partial success**"となることがあります。
  詳細は Veritas NetBackup 10 のドキュメントを参照してください。
- 本検証で使用した Veritas NetBackup 10.0 では、ストレージのパス構成としてはシングルパス構成のみがサポートとなります。
  (Veritas NetBackup 10.0 ではマルチパス構成未サポートのため、本検証ではシングルパス構成で実施)
  但し、後続の Veritas NetBackup リリースでマルチパス構成のサポートが予定されています。
  詳細は Veritas 社にご確認ください。

A1　付録

本付録では、Veritas NetBackup 10.1.1 でサポートされたマルチパス構成の設定方法、および Veritas NetBackup 10.1.1 の設定方法の変更点について説明します。

A1.1　Veritas NetBackup 10.1.1 でのマルチパス構成のサポートについて

Veritas NetBackup 10.1.1 では、StorageClass に新しいラベルが追加されました。この新しいラベルを用いることで、ストレージ接続のマルチパス構成に対応します。
Veritas NetBackup の操作方法及び利用できる機能は、ストレージのパス構成に影響しません。

ストレージ接続のマルチパス構成は、Device Mapper Multipath を用いて実現します。
Device Mapper Multipath の設定方法については、Hitachi Storage Plug-in for Containers ドキュメントである Storage Plug-in for Containers Quick Reference Guide の Overview 内の Multipath settings に関する設定部分を参照してください。
Hitachi Storage Plug-in for Containers ドキュメントページ：
https://knowledge.hitachivantara.com/Documents/Adapters_and_Drivers/Storage_Adapters_and_Drivers/Containers/Storage_Plug-in_for_Containers

A1.2　マルチパス構成のシステム要件

マルチパス構成で、Veritas NetBackup 10.1.1 と Hitachi Storage Plug-in for Containers を用いた Red Hat OpenShift Container Platform における、バックアップシステムを構築するために必要となるハードウェアおよびソフトウェアコンポーネントについて説明します。

A1.2.1 ハードウェアコンポーネント

Veritas NetBackup 10.0 を用いたバックアップシステムを構築するために必要となるハードウェアと同じです。
シングルパス構成ではストレージとの接続経路は 1 つでしたが、マルチパス構成ではストレージとの接続経路が複数経路となるように、ストレージとの接続経路を追加してください。

A1.2.2 ソフトウェアコンポーネント

Veritas NetBackup 10.1.1 を用いたソリューションで必要となるソフトウェアコンポーネントを Table 4 に示します。

Table 4. Required software components for Veritas NetBackup 10.1.1

	Software	Version
Hitachi	Hitachi Storage Virtualization Operating System (SVOS) - Hitachi LUN Manager - Hitachi Dynamic Provisioning	90-08-01 or later (*1) 93-06-01 or later (*2)
	Hitachi Local Replication (Hitachi Thin Image)	
	Hitachi Storage Plug-in for Containers	3.9.0 or later
Red Hat	Red Hat OpenShift Container Platform	4.7 - 4.9
	Red Hat Enterprise Linux CoreOS	7.0 - 7.9, 8.2 - 8.4
Veritas	NetBackup	10.1.1

(*1) : Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H

(*2) : Hitachi Virtual Storage Platform E1090, E1090H, E990, E790, E790H, E590, E590H

A1.3　マルチパス構成での NetBackup によるバックアップの準備

Veritas NetBackup 10.1.1 では、新しい StorageClass のラベルが追加されました。
マルチパス構成に対応するため、使用するラベルを新しい StorageClass のラベルに変更します。

本資料の説明箇所

4 環境構築

┗4.3 NetBackup によるバックアップの準備

┗4.3.3 バックアップおよびリストア操作のための構成設定

┗StorageClass および VolumeSnapshotClass にラベルを追加する

┗手順 2

変更内容

変更 前 ： ***netbackup.veritas.com/default-csi-storage-class=true***

変更 後 ： ***netbackup.veritas.com/default-csi-filesystem-storage-class=true***

A1.4　Veritas NetBackup 10.1.1 設定における変更点

- Veritas NetBackup 10.1.1 の詳細については、製品ドキュメントを参照してください。
  Veritas 社ドキュメント検索ページ： https://sort.veritas.com/documents/

- Veritas NetBackup 10.1.1 では、Kubernetes クラスタの追加時に使用する CA certificate(ca.crt)と Token(token)の確認方法が変更されました。
  これに伴う本資料の変更点を以下に示します。詳細は Veritas NetBackup 10.1.1 の製品ドキュメントを参照してください。

  本資料の説明箇所

4 環境構築
└4.3 NetBackup によるバックアップの準備
└4.3.1 Kubernetes クラスタの追加
├手順 1
└手順 2

手順 1 の変更内容
変更前
次のコマンドを作業用 server で実行し「netbackup-backup-server」サービスアカウントの詳細を確認し、使用している token の secret を確認します。
変更後
手順 2 を実施してください。
Veritas NetBackup 10.0 で実施していたサービスアカウントの詳細確認は不要となりました。

手順 2 の変更内容
変更前
手順 1 で確認した secret 名を指定して次のコマンドを作業用 server で実行し、Secret の詳細出力から CA certificate(ca.crt)と token(token)の値をコピーします。
[実行例] `# oc get secret netbackup-backup-server-token-89521 -o yaml`
変更後
次のコマンドを作業用 server で実行し、Secret の詳細出力から CA certificate(ca.crt)と Token(token)の値をコピーします。
[実行例] `# oc get secret netbackup-backup-server-secret -n netbackup -o yaml`

- Veritas NetBackup 10.1.1 では、BackupServerCert に記載する **clusterName** が変更されました。
これに伴う本資料の変更点を以下に示します。詳細は Veritas NetBackup 10.1.1 の製品ドキュメントを参照してください。

本資料の説明箇所
4 環境構築
└4.3 NetBackup によるバックアップの準備
└4.3.3 バックアップおよびリストア操作のための構成設定
└Secret、ConfigMap および BackupServerCert を作成する
└手順 7

clusterName の変更内容を Table 5. に示します。

Table 5. Version と clusterName の記載内容

Version	clusterName
Veritas NetBackup 10.0 （変更 前）	III. OpenShiftのクラスタ名、ドメイン名
Veritas NetBackup 10.1.1 （変更 後）	III. OpenShiftのクラスタ名、もしくはドメイン名:port番号

Figure 56. の設定例に port 番号を付加した例を Figure 121. に示します。

```
[root@registry-host NBU10-GA]# cat NBU_BackupServerCert.yaml
apiVersion: netbackup.veritas.com/v1
kind: BackupServerCert
metadata:
        name: master-0.nbu.isetsu.com           ← (Ⅰ) BackupServerCert name
        namespace: netbackup                    ← (Ⅱ) Namespace of the NetBackup operator
spec:
        clusterName: api.ocp.isetsu.com:6443    ← (Ⅲ) Cluster name or Domain name of the OpenShift : Port number
        backupServer: master-0.nbu.isetsu.com   ← (Ⅳ) Host name of the NetBackup Master Server
        certificateOperation: Create
        certificateType: NBCA
        nbcaAttributes:
                nbcaCreateOptions:
                        secretName: master-0.nbu.isetsu.com   ← (Ⅴ) Name of secret containing token and fingerprint
[root@registry-host NBU10-GA]#
```

Figure 121. port 番号を付加した BackupServerCert 例