NetBackup™ Web UI Kubernetes 管理者ガイド

リリース 9.1

VERITAS™

最終更新日: 2021-06-28

法的通知と登録商標

Veritas、Veritas ロゴ、NetBackup は、Veritas Technologies LLC または関連会社の米国およびその他の国における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。

この製品には、Veritas 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア (「サードパーティ製プログラム」) が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このVeritas製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

https://www.veritas.com/about/legal/license-agreements

本書に記載されている製品は、その使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されます。Veritas Technologies LLC からの書面による許可なく本書を複製することはできません。

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Veritasがオンプレミスまたはホスト型サービスとして提供するかを問わず、必要に応じて FAR 52.227-19「商用コンピュータソフトウェア - 制限される権利 (Commercial Computer Software - Restricted Rights)」、DFARS 227.7202「商用コンピュータソフトウェアおよび商用コンピュータソフトウェア文書 (Commercial Computer Software and Commercial Computer Software Documentation)」、およびそれらの後継の規制に定める制限される権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

現在のサポート契約についてご不明な点がある場合は、次に示すお住まいの地域のサポート契約管理チームに電子メールでお問い合わせください。

世界共通 (日本を除く)	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が記載されています。最新のマニュアルは、Veritasの Web サイトで入手できます。

https://sort.veritas.com/documents

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

NB.docs@veritas.com

次の Veritas コミュニティサイトでマニュアルの情報を参照したり、質問したりすることもできます。

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas SORT (Service and Operations Readiness Tools) は、特定の時間がかかる管理タスクを自動化および簡素化するための情報とツールを提供するWeb サイトです。製品によって異なりますが、SORT はインストールとアップグレードの準備、データセンターにおけるリスクの識別、および運用効率の向上を支援します。SORT がお客様の製品に提供できるサービスとツールについては、次のデータシートを参照してください。

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目次

1

NetBackup Web ユーザーインターフェースの概要

この章では以下の項目について説明しています。

NetBackup Web UI について

NetBackup Web ユーザーインターフェースは、次の機能を提供します。

- Chrome や Firefox などの Web ブラウザからプライマリサーバーにアクセスする機能。Web UI でサポートされるブラウザについて詳しくは、NetBackup ソフトウェア互換性リストを参照してください。
  NetBackup Web UI は、ブラウザによって動作が変わる場合があります。日付選択などの一部の機能は、一部のブラウザでは利用できないことがあります。こうした違いは、NetBackup の制限によるものではなく、ブラウザの機能によるものです。
- 重要な情報の概要を表示するダッシュボード。
- 役割ベースのアクセス制御 (RBAC) により、管理者は NetBackup へのユーザーアクセスを構成し、作業負荷の保護のタスクを委任できます。
- 資産の保護は、保護計画、ジョブ管理、資産の保護状態の可視性を通じて実現します。
  また、ポリシー管理は、限られた数のポリシー形式でも利用できます。ポリシー形式の詳細を参照できます。

- 作業負荷管理者は、保護計画を作成し、SLO を満たす保護計画に資産をサブスクライブし、保護状態を監視し、資産のセルフサービスリカバリを実行できます。

メモ: NetBackup Web UI は、1280x1024 以上の画面解像度で最適に表示されます。

NetBackup Web UI のアクセス制御

NetBackup では、役割ベースのアクセス制御を使用して Web UI へのアクセス権を付与します。アクセス制御は、役割を通じて実行されます。

- 役割は、ユーザーが実行できる操作と、Web UI でユーザーがアクセスできる機能を定義します。たとえば、作業負荷の資産、保護計画、またはクレデンシャルへのアクセスなどがあります。
- RBAC は、Web UI と API でのみ利用可能です。
  NetBackup のその他のアクセス制御方法は、拡張監査 (EA) を除いて、Web UI と API ではサポートされません。

NetBackup ジョブの監視

NetBackup Web UI を使用すると、管理者はより簡単に NetBackup ジョブの操作を監視し、注意が必要な問題を特定できます。

保護計画: スケジュール、ストレージ、およびストレージオプションを一元的に構成する場所

保護計画には、次の利点があります。

- デフォルトの作業負荷管理者は、資産を保護するために使用する保護計画を選択できます。
- 必要な RBAC 権限を使用して、作業負荷管理者は、使用されているバックアップスケジュールやストレージを含む保護計画を作成して管理できます。
- バックアップのスケジュールに加えて、保護計画には、レプリケーションと長期保持のスケジュールも含めることができます。
- 利用可能なストレージから選択するときに、そのストレージで利用可能な追加機能を確認できます。

セルフサービスリカバリ

NetBackup Web UI を使用すると、作業負荷管理者が、その作業負荷に適用可能な VM、データベース、その他の資産形式を簡単にリカバリできるようになります。

用語

次の表では、Web ユーザーインターフェースの概念と用語について説明します。

表 1-1 Web ユーザーインターフェースの用語および概念

用語	定義
資産グループ	「*インテリジェントグループ*」を参照してください。
資産	物理クライアント、仮想マシン、データベースアプリケーションなどの保護対象データです。
今すぐバックアップ	資産のバックアップをすぐに作成します。NetBackup は、選択した保護計画を使用して資産の完全バックアップを 1 回のみ実行します。このバックアップは、スケジュールバックアップには影響しません。
インテリジェントグループ	指定した条件 (問い合わせ) に基づいて、NetBackup が保護対象資産を自動的に選択することを可能にします。インテリジェントグループは、本番環境の変更が含まれるように、自動的に最新の状態に維持されます。これらのグループは、資産グループとも呼ばれます。 [インテリジェント VM グループ (Intelligent VM groups)]タブまたは[インテリジェントグループ (Intelligent groups)]タブにこれらのグループが表示されます。
保護計画	保護計画は、バックアップを実行するタイミング、バックアップの保持期間、使用するストレージ形式を定義します。保護計画を設定したら、資産を保護計画にサブスクライブできます。
RBAC	役割ベースのアクセス制御です。役割の管理者は、RBAC で設定されている役割を通じて、NetBackup Web UI へのアクセスを委任または制限できます。 注意: RBAC で設定した役割は、NetBackup 管理コンソールまたは CLI へのアクセスを制御しません。
役割	RBAC では、ユーザーが実行できる操作と、ユーザーがアクセスできる資産やオブジェクトを定義します。たとえば、特定のデータベースのリカバリを管理する役割と、バックアップおよびリストアに必要なクレデンシャルを設定できます。
ストレージ	データのバックアップ、レプリケート、または複製 (長期保持用) 対象となるストレージです。
保護計画にサブスクライブする	保護計画にサブスクライブする資産または資産グループを選択する処理です。資産は、保護計画のスケジュールに従って保護されます。Web UI では、*サブスクライブ*を「保護の追加」とも表記します。
保護計画からサブスクライブ解除する	*サブスクライブ解除*は、保護を解除する処理、または計画から資産や資産グループを削除する処理を指します。
作業負荷 (Workload)	資産のタイプです。たとえば、VMware、RHV、AHV、またはクラウドです。

NetBackup Web UI へのサインイン

権限を持つユーザーは、NetBackup Web UI を使用して、NetBackup プライマリサーバーに Web ブラウザからサインインできます。

利用可能なサインインオプションは次のとおりです。

- 「ユーザー名とパスワードでサインインする」
- 「証明書またはスマートカードでサインインする」
- 「シングルサインオン (SSO) でサインインする」

ユーザー名とパスワードでサインインする

認可済みのユーザーのみが NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

ユーザー名とパスワードを使用して NetBackup プライマリサーバーにサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*primaryserver*/webui/login

   primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

2. クレデンシャルを入力して、[サインイン (Sign in)]をクリックします。

   次に例を示します。

ユーザーの種類	使用する形式	例
ローカルユーザー	*username*	jane_doe
Windows ユーザー	*DOMAIN¥username*	WINDOWS¥jane_doe
UNIX ユーザー	*username@domain*	john_doe@unix

証明書またはスマートカードでサインインする

権限を持つユーザーである場合は、スマートカードまたはデジタル証明書を使用して NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

スマートカードにないデジタル証明書を使用するには、まずブラウザの証明書マネージャに証明書をアップロードする必要があります。詳しくはブラウザのマニュアルで手順を参照するか、証明書管理者にお問い合わせください。

証明書またはスマートカードでサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*primaryserver*/webui/login

   primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

2. [証明書またはスマートカードでサインイン (Sign in with certificate or smart card)] をクリックします。
3. ブラウザにプロンプトが表示されたら、証明書を選択します。

シングルサインオン (SSO) でサインインする

NetBackup 環境内で SAML が ID プロバイダとして設定されている場合、シングルサインオン (SSO) オプションを使用して NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

SSO を使用して NetBackup プライマリサーバーにサインインするには

1. Web ブラウザを開き、次の URL に移動します。

   https://*primaryserver*/webui/login

   primaryserver は、サインインする NetBackup プライマリサーバーのホスト名または IP アドレスです。

2. [シングルサインオンでサインイン (Sign in with single sign-on)] をクリックします。
3. 管理者が指示する手順に従ってください。

   以降のログオンでは、NetBackup によって自動的にプライマリサーバーへのサインインが行われます。

NetBackup Web UI からのサインアウト

NetBackup は、24 時間 (ユーザーセッションで許可される最大時間) 後に Web UI からの自動サインアウトを強制的に実行します。その時間が経過すると、NetBackup は再びサインインを要求します。また、使用するサインインオプション (ユーザー名とパスワード、スマートカード、またはシングルサインオン (SSO)) を変更する場合にもサインアウトできます。

NetBackup Web UI からサインアウトするには

- 右上で、プロファイルアイコン、[サインアウト (Sign out)] の順にクリックします。

2

NetBackup の監視

この章では以下の項目について説明しています。

NetBackup ダッシュボード

NetBackup ダッシュボードは、組織内のロールに関連する詳細情報のクイックビューを提供します。

表 2-1 NetBackup ダッシュボード

ダッシュボードウィジェット	説明
ジョブ	実行中のジョブやキューに投入済みのジョブの数、試行されたジョブや完了したジョブの状態などのジョブ情報を一覧表示します。

ジョブの監視

[ジョブ (Jobs)]ノードを使用して、NetBackup 環境のジョブを監視し、特定のジョブの詳細を表示します。

ジョブを監視するには

1 表示するジョブの名前をクリックします。

[概要 (Overview)]タブで、ジョブに関する情報を表示します。

- [ファイルリスト (File List)]には、バックアップイメージに含まれているファイルが表示されます。

- ［状態 (Status)］セクションには、ジョブに関連する状態と状態コードが表示されます。状態コード番号をクリックすると、この状態コードについてのベリタスナレッジベースの情報が表示されます。
  『NetBackup 状態コードリファレンスガイド』を参照してください。

2 ［詳細 (Details)］タブをクリックして、ジョブについて記録された詳細を表示します。ドロップダウンメニューを使用して、エラーの種類によってログをフィルタできます。

p.12 の「ジョブリストのジョブフィルタ」を参照してください。

ジョブリストのジョブフィルタ

特定の状態のジョブを表示するために、ジョブをフィルタできます。たとえば、実行中のジョブまたは一時停止中のジョブをすべて表示できます。

ジョブリストをフィルタするには

1 ［ジョブ (Jobs)］をクリックします。

2 ジョブリストの上にある［フィルタ (Filter)］オプションをクリックします。

3 ［フィルタ (Filter)］ウィンドウでフィルタオプションを選択すると、表示されるジョブが動的に変わります。フィルタオプションは次のとおりです。

- すべて (All)
- 有効 (Active)
- 完了 (Done)
- 失敗 (Failed)
- 未完了 (Incomplete)
- 部分的に成功 (Partially Successful)
- キューへ投入済み (Queued)
- 成功 (Successful)
- 一時停止 (Suspended)
- 再試行を待機中 (Waiting for Retry)

4 ［フィルタの適用 (Apply Filters)］をクリックします。

5 選択したフィルタを解除するには、［すべて消去 (Clear All)］をクリックします。

3

NetBackup for Kubernetes の概要

この章では以下の項目について説明しています。

概要

NetBackup Web UI は、名前空間の形式で、Kubernetes アプリケーションのバックアップとリストアの機能を提供します。Kubernetes クラスタ内の保護可能な資産は NetBackup 環境内で自動的に検出され、管理者は必要なスケジュール、バックアップ、保持の各設定を含む 1 つ以上の保護計画を選択できます。

NetBackup Web UI では、次の操作を実行できます。

- 保護のための Kubernetes クラスタの追加
- 検出された名前空間の表示
- 役割の権限の管理
- リソース制限を設定してネットワークの負荷を最適化
- Kubernetes 資産を保護するための保護計画の選択
- 名前空間と永続ボリュームのリストア
- バックアップおよびリストア操作の監視

Kubernetes 用の NetBackup サポート機能

表 3-1 NetBackup for Kubernetes

機能	説明
NetBackup RBAC (役割ベースのアクセス制御) との統合	NetBackup Web UI は RBAC の役割を提供し、どの NetBackup ユーザーが NetBackup の Kubernetes 操作を管理できるかを制御します。ユーザーは Kubernetes 操作を管理するために NetBackup 管理者である必要はありません。
ライセンス	容量ベースのライセンス
保護計画	次の利点があります。 ■ 単一の保護計画を使用して、複数の Kubernetes 名前空間を保護します。複数のクラスタに資産を分散できます。 ■ 部分的に成功したバックアップを保持または破棄する機能。 ■ Kubernetes 資産を保護するために、Kubernetes コマンドを知る必要はありません。
Kubernetes 資産のインテリジェントな管理	NetBackup は自動的に、Kubernetes クラスタ内の名前空間、永続ボリューム、永続ボリューム要求などを検出します。また、手動検出を実行できます。資産が検出されると、Kubernetes 作業負荷管理者は、資産を保護するために 1 つ以上の保護計画を選択できます。
Kubernetes 固有のクレデンシャル	クラスタの認証と管理に使用する Kubernetes サービスアカウント。
バックアップおよびリストア機能	バックアップとリストアでは次の機能を利用できます。 ■ バックアップとリストアは、NetBackup サーバーによって中央サイトから完全に管理されます。管理者は、さまざまな Kubernetes クラスタで、名前空間の自動的な無人バックアップをスケジュールできます。 ■ NetBackup Web UI は、1 つのインターフェースからの名前空間のバックアップとリストアをサポートします。 ■ 完全バックアップのバックアップスケジュール。 ■ 手動バックアップとスナップショットのみのバックアップ。 ■ Kubernetes 名前空間と永続ボリュームを異なる場所にリストアします。 ■ バックアップのパフォーマンスを向上するための各クラスタのリソースのスロットル。
スナップショットバックアップ	NetBackup はスナップショット方式を使用して Kubernetes 名前空間のバックアップを実行し、リカバリ時間目標を短縮できます。

4

NetBackup Kubernetes Operator の配備と構成

この章では以下の項目について説明しています。

Kubernetes のクラスタの構成

NetBackup™ Kubernetes Operator を配備するには、クラスタを構成する必要があります。Helm Chart を使用して、次の 3 種類のプラットフォームで NetBackup Kubernetes Operator を配備できます。

- Red Hat OpenShift
- GKE (Google Kubernetes Engine)
- VMware Tanzu

NetBackup 用の OpenShift の構成

開始する前に、これらの操作を実行するために必要な権限を OpenShift アカウントに付与していることを確認してください。

OpenShift を構成するには:

- CLI で次のコマンドを使用して、OpenShift OC にログオンします。

  ```
  oc login --token=<TOKEN> --server=<URL>
  ```

  ここで示された文字列については、次のとおりです。

  - <TOKEN>: ログオントークン
  - <URL>: OpenShift サーバーの URL

メモ: OpenShift アカウントにログオンすると、トークンと URL を取得できます。コンソールにログインする OpenShift 管理者アカウントの名前 (ホームページの右上) をクリックし、[ログインコマンドのコピー (Copy Login Command)]オプションをクリックします。表示された新しいページで[トークンの表示 (Display Token)]をクリックしてコマンドを表示します。

このコマンドを実行すると、新しい kubectl コンテキストが `~/.kube/config` ファイルに追加され、この新しいコンテキストが現在の kubectl コンテキストとして設定されます。

NetBackup 用の GKE の構成

構成を開始する前に、これらの操作を実行するために必要な権限を GKE アカウントに付与していることを確認します。

前提条件:

- GKE クラスタのポート番号には、443、6443、または 8443 を使用できます。デフォルトポートは 443 です。追加する前に、正しいセキュアなポート番号を確認します。
- GKE で永続ボリュームまたは永続ボリューム要求を作成するときは、**プロビジョナ**が `kubernetes.io/gce-pd` であるストレージクラスを指定します。

既存のアカウントを使用してログオンするには:

1. 既存のユーザーアカウントを使用して GKE アカウントにログオンするには、次のコマンドを使用します。

   ```
   gcloud auth login <account>
   ```

2. ログオンクレデンシャルは、対話式または非対話式で入力します。

3 すべてのクラスタを一覧表示してクラスタ名を見つけるには、次のコマンドを実行します。

```
gcloud container clusters list
```

出力は次のようになります。

```
NAME                LOCATION       MASTER_VERSION    MASTER_IP

csi-cluster        us-central1-c  1.17.14-gke.400   35.238.135.170

sailor             us-central1-c  1.16.15-gke.6000  35.224.28.128

surens-cluster     us-east1-b     1.17.14-gke.1600  35.231.17.183

bw-kube-cluster-1  us-east1-c     1.16.15-gke.6000  35.196.24.132
```

4 クラスタのクレデンシャルを取得して `.kube/config` に追加するには、次のコマンドを実行します。

```
gcloud container clusters get-credentials <cluster name>
```

例: gcloud container clusters get-credentials bw-kube-cluster-1

または、ログオン専用のクラスタのサービスアカウントを作成して使用できます。

専用サービスアカウントを作成するには:

1 アカウントを作成するには、次のコマンドを実行します。

```
gcloud iam service-accounts create <account name> --display-name
"<account description>"
```

例: gcloud iam service-accounts create veritas-netbackup-k8s-sa --display-name "Veritas NetBackup K8s Service Account"

2 ユーザーを一覧表示するには、次のコマンドを実行します。

```
gcloud iam service-accounts list --filter <email ID>@<project
ID>.gserviceaccount.com
```

例: gcloud iam service-accounts list --filter veritas-netbackup-k8s-sa@projectID.gserviceaccount.com

3 サービスアカウントキーをダウンロードするには、次のコマンドを実行します。

```
gcloud iam service-accounts keys create <key json file name>
--iam-account <e-mail address of the service account>
```

例: gcloud iam service-accounts keys create veritas-netbackup-k8s-sa-key.json --iam-account <サービスアカウントの電子メール ID>

4 役割を関連付けるには、次のコマンドを実行します。

```
gcloud iam roles create <role name> --project <project ID> --file
./<role name>.yaml
```

例: gcloud iam roles create rolename --project projectID --file ./rolename.yaml

5 サービスアカウントを有効にするには、次のコマンドを実行します。

```
gcloud auth activate-service-account --project=<project ID>
--key-file=<key file name>
```

例: gcloud auth activate-service-account --project=<プロジェクト ID>
--key-file=veritas-netbackup-k8s-sa-key.json

6 すべてのクラスタを一覧表示してクラスタ名を見つけるには、次のコマンドを実行します。

```
gcloud container clusters list
```

出力は次のようになります。

```
NAME                LOCATION       MASTER_VERSION    MASTER_IP

csi-cluster        us-central1-c  1.17.14-gke.400   35.238.135.170

sailor             us-central1-c  1.16.15-gke.6000  35.224.28.128

surens-cluster     us-east1-b     1.17.14-gke.1600  35.231.17.183

bw-kube-cluster-1  us-east1-c     1.16.15-gke.6000  35.196.24.132
```

7 クラスタのクレデンシャルを取得して .kube/config に追加するには、次のコマンドを実行します。

```
gcloud container clusters get-credentials <cluster name>
```

例: gcloud container clusters get-credentials bw-kube-cluster-1

NetBackup 用の VMware Tanzu の構成

開始する前に、これらの操作を実行するために必要な権限を Tanzu アカウントに付与していることを確認します。TKG クライアントがインストールされていることを確認します。

ローカルの TKG インスタンスに既存の Tanzu 管理クラスタを追加します。

1 管理クラスタからローカルユーザーのホームディレクトリ ~/ に kube-tkg/config ファイルをコピーします。

2 コマンド chmod 775 ~/.kube-tkg/config を実行します。

3 コマンド `export KUBECONFIG=.kube-tkg/config` を実行します。

4 コンテキストのリストを取得するには、コマンド `tkg get mc` を実行します。出力は次のようになります。

```
  MANAGEMENT-CLUSTER-NAME  CONTEXT-NAME                 STATUS
  tkg-mgmt *               tkg-mgmt-admin@tkg-mgmt     Success
  tkg1-mgmt                tkg1-mgmt-admin@tkg1-mgmt   Success
  tkg2-mgmt                tkg2-mgmt-admin@tkg2-mgmt   Success
```

5 TKG コンテキストに切り替えるには、コマンド `tkg set mc tkg1-mgmt` を実行します。

現在の管理クラスタコンテキストが tkg1-mgmt に切り替えられました。

6 kubectl コンテキストを確認するには、コマンド `kubectl config get-contexts` を実行します。出力は次のようになります。

```
 CURRENT NAME             CLUSTER AUTHINFO   NAMESPACE
tkg1-mgmt-admin@tkg1-mgmt      tkg1-mgmt    tkg1-mgmt-admin
tkg2-mgmt-admin@tkg2-mgmt      tkg2-mgmt    tkg2-mgmt-admin
```

7 ローカル TKG インスタンスの管理クラスタを確認するには、コマンド `tkg get mc` を実行します。出力は次のようになります。

```
[dxxxx@xxxxxxxxx01vm1392 ~]$ tkg get mc
  MANAGEMENT-CLUSTER-NAME  CONTEXT-NAME                 STATUS
  tkg-mgmt                 tkg-mgmt-admin@tkg-mgmt     Success
  tkg1-mgmt *                 tkg1-mgmt-admin@tkg1-mgmt  Success
  tkg2-mgmt                 tkg2-mgmt-admin@tkg2-mgmt   Success
```

8 現在のコンテキストですべてのクラスタを取得するには、コマンド `tkg get clusters` を実行します。出力は次のようになります。

```
 NAME         NAMESPACE  STATUS  CONTROLPLANE  WORKERS  KUBERNETES

  tkg1-cluster1  default  running  3/3        3/3
v1.19.3+vmware.1
  tkg1-cluster2  default  running  3/3        3/3
v1.19.3+vmware.1
  tkg1-cluster3  default  running  3/3        3/3
v1.19.3+vmware.1
```

9 クレデンシャルを kubectl 構成ファイルに追加するには、コマンド tkg get credentials tkg1-cluster1 を実行します。

これにより、作業負荷クラスタ tkg1-cluster1 のクレデンシャルが構成ファイルに保存されます。クラスタにアクセスするには、コマンド kubectl config use-context tkg1-cluster1-admin@tkg1-cluster1 を実行します。

10 kubectl コンテキストに切り替えるには、コマンド kubectl config use-context tkg1-cluster1-admin@tkg1-cluster1 を実行します。

11 kubectl コンテキストを確認するには、コマンド kubectl config get-contexts を実行します。

出力は次のようになります。

```
 CURRENT NAME              CLUSTER AUTHINFO          NAMESPACE
tkg1-cluster1-admin@tkg1-cluster1   tkg1-cluster1
tkg1-cluster1-admin
tkg1-mgmt-admin@tkg1-mgmt           tkg1-mgmt
tkg1-mgmt-admin
tkg2-mgmt-admin@tkg2-mgmt           tkg2-mgmt
tkg2-mgmt-admin
```

これで、tkg1-cluster1 で任意の kubectl コマンドを使用できるようになりました。

配備の前提条件

NetBackup Kubernetes Operator を配備するクラスタに、Velero をダウンロードしてインストールします。

メモ: Velero のサポート対象のバージョンについては、NetBackup ソフトウェア互換性リストを参照してください。Velero のインストールと構成については、Velero のマニュアルを参照してください。

NetBackup Kubernetes Operator の配備

クラスタを構成した後、クラスタに NetBackup Kubernetes Operator を配備できます。NetBackup を使用する各クラスタにオペレータを配備する必要があります。

Helm Chart の構成

Helm Chart を使用して、NetBackup Kubernetes Operator を配備できます。NetBackup Kubernetes Operator 用のチャートを作成できます。Helm Chart とツリー構造のレイアウトを次に示します。

```
netbackupkops-helm-chart
    ├── charts
    ├── Chart.yaml
    ├── templates
    │   └── deployment.yaml
    └── values.yaml
```

NetBackup Kubernetes Operator を配備するには:

1. オペレータサービスパッケージをダウンロードします。
2. ホームディレクトリにパッケージを抽出します。`netbackupkops-helm-chart` フォルダは、ホームディレクトリに存在する必要があります。
3. すべてのクラスタコンテキストを一覧表示するには、コマンド `kubectl config get-contexts` を実行します。
4. オペレータサービスを配備するクラスタに切り替えるには、コマンド `kubectl config use-context <cluster-context-name>` を実行します。
5. 現在のディレクトリをホームディレクトリに変更するには、コマンド `cd ~` を実行します。
6. プライベート Docker レジストリを使用している場合は、この手順の指示に従って、Velero 名前空間に Secret `nb-docker-cred` を作成します。それ以外の場合は、次の手順にスキップします。
   - プライベート Docker レジストリにログオンするには、コマンド `docker login -d <user name> -p <password>` を実行します。
     ログオン後、認証トークンを含む `config.json` ファイルが作成または更新されます。`config.json` ファイルを表示するには、コマンド `cat ~/.docker/config.json` を実行します。
     出力は次のようになります。

```
{
   "auths": {
       "https://index.docker.io/v1/": {
           "auth": "c3R...zE2"
```

```
        }

    }

}
```

- Velero 名前空間で netbackupkops-docker-cred という名前の Secret を作成するには、次のコマンドを実行します。

  ```
  kubectl create secret generic netbackupkops-docker-cred ¥
  --from-file=.dockerconfigjson=.docker/config.json ¥
  --type=kubernetes.io/dockerconfigjson -n velero
  ```

- Velero 名前空間で Secret netbackupkops-docker-cred が作成されたかどうかを確認するには、コマンド kubectl get secrets -n velero を実行します。
- イメージ tar ファイルを使用している場合、Docker キャッシュにイメージをロードして Docker イメージリポジトリにイメージをプッシュするには、次のコマンドを実行します。

  ```
  docker load -i <name of the tar file>
  docker tag <image name:tag of the loaded image>
  <repo-name/image-name:tag-name>
  docker push <repo-name/image-name:tag-name>
  ```

- テキストエディタで netbackupkops-helm-chart/values.yaml ファイルを開き、*manager* セクションの *image* の値を、タグ (*repo-name/image-name:tag-name)* の付いたイメージ名に置き換えて、ファイルを保存します。

7 NetBackup Kubernetes Operator サービスを配備するには、次のコマンドを 1 行で実行します。

```
helm install <release name of the deployment>
./netbackupkops-helm-chart -n <namespace in which NetBackup
operator service will run>
```

例: helm install veritas-netbackupkops ./netbackupkops-helm-chart -n netbackup

- 必要に応じて配備のリリース名を変更できます。
- NetBackup オペレータサービスを実行する名前空間を指定するには、-n オプションが必要です。この名前空間は、Velero を実行する名前空間と同じである必要があります。

8 配備の状態を確認するには、次のコマンドを実行します。

```
helm list -n <namespace in which NetBackup operator service will run>
```

例:

```
helm list -n netbackup
```

9 リリース履歴を確認するには、コマンド `helm history veritas-netbackupkops -n <namespace in which NetBackup operator service will run>` を実行します。

例:

```
helm history veritas-netbackupkops -n netbackup
```

NetBackup Kubernetes Operator の配備のアップグレード

Helm コマンドを使用して、NetBackup Kubernetes Operator の配備をアップグレードできます。

```
helm upgrade <release name> ./<directory of the chart> -n <namespace>
```

例: `helm upgrade veritas-netbackupkops ./nbukops-helm-chart -n netbackup`

NetBackup Kubernetes Operator の配備の削除

必要に応じて、クラスタから NetBackup Kubernetes Operator の配備を削除できます。

NetBackup Kubernetes Operator の配備を削除するには、次のコマンドを実行します。

```
helm uninstall <release name> -n <namespace>
```

例: `helm uninstall veritas-netbackupkops -n netbackup`

NetBackup 側のオペレータの構成

NetBackup 9.1 では、2 つの新しいデフォルトの RBAC の役割が導入されています。

- デフォルトの NetBackup Kubernetes Operator: この役割は、NetBackup Web サービスと通信するため、Kubernetes クラスタで実行するオペレータに必要な権限を提供します。セキュリティ管理者または NetBackup 管理者は、必要なユーザーをこの役割に割り当てることができます。この API キーには、役割の一部として定義された

制限付きのアクセス権が付与されています。API キーと CA 証明書は、Kubernetes クラスタ側の構成に必要です。

メモ: NetBackup CA 証明書をフェッチするには、セキュリティ管理者または NetBackup 管理者にお問い合わせください。

- デフォルトの Kubernetes 管理者: この役割には、NetBackup Web UI と API に必要なすべての権限が付与されています。

Kubernetes 側のオペレータの構成

NetBackup Kubernetes Operator を実行するために Kubernetes クラスタで必要な構成の一部として、Kubernetes の Secret リソースを作成する必要があります。Secret のファイル名は構成済みのプライマリサーバーと同じで、名前空間は NetBackup Kubernetes Operator が実行されている場所と同じである必要があります。NetBackup プライマリサーバーの API キーと CA 証明書は、Kubernetes クラスタ側の構成に必要です。

メモ: NetBackup CA 証明書をフェッチするには、セキュリティ管理者または NetBackup 管理者にお問い合わせください。

Secret の形式は次のとおりです。三角カッコ内で指定されているとおりに値を指定します。

```
apiVersion: v1
kind: Secret
metadata:
  name: <NetBackp primary server host name or IP address.>>
  namespace: <Namespace name where the NetBackup Kubernetes operator
 is deployed>>


type: Opaque
stringData:
  apiKey: <API key of the primary server>>
  caCert: "<CA certificate of the primary server>>"
```

API キーと CA 証明書については、セキュリティ管理者にお問い合わせください。

クラスタを追加するためのトークンの取得

NetBackup に Kubernetes クラスタを追加するには、CA 証明書とトークンが必要です。CA 証明書とトークンを取得するには、Kubernetes クラスタで次のコマンドを実行します。

```
kubectl get secret <[namespace-name]-backup-server-token-<id>> -n
<namespace name> -o yaml
```

注釈フィールドなしでトークンを選択する

CA 証明書のサンプルを次に示します。

```
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSURCakNDQWU2
Z0F3SUJBZ0lCQVRBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VR
WURWUVFERXdwdGFXNXAKYTNWaVpVTkJNQjRYRFRJd01URXhPVEV3
TURZeU1sb1hEVE13TVRFeE9ERXdNRFl5TWxvd0ZURVRNQkVHQTF
VRQpBeE1LYldsdWFXdDFZbVZEUVRDQ0FTSXdEUVlKS29aSWh2Y05
BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTklaClduc0MvTEpjaUV
NOGx0ZnU0dzFPcmNaeTVZemhOTXoxQWV0V09xRmUrQ0VxblFVY3h
mVEpwOElWMFRTei9yYmYKSHVBdWlmWTd2ZGxNdC9zREJUbDlIMGF
xUkxLdG9KMDZaUHVBRzN0WjA5Nm1VUzV5bXYzRktWV2kvaVMyYz
I0ZQpFc2NENTBRaTRyYUM5YTlHK1NuSWVRNXYrQzZGUU9vYnBuS
ERXOTNIMlRpK3gyaEMrTHVoSndVVlRldG1EbzkyCktHendENU5OU
kV0L1FPYnVtaTN0QnFPMTdpSThua2xwb0tBd0RYQWlYd2ZjeFpQ
RXNrKytkajRBNVo2bWFGRHMKMUxxVkQ3ZFpkYk1vM08rTDJ6bzB
KdFIzWXYzenY3L0tYM0JDVmdzQWduQWdNeWJUYWMyenRRYzhsWH
hwLzZxcAowbTRPT0h0ME1KYnRSMmo4bWJrQ0F3RUFBYU5oTUY4d
0RnWURWUjBQQVFIL0JBUURBZ0trTUIwR0ExVWRKUVFXCk1CUUdD
Q3NHQVFVRkJ3TUNCZ2dyQmdFRkJRY0RBVEFQQmdOVkhSTUJBZjh
FQlRBREFRSC9NQjBHQTFVZERnUVcKQkJSUkVNM3JxQjhFTjRJW
FFiQ3RJd2hhb3hzeW1EQU5CZ2txaGtpRzl3MEJBUXNGQUFPQ0F
RRUFsY2ZURGNObwpoZi9EM3BQYmx6V3BXUm5xbUc2aTF5eG0wT
2V3OUJWMjhVeDc0S1ppcGEvUm5valpaVDlRdmwvcmg3YW5rRHd
NCllDSlVsZUNHVWJkc1dwRHpycFlqa0lJVlMybHkxeHpUWkNLY0
FWOENEWWkzdjdHdWswR2R2SXc0VENndk5XajIKanBDbC9QWkFp
ZUFXdTlYL2R4THU1S01FN05uTnlGNWx4Uy85cTVvMkRUSS8reD
RncEQwQ09rQVl3SDZ4SzViUgp2WGNabFJ3NmNlMWlTZG43dVE1
V1dxcU50ZEQ1MHRNRHlzWERqUzI4WVh6WjlRYThkMEVnR1E1dW
JMZnZZdzJkCm9xcmZIZjN6bitYajNFVUg0eXROORkdOc1hMN0t4
NVdtNjNjTGlrSzBLV1dOQjMwdVpsVEljUXIyenQ2MGFjK28KbC9
0dFhsUWdoaGUwaFE9PQotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==
```

サンプルトークンを次に示します。

ZXlKaGJHY2lPaUpTVXpJMU5pSXNJbXRwWkNJNkluRjZNMUl5UlR
reWJVSmFkbTFqV1Zaa1FtNVNkbkZwWjFSSWIzWmpTa1ZhWm5KSV
NVSnBRVEJUWVhjaWZRLmV5SnBjM01pT2lKcmRXSmxjbTVsZEdW
ekwzTmxjblpwWTJWaFkyTnZkVzUwSWl3aWEzVmlaWEp1WlhSbGN
5NXBieTl6WlhKMmFXTmxZV05qYjNWdWRDOXVZVzFsYzNCaFkyVW
lPaUoyWld4bGNtOGlMQ0pyZFdKbGNtNWxkR1Z6TG1sdkwzTmxjbl
pwWTJWaFkyTnZkVzUwTDNObFkzSmxkQzV1WVcxbElqb2lkbVZz
WlhKdkxXSmhZMnQxY0MxelpYSjJaWEl0ZEc5clpXNHRhSEpqT0
cwaUxDSnJkV0psY201bGRHVnpMbWx2TDNObGNuWnBZMlZoWTJOd
mRXNTBMM05sY25acFkyVXRZV05qYjNWdWRDNXVZVzFsSWpvaWRt
VnNaWEp2TFdKaFkydDFjQzF6WlhKMlpYSWlMQ0pyZFdKbGNtNWx
kR1Z6TG1sdkwzTmxjblpwWTJWaFkyTnZkVzUwTDNObGNuWnBZMl
V0WVdOamIzVnVkQzUxYVdRaU9pSTFNVEptWldNd09DMWlaRFV5T
FRRd01HRXRZV1V3TWkwMlpUbGpaVGhpWmpObE1Ea2lMQ0p6ZFdJ
aU9pSnplWE4wWlcwNmMyVnlkbWxqWldGalkyOTFiblE2ZG1Wc1p
YSnZPblpsYkdWeWJ5MWlZV05yZFhBdGMyVnlkbVZ5SW4wLnFEWm
t2bDNmSHlabTQzNUQyakZGX2Q5MlA2RkdFb1R0Mmx2V1J6RGR5V
GItYngxSnZ3S25Wa1M0MGswRF9jeGlMcEx5X3liNGVqelZJM2dz
UG0xM0hJUlV2bWhiSEZaUzhlX0FvOTdnbGhOd3VpQlhncjRjNW0
3dUd3eGVKOWs4eERWazVhUVhUalM4cWJlMHB4QXhpVG9EOUt4aF
BtMTVoNy1EaUtjbHBlZEJkZ2N1V2JHenRuci1uXzAzYUFFbkY3Y
zU2c1Z5N1VrV2ZUQXZMZXBZUG9jZkJoRjY3cUR4eEMza2d0S2U4
SnJUNlItclgxYWRnQVhnRnJ5WDJYNGM0RUI3WE14NFd6SFMzQXR
RdEFqNno3eEVMNXQ4eHlQZ1EtMnlpeGJudzVUTXVac1JLcnZyak
1OX2FxUTRDTEJlM29BWEVXaEdJaW1uaXgydkdpNVVVdw==

期限切れのイメージについて

期限切れの Kubernetes イメージが占有するストレージ領域を再生利用するため、NetBackup は `deletebackuprequest` カスタムリソースを作成し、削除要求を送信します。ただし、NetBackup は削除が完了するまで待機したり、削除要求の状態を追跡したりはしません。Velero が削除要求を受け入れ、削除を実行します。

Kubernetes クラスタ内の `deletebackuprequest.velero.io` CR を一覧表示すると、削除要求の進行状況を追跡できます。Velero バックアップを削除すると、`deletebackuprequest` CR も削除されます。

メモ: イメージの手動での期限切れは、CLI と API でのみサポートされます。Web UI と Java UI ではサポートされません。

5

Kubernetes 資産の管理

この章では以下の項目について説明しています。

Kubernetes クラスタの追加

NetBackup に Kubernetes クラスタを追加し、クラスタ内のすべての資産を自動的に検出できます。クラスタを追加した後に資産の検出を実行するには、オペレータの構成をクラスタに追加する必要があります。

p.24 の「Kubernetes 側のオペレータの構成」を参照してください。

クラスタを追加するには

1. 左側の[作業負荷 (Workloads)]で、[Kubernetes]をクリックします。
2. [Kubernetes クラスタ (Kubernetes clusters)]タブをクリックし、[追加 (Add)]をクリックします。
3. [Kubernetes クラスタの追加 (Add Kubernetes cluster)]ページで、次を入力します。
   - [クラスタ名 (Cluster name)]: クラスタの名前を入力します。この名前は DNS の解決可能な値または IP アドレスである必要があります。
   - [ポート (Port)]: Kubernetes API サーバーのポート番号を入力します。
   - [コントローラの名前空間 (Controller namespace)]: Kubernetes クラスタ内で NetBackup Kubernetes Operator が配備されている名前空間を入力します。
4. [次へ (Next)]をクリックします。[クレデンシャルの管理 (Manage credentials)]ページで、クラスタにクレデンシャルを追加できます。

- 既存のクレデンシャルを使用するには、[既存のクレデンシャルから選択してください (Select from existing credentials)]を選択し、[次へ (Next)]をクリックします次のページで、必要なクレデンシャルを選択し、[次へ (Next)]をクリックします。
- 新しいクレデンシャルを作成するには、[クレデンシャルの追加 (Add credential)]をクリックし、[次へ (Next)]をクリックします。[クレデンシャルの管理 (Manage credentials)]ページで、次を入力します。
  - [クレデンシャル名 (Credential name)]: クレデンシャルの名前を入力します。
  - [タグ (Tag)]: クレデンシャルに関連付けるタグを入力します。
  - [説明 (Description)]: クレデンシャルの説明を入力します。
  - [トークン (Token)]: 認証トークンの値を Base64 エンコード形式で入力します。
    p.25 の「クラスタを追加するためのトークンの取得」を参照してください。
  - [CA 証明書 (CA certificate)]: CA 証明書ファイルの内容を指定します。
    p.25 の「クラスタを追加するためのトークンの取得」を参照してください。

5 [次へ (Next)]をクリックします。

クレデンシャルが検証され、検証に成功すると、クラスタが追加されます。クラスタが追加されると、自動検出が実行され、クラスタ内の利用可能な資産が検出されます。

設定の構成

Kubernetes の設定では、Kubernetes の配備のさまざまな側面を構成できます。

Kubernetes のリソース制限の設定

この設定によって、Kubernetes クラスタで同時に実行できるバックアップの数を制御できます。たとえば、20 の資産を保護し、制限を 5 に設定している場合、5 つの資産のみ同時にバックアップを実行でき、残りの 15 の資産はキューに入ります。最初の 5 つの資産のうち 1 つのバックアップが完了すると、キューの資産にバックアップの順番が回ります。

このリソース制限のデフォルト値は 1 です。これは、クラスタごとに 1 つのバックアップジョブのみが進行中になり、残りの資産はキューに投入された状態になることを示します。

システムとネットワークリソースの使用を最適化するため、この設定を構成することをお勧めします。この設定は、選択しているプライマリサーバーのすべての Kubernetes バックアップに適用されます。

リソース制限を設定するには

1. 左側で[作業負荷 (Workloads)]、[Kubernetes]の順にクリックします。
2. 右上で[Kubernetes 設定 (Kubernetes settings)]、[リソース制限 (Resource limits)]の順にクリックします。
3. [Kubernetes クラスタあたりのバックアップジョブ (Backup jobs per Kubernetes cluster)]の横にある[編集 (Edit)]をクリックします。
4. [Kubernetes クラスタの編集 (Edit Kubernetes cluster)]ダイアログで、次の操作を行います。
   - [グローバル (Global)]フィールドに値を入力し、すべてのクラスタのグローバル制限を設定します。この制限は、クラスタで同時に実行されるバックアップジョブの数を示します。
   - そのクラスタのグローバル制限を上書きする個別の制限をクラスタに追加できます。クラスタに個々の制限を設定するには、[追加 (Add)]をクリックします。
   - リストからクラスタを選択し、制限の値を入力します。配備されている利用可能な各クラスタに制限を追加できます。
   - [保存 (Save)]をクリックして、変更を保存します。

自動検出の間隔の構成

自動検出により、クラスタ内で NetBackup によって保護される資産数が記録されます。この設定を使用すると、NetBackup が自動検出を実行して、クラスタ内の新しい資産を特定し、クラスタから排除または削除された資産の数を収集する間隔を設定できます。

指定できる値は、5 分から 1 年の間です。デフォルト値は 30 分です。

自動検出の間隔を設定するには

1. 左側で[作業負荷 (Workloads)]、[Kubernetes]の順にクリックします。
2. 右上で[Kubernetes 設定 (Kubernetes settings)]、[自動検出 (Autodiscovery)]の順にクリックします。
3. [間隔 (Frequency)]の近くにある[編集 (Edit)]をクリックします。
4. NetBackup が自動検出を実行した後の時間数を入力します。[保存 (Save)]をクリックします。

権限の構成

管理権限を使用して、ユーザーロールに異なるアクセス権を割り当てることができます。詳しくは、『NetBackup Web UI 管理者ガイド』の「役割ベースのアクセス制御の管理」の章を参照してください。

Kubernetes 資産の管理

[名前空間 (Namespaces)]タブ ([作業負荷 (Workloads)]、[Kubernetes]) を使用して、Kubernetes クラスタ内の資産の監視、保護状態の確認、保護されていない資産への保護の追加を簡単に行えます。また、[今すぐバックアップ (Backup now)]機能を使用して資産のクイックバックアップを作成できます。この機能は、スケジュール設定されたバックアップに影響を与えることなく、選択した資産のワンタイムバックアップを作成します。

[名前空間 (Namespaces)]タブに、NetBackup によって保護できる検出済みの Kubernetes 資産がすべて表示されます。このタブには、次の情報が表示されます。

- [名前空間 (Namespaces)]: 資産の表示名。
- [クラスタ (Cluster)]: 資産が属するクラスタ。
- [保護計画名 (Protected by)]: 資産に適用された保護計画の名前。
- [最後に成功したバックアップ (Last successful backup)]: 資産のバックアップが最後に成功した日時。

[名前空間 (Namespaces)]タブで次の操作を実行できます。

保護されていない資産に保護を追加するには

1. 左側で[作業負荷 (Workloads)]、[Kubernetes]の順にクリックします。
2. 資産の行でオプションを選択します。右上の[保護の追加 (Add protection)]をクリックします。または、資産の行の[処理 (Actions)]メニューをクリックして、[保護の追加 (Add protection)]をクリックします。
3. リストから保護計画を選択し、[次へ (Next)]をクリックします。次のページで、[保護 (Protect)]をクリックします。

資産をすばやくバックアップするには

1. 資産の行でオプションを選択し、右上の[今すぐバックアップ (Backup now)]をクリックします。または、資産の行の[処理 (Actions)]メニューをクリックして、[今すぐバックアップ (Backup now)]をクリックします。
2. 次のページで、
   - すでに保護されている資産をバックアップする場合は、資産がすでにサブスクライブされている計画のリストから保護計画を選択し、[バックアップの開始 (Start backup)]をクリックします。
   - 保護されていない資産をバックアップする場合は、その資産で利用可能な計画から保護計画を選択し、[バックアップの開始 (Start backup)]をクリックします。

6

Kubernetes 資産の保護

この章では以下の項目について説明しています。

Kubernetes 保護計画

他の NetBackup の作業負荷と同様に、Kubernetes の作業負荷を保護するには保護計画を作成する必要があります。Kubernetes の保護計画:

- 保護計画でストレージを指定する必要はありません。
- 完全バックアップスケジュールのみをサポートします。

Kubernetes 保護計画のバックアップオプションの構成

Kubernetes 保護計画を使用すると、部分的に成功したバックアップを識別し、必要に応じてそれらを保持または破棄できます。部分的に成功したバックアップでは、バックアップする予定のすべてのリソースが正常にバックアップされているとはかぎりません。このようなバックアップを保持するか破棄するかを判断し、各保護計画に対して個別にこの指定を行います。

保護計画の作成方法について詳しくは、『NetBackup Web UI 管理者ガイド』の「保護計画の管理」のセクションを参照してください。

Kubernetes で保護計画を構成する際にバックアップオプションを構成するには、[バックアップオプション (Backup options)]ページで、[いずれかのリソースの保護に失敗した場合、バックアップジョブを失敗にします (Fail a backup job, if any of the resources fail to get protected)]オプションを選択します。この設定により、部分的に成功したバックアップジョブは破棄されます。

7

Kubernetes 資産のリカバリ

この章では以下の項目について説明しています。

Kubernetes 資産のリカバリ

NetBackup を使用して、Kubernetes 名前空間と永続ボリュームをリカバリできます。

メモ: NetBackup 9.1 では、永続ボリュームの排他的なリカバリは GCP (Google Cloud Platform) 用の Velero プラグインでのみサポートされます。

メモ: リカバリ後、新しく作成された名前空間、永続ボリューム、その他のリソースには、新しいシステム生成 UID が割り当てられます。

名前空間をリカバリするには

1. 左側の[作業負荷 (Workloads)]で、[Kubernetes]をクリックします。
2. [名前空間 (Namespaces)]タブで、リカバリする資産の名前空間をクリックします。[リカバリポイント (Recovery points)]タブをクリックします。
3. [リカバリポイント (Recovery points)]タブには、すべてのリカバリポイントがバックアップの日時とともに表示されます。フィルタを設定して、表示されたリカバリポイントをフィルタ処理できます。[日付 (Date)]列の日付をクリックすると、リカバリポイントの詳細が表示されます。[リカバリポイントの詳細 (Recovery points details)]ダイアログには、ConfigMap、名前空間、Secret、永続ボリューム、リカバリ、ポッドなど、バックアップされたリソースが表示されます。これらのリソースについて詳しくは、https://kubernetes.io/docs/reference/kubernetes-api/workload-resources/ を参照してください。

4 リカバリするリカバリポイントの行にある省略記号メニュー (3 つのドット) をクリックします。名前空間をリカバリするには、[名前空間のリストア (Restore namespace)]をクリックします。

5 [リカバリターゲット (Recovery target)]ページで、資産を同じソースクラスタにリカバリするには、[次へ (Next)]をクリックします。代替クラスタにリカバリするには、[クラスタの選択 (Select cluster)]をクリックします。[クラスタの選択 (Select cluster)]ダイアログでターゲットクラスタを選択し、[選択 (Select)]をクリックします。[次へ (Next)]をクリックします。

メモ: 元のクラスタと異なるターゲットクラスタを選択する場合は、両方のクラスタ上の Velero プラグインで使用されるオブジェクトストレージが同じである必要があります。

6 [リカバリオプション (Recovery options)]ページで、次の操作を行います。

- 元の名前空間にリカバリするには、[元の名前空間を使用 (Use original namespace)]を選択します。資産を代替名前空間にリストアするには、[代替名前空間を使用 (Use alternate namespace)]を選択し、新しい名前空間の名前を入力します。この名前は、Kubernetes の仕様に従う必要があります。
- 同じ名前空間がすでに存在する場合でもリストアを許可するには、[名前空間がすでに存在する場合はリストアを続行 (Proceed with restore if namespace already exists)]を選択します。このオプションは、既存の名前空間で不足しているリソースをリストアするために役立ちます。クラスタ内の資産でリソースが不足しており、バックアップコピーに同じリソースが存在する場合、このオプションを使用して資産内の不足しているリソースをリストアできます。このオプションでは、資産内の既存のリソースが上書きされるのではなく、不足しているリソースのみがリストアされます。
- 資産内のすべてのリソースをリストアするには、[すべてのリソースをリカバリ (Recover all resources)]を選択します。選択したリソース形式の資産をリストアするには、[リソース形式を選択 (Select resource types)]、リカバリするリソース形式の順に選択します。個々のリソースまたはインスタンスはリストアできません。リソースの形式を選択する必要があり、これには個々のリソースまたはインスタンスが多数含まれる可能性があります。

メモ: [リソース形式を選択 (Select resource types)]オプションは、上級ユーザー向けです。リストアするリソースの選択に注意しないと、リストア後に完全に機能する名前空間が得られない場合があります。

7 [次へ (Next)]をクリックします。

8 [リカバリの概要 (Recovery overview)]ページで、選択したすべてのリカバリオプションを確認します。前に戻って設定を変更するには、[前へ (Previous)]をクリックします。すべてのパラメータを変更したら、[リカバリの開始 (Start recovery)]をクリックします。

永続ボリュームをリカバリするには

1 前述の手順 1 から 3 を実行します。

2 リカバリするリカバリポイントの行にある省略記号メニュー (3 つのドット) をクリックします。永続ボリュームをリカバリするには、[永続ボリュームのリストア (Restore persistent volumes)]をクリックします。

3 [リカバリターゲット (Recovery target)]ページで、永続ボリュームを同じソースクラスタにリカバリするには、[次へ (Next)]をクリックします。代替クラスタにリカバリするには、[クラスタの選択 (Select cluster)]をクリックします。[クラスタの選択 (Select cluster)]ダイアログでターゲットクラスタを選択し、[選択 (Select)]をクリックします。[次へ (Next)]をクリックします。

メモ: 元のクラスタと異なるターゲットクラスタを選択する場合は、両方のクラスタ上の Velero プラグインで使用されるオブジェクトストレージが同じである必要があります。

---

4 [リカバリオプション (Recovery options)]ページで、次のいずれかの操作を行います。

- 元の名前空間にリカバリするには、[元の名前空間を使用 (Use original namespace)]を選択します。同じ名前空間がすでに存在する場合でもリストアを許可するには、[名前空間がすでに存在する場合はリストアを続行 (Proceed with restore if namespace already exists)]を選択します。このオプションは、既存の名前空間で不足している永続ボリュームをリストアするために役立ちます。クラスタ内の資産で永続ボリュームが不足しており、バックアップコピーに同じ永続ボリュームが存在する場合は、このオプションを使用して資産内の不足している永続ボリュームをリストアできます。このオプションでは、資産内の既存の永続ボリュームが上書きされるのではなく、不足している永続ボリュームのみがリストアされます。
- 一意のシステム生成名前空間を使用する場合は、[一時的なシステム生成の名前空間を使用 (Use temporary system generated namespace)]を選択します。この名前空間は、リストア操作の完了後に削除されます。名前空間ではなく、永続ボリュームのデータのリストアを優先する場合は、このオプションを使用します。

5 ［次へ (Next)］をクリックします。

6 ［リカバリの概要 (Recovery overview)］ページで、選択したすべてのリカバリオプションを確認します。設定を修正するには、そのオプションの［編集 (Edit)］か、［前へ (Previous)］をクリックします。すべてのパラメータが正しい場合は、［リカバリの開始 (Start recovery)］をクリックします。

8

Kubernetes の問題のトラブルシューティング

この章では以下の項目について説明しています。

短縮ホスト名を使用したプライマリサーバーへの接続

NetBackup プライマリサーバーは、NetBackup Kubernetes Operator から到達できる必要があります。NetBackup プライマリサーバー名には FQDN または短縮ホスト名を指定できますが、NetBackup Kubernetes Operator でこの名前を解決できる必要があります。

Velero コントローラマネージャの配備で hostAliases を使用して、NetBackup Kubernetes Operator から短縮ホスト名で NetBackup プライマリサーバーに到達させることができます。

```
hostAliases:
- hostnames:
  - falcon
    ip: 10.x.x.x
```

クラスタ検出の失敗

Discovery Reconciler (NetBackup Kubernetes Operator) が、資産のデータを NetBackup に送信します。オペレータがこのタスクを実行するには、Secret ファイル内に API キーと caCert が存在する必要があります。

推奨処置:

- NetBackup Kubernetes Operator が配備されている名前空間に、NetBackup プライマリサーバー名と同じ名前の Secret が存在することを確認します。
- NetBackup Kubernetes Operator ポッドと同じ名前空間に Secret ファイルが存在することを確認します。
- API キーと CA 証明書が有効であることを確認します。

バックアップ中のエラー: 名前空間が削除用にマークされました (Namespace has been marked for deletion)

このエラーは、バックアップの作成を試行した名前空間が、Kubernetes クラスタから削除されていた場合に表示されます。また、NetBackup 資産サービスが資産データベースからその資産を削除します。しかし、その名前空間で利用可能なバックアップが存在していた場合、資産サービスは資産を削除せず、削除済みのマークを付けます。この場合、そのような資産または名前空間のバックアップを作成する必要はありません。

推奨処置: 名前空間がクラスタに存在するかどうかを確認します。

リストア中のエラー: ジョブの最終状態で一部が失敗しています (Final job status is partially failed)

ジョブの最終状態で一部が失敗しており、リソース RoleBinding に固有の警告がいくつか表示されます。

これらの警告は、API グループの認可用のリソース RoleBinding に固有です。RoleBinding はコントローラによって自動的に管理され、新しい名前空間を作成するときに作成されるため、`openshift.io` と `rbac.authorization.Kubernetes.io` がスローされます。

推奨処置: 関連する RoleBinding リソースをリストアから除外すると、これらの警告を回避できます。

バックアップが進行中状態でスタックする

シナリオ 1: これは、バックアップジョブの実行中に、Kubernetes クラスタで実行中の Velero ポッドが再起動した場合に発生します。

推奨処置:

ジョブが動作しなくなった、または動作が遅いかどうかを識別するには、Velero のマニュアルに記載された手順に従います。詳しくは、Velero のマニュアルを参照してください。NetBackup バックアップ (「backups.netbackup.veritas.com」) CRD ジョブと Velero バックアップ (「backups.velero.io」) CRD ジョブを削除します。

シナリオ 2: スナップショットが *UploadFailed* 状態にあるか、アップロードが失敗し、アップロードジョブが再試行される可能性があります。

推奨処置:

`datamanager` のログ (処理ノード上) とバックアップドライバのログを参照して、アップロードエラーの根本原因を特定し、問題の原因を確認します。NetBackup ジョブを有効にするには、NetBackup バックアップ CR (「backups.netbackup.veritas.com」) を削除します。これによりバックアップジョブは失敗とマークされます。また、対応する Velero バックアップジョブ (「backups.velero.io」)、スナップショットジョブ (「snapshots.backupdriver.cnsdp.vmware.com」) およびアップロードジョブ (「uploads.datamover.cnsdp.vmware.com」) を消去します。

リストアが進行中状態でスタックする

この問題は、リストアジョブの実行中に、Kubernetes クラスタで実行中の Velero ポッド機能が再起動した場合に発生します。

推奨処置:

vSphere 用の Velero プラグインの場合:

リストアに永続ボリュームが含まれる場合、リストアジョブに対応する CloneFromSnapshot (「clonefromsnapshots.backupdriver.cnsdp.vmware.com」) CRD の状態を確認します。ダウンロードの要求 (「downloads.datamover.cnsdp.vmware.com」) が失敗した場合、オブジェクトストアのアクセスまたはリストア先の名前空間に問題がある可能性があります。名前空間に、同じ名前の既存の永続ボリューム要求がすでに含まれている可能性があります。NetBackup リストア (「restores.netbackup.veritas.com」) CRD ジョブと、Velero リストア (「restores.velero.io」) CRD ジョブを、対応する clonefromsnapshots CRD とともに削除します (該当する場合)。対応するデータムーバーダウンロード (「downloads.datamover.cnsdp.vmware.com」) CRD の削除は省略可能です。

GCP 用の Velero プラグインの場合:

NetBackup リストア (「restores.netbackup.veritas.com」) CRD ジョブと、Velero リストア (「restores.velero.io」) CRD ジョブを削除します。任意で、ダウンロード (「downloadrequests.velero.io」) CRD を削除します。