NetBackup™ for OpenStack 管理者ガイド

リリース 10.3

VERITAS™

NetBackup™ for OpenStack 管理者ガイド

マニュアルバージョン: 2.7.1

法的通知と登録商標

Veritas、Veritas ロゴは、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、サードパーティの所有物であることをベリタスが示す必要のあるサードパーティソフトウェア(「サードパーティプログラム」)が含まれている場合があります。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。このベリタス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 は、この文書の供給、履行、または使用に関連して付随的または間接的に起こる損害に対して責任を負いません。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、ベリタスがオンプレミスサービスまたはホスト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。テクニカルサポートの主な役割は、製品の特徴や機能に関する具体的な問い合わせに対応することです。テクニカルサポートグループは、オンラインナレッジベースのコンテンツも作成します。テクニカルサポートグループは、その他の部門と連携して、迅速にお客様の質問に回答します。

ベリタスが提供しているメンテナンスには、次のものが含まれます。

- 任意のサイズの組織に合わせた適切な量のサービスを選択できる柔軟性を備えた幅広いサポートオプション
- 迅速な応答と最新の情報を提供する、電話および/または Web によるサポート
- ソフトウェアアップグレードを配信するアップグレード保証
- 各地域の営業時間、または年中無休の 24 時間体制のグローバルサポートを購入可能
- Account Management Services を含むプレミアムサービスの提供

ベリタスが提供しているメンテナンスについて詳しくは、次の URL の Web サイトを参照してください。

www.veritas.com/support

すべてのサポートサービスは、お客様のサポート契約およびその時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。

テクニカルサポートへの連絡

現在サポート契約のあるお客様は、次の URL でテクニカルサポートの情報にアクセスすることができます。

www.veritas.com/support

テクニカルサポートを連絡する前に、製品マニュアルに記載されているシステムの必要条件を満たしていることを確認してください。また、問題の再現が必要な場合に備え、問題が起きたコンピュータの前にいるようにしてください。

テクニカルサポートに連絡するときは、次の情報を用意してください。

- 製品のリリースレベル
- ハードウェア情報
- 利用可能なメモリ、ディスク領域、NIC 情報
- オペレーティングシステム
- バージョンとパッチレベル

- ネットワークトポロジー
- ルーター、ゲートウェイ、IP アドレス情報
- 問題の説明:
  - エラーメッセージとログファイル
  - テクニカルサポートに連絡する前に実行したトラブルシューティング
  - 最近のソフトウェア構成の変更とネットワークの変更

ライセンスと登録

製品で登録またはライセンスキーが必要になる場合は、次の URL にあるテクニカルサポート Web ページにアクセスしてください。

www.veritas.com/support

カスタマサービス

カスタマサービスの情報は次の URL で入手可能です。

www.veritas.com/support

カスタマサービスを利用すると、次の問題のような非技術的な疑問に役立ちます。

- 製品のライセンスまたはシリアル化に関する疑問
- アドレス変更または名義変更のような製品登録の更新
- 製品の概要情報 (機能、利用可能な言語、販売窓口)
- 製品の更新とアップグレードについての最新情報
- アップグレード保証とサポート契約についての情報
- テクニカルサポートオプションについての助言
- 特別販売に関する非技術的な疑問
- CD-ROM、DVD、またはマニュアルに関連する問題

サポート契約のリソース

既存のサポート契約に関してベリタスに問い合わせる場合は、次に示す地域のサポート契約管理チームに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

目次

1

概要

この章では以下の項目について説明しています。

NetBackup for OpenStack について

Veritas NetBackup for OpenStack は、OpenStack 作業負荷に対してポリシーベースの包括的なバックアップとリカバリを提供するネイティブの OpenStack サービスです。このソリューションは、ある時点の作業負荷 (環境のアプリケーション、OS、計算、ネットワーク、構成、データ、およびメタデータ) を完全スナップショットまたは増分スナップショットとしてキャプチャします。これらのスナップショットは、NFS AWS S3 と互換性のあるストレージを含むさまざまなストレージ環境で保持できます。NetBackup for OpenStack とそのワンクリックリカバリを使用すると、組織は RTO (リカバリ時間目標) と RPO (リカバリポイント目標) を改善できます。NetBackup for OpenStack を使用すると、IT 部門は OpenStack ソリューションを完全に配備し、データの保持、保護、および整合性を拡張してビジネスの信頼性を高めることができます。

企業の IT 部門とクラウドサービスプロバイダは、NetBackup for OpenStack の VAST (Virtual Snapshot Technology) を使用することで、バックアップとディザスタリカバリをサービスとして配備し、特定時点のスナップショットとシームレスなワンクリックリカバリを行ってデータ損失やデータの破損を防げるようになりました。NetBackup for OpenStack は、計算リソース、ネットワーク構成、ストレージデータで構成される作業負荷全体を 1 つの単位として特定時点のバックアップ作成します。また、前回のバックアップ以降に行われた変更のみをキャプチャする増分バックアップも作成します。増分スナップショットは、バックアップに前回のバックアップ以降の変更のみが含まれるため、時間とストレージ領域を節約できます。バックアップおよびリストアに VAST を使用する利点は、次のように要約できます。

- スナップショットの効率的なキャプチャと保持。完全バックアップにはストレージボリュームにコミットされたデータのみが含まれ、増分バックアップには前回のバックアップ以

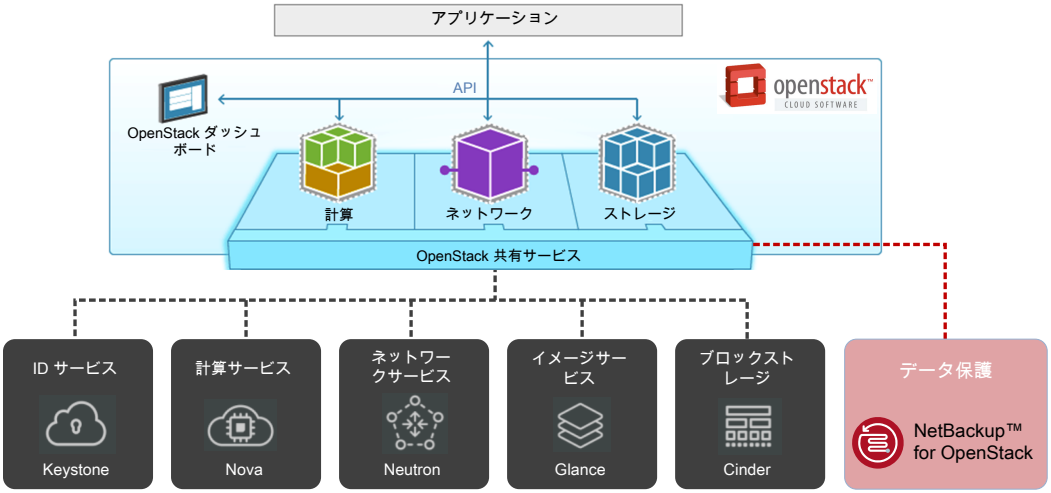
降に変更されたデータブロックのみが含まれるため、バックアップ処理が効率的で、バックアップイメージをバックアップメディアに効率的に格納します。

- 迅速で信頼性の高いリカバリ。アプリケーションが複雑になって、複数の VM とストレージボリュームのスナップショットを作成する場合に、効率的なリカバリプロセスによって、ボタンをクリックするだけでアプリケーションをゼロから運用可能な状態にできます。
- クラウド間でのポリシーの簡単な移行。NetBackup for OpenStack はアプリケーションのすべての詳細をキャプチャするため、移行にアプリケーションスタック全体が含まれるようになり、推測に基づくデータは存在しません。
- ポリシーと自動化を通じた、総所有コストの低減。テナント主導のバックアップ処理と自動化により、専用のバックアップ管理者を必要とせず、総所有コストが低減されます。

NetBackup for OpenStack アーキテクチャ

BaaS (Backup as a Service)

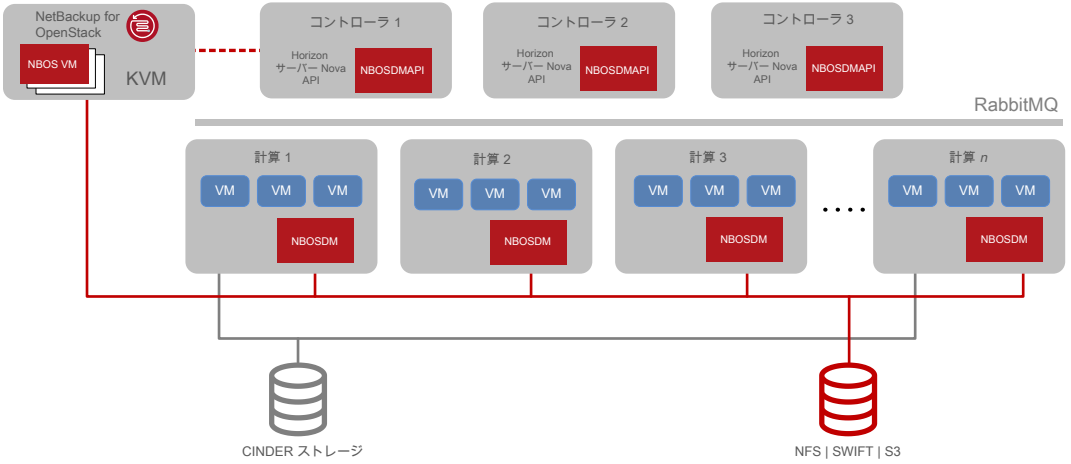
図 1-1 BaaS (Backup as a Service) を提供するデータ保護プロジェクト



NetBackup for OpenStack は、OpenStack クラウドインフラのアドオンサービスであり、テナントポリシーのバックアップとディザスタリカバリ機能を提供します。NetBackup for OpenStack は Nova、Cinder、Glance などの他の OpenStack サービスと非常に類似しており、OpenStack のすべてのテナントに準拠しています。これは、クラウドに合わせて拡張できるステートレスサービスです。

主なコンポーネント

図 1-2 NetBackup for OpenStack アーキテクチャの概要

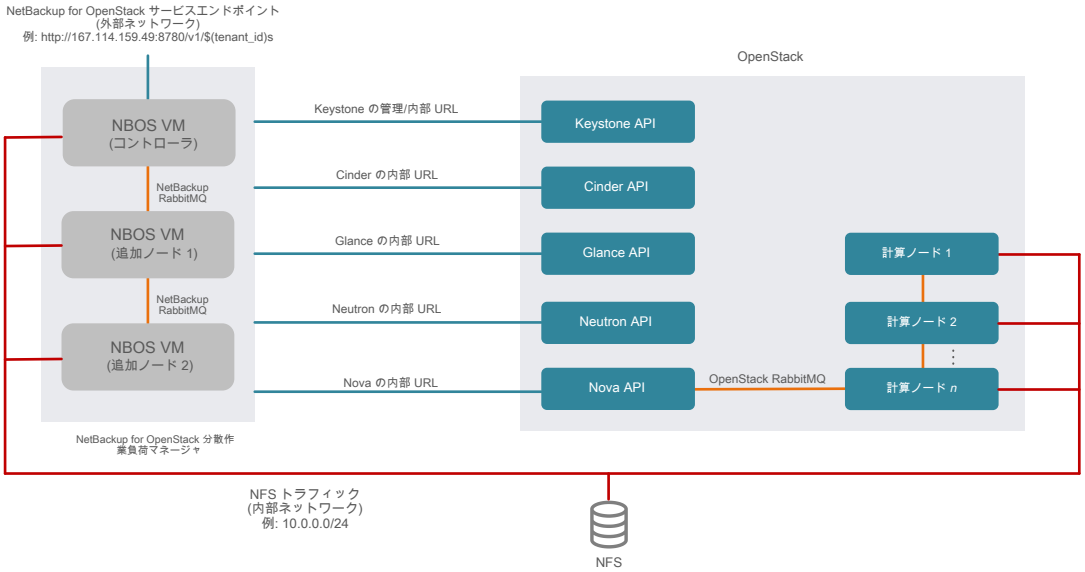


NetBackup for OpenStack には、4 つの主要なソフトウェアコンポーネントがあります。

1. NetBackup for OpenStack は QCOW2 イメージとして出荷されます。ユーザーは、スタンドアロン KVM ボックスの QCOW2 イメージから 1 つ以上の VM をインスタンス化できます。
2. NetBackup for OpenStack Datamover API (NBOSDMAPI) は、nova-api サービスが実行されているすべての OpenStack コントローラノードにインストールされる Python モジュールです。
3. NetBackup for OpenStack Datamover (NBOSDM) は、各 OpenStack 計算ノードにインストールされる Python モジュールです。
4. NetBackup for OpenStack Horizon プラグインは、Horizon サーバーへのアドオンとしてインストールされます。このモジュールは、Horizon サービスを実行するすべてのサーバーにインストールされます。

サービスのエンドポイント

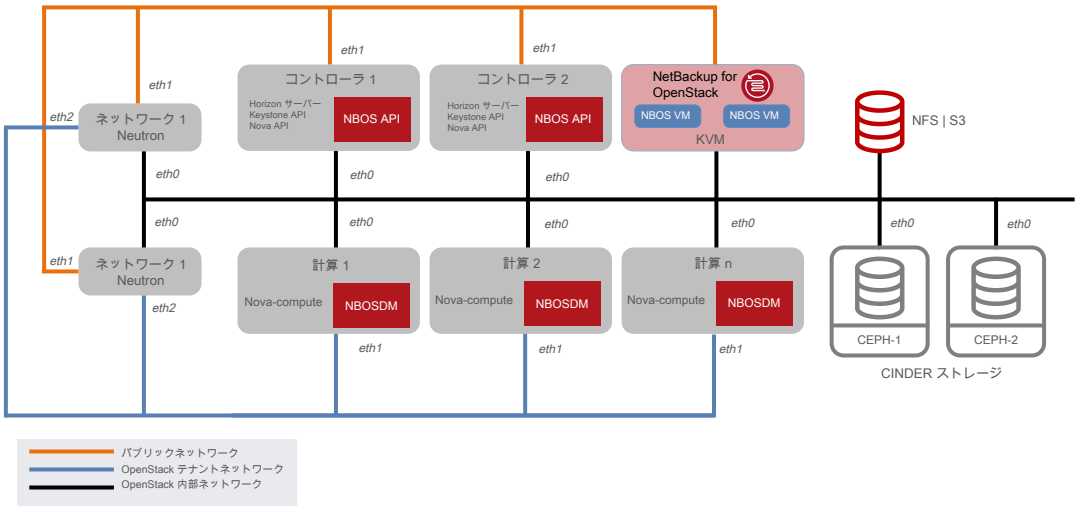
図 1-3　　サービスのエンドポイントの概要



NetBackup for OpenStack は、OpenStack エコシステムではプロバイダとコンシューマーの両方になります。Nova、Cinder、Glance、Neutron、Keystone などの他の OpenStack サービスを使用し、OpenStack テナントに独自のサービスを提供します。すべての可能な OpenStack 配備に対応するために、NetBackup for OpenStack はパブリック URL またはサービスの内部 URL のいずれかを使用するように構成できます。同様に、NetBackup for OpenStack は独自のパブリック URL、内部 URL、管理 URL を提供します。

ネットワークトポロジー

図 1-4 ネットワークトポロジーの例



この図は、典型的なネットワークトポロジーを表しています。NetBackup for OpenStack は、パブリックネットワークと NetBackup for OpenStack 仮想アプライアンスにパブリック URL エンドポイントを公開し、データムーバーは通常、バックアップストアからバックアップイメージを保存して取り込むのに内部ネットワークまたは専用のバックアップネットワークを使用します。

2

NetBackup for OpenStack の配備

この章では以下の項目について説明しています。

要件

NetBackup for OpenStack には、4 つの主要なソフトウェアコンポーネントがあります。

1. NetBackup for OpenStack は QCOW2 イメージとして出荷されます。ユーザーは、スタンドアロン KVM ボックスの QCOW2 イメージから 1 つ以上の VM をインスタンス化できます。

2. NetBackup for OpenStack API は、Nova API サービスの拡張機能である Python モジュールです。このモジュールは、すべての OpenStack コントローラノードにインストールされます。
3. NetBackup for OpenStack Datamover は、各 OpenStack 計算ノードにインストールされる Python モジュールです。
4. NetBackup for OpenStack Horizon プラグインは、Horizon サーバーへのアドオンとしてインストールされます。このモジュールは、Horizon サービスを実行するすべてのサーバーにインストールされます。

p.19 の「ソフトウェア要件 」を参照してください。

NetBackup for OpenStack VM のシステム要件

NetBackup for OpenStack VM は qcow2 イメージとして配信され、仮想マシンに接続されます。

ベリタスでは KVM ベースのハイパーバイザのみをサポートします。

メモ: NetBackup for OpenStack VM は NetBackup for OpenStack 内のインスタンスとしてはサポートされません。

NetBackup for OpenStack Appliance の VM の推奨サイズは次のとおりです。

リソース	値
vCPU	8
RAM	24 GB

qcow2 イメージ自体は、VM の 40 GB ディスクサイズを定義します。

NetBackup for OpenStack VM データベースまたはログファイルが 40 GB ディスクを超えるようなまれなケースでは、ベリタスのテクニカルサポートにお問い合わせいただくかチケットを発行して、NetBackup for OpenStack VM に別のドライブを接続します。

ソフトウェア要件

NetBackup for OpenStack はテストおよび検証されています

ソフトウェア	バージョン
CentOS	7.9
Virsh	libvirt 2.0.0 以降

ソフトウェア	バージョン
QEMU	2.0.0 以降
Qemu-img	2.6.0 以降

さらに、NFS バックアップターゲットでは、計算ノードに `nfs-common` パッケージをインストールする必要があります。

NetBackup for OpenStack ネットワークに関する注意事項

NetBackup for OpenStack は、OpenStack とネイティブに統合されます。NetBackup for OpenStack は、OpenStack エンドポイントを使用して API を介して完全に通信します。NetBackup for OpenStack は、独自の OpenStack エンドポイントも生成します。さらに、バックアップターゲットとの間で読み書きを行う NetBackup for OpenStack アプライアンスと計算ノードです。これらのポイントは、NetBackup for OpenStack インストールのネットワーク計画に影響します。

OpenStack の既存のエンドポイント

OpenStack は 3 種類のエンドポイントを認識します。

- パブリックエンドポイント
- 内部エンドポイント
- 管理エンドポイント

これらのエンドポイントの種類はそれぞれ、特定の目的のために設計されています。パブリックエンドポイントは、OpenStack ユーザーが OpenStack と連携するために使用することを目的としています。内部エンドポイントは、OpenStack サービスが相互に通信するために使用することを目的としています。管理エンドポイントは、OpenStack 管理者が使用することを目的としています。

これらの 3 つのエンドポイントの種類のうち、管理エンドポイントにのみ他のどのエンドポイントの種類でも利用できない API が含まれる場合があります。

OpenStack エンドポイントについて詳しくは、公式の OpenStack マニュアルを参照してください。

NetBackup for OpenStack で必要な OpenStack エンドポイント

NetBackup for OpenStack は、定義済みのエンドポイントの種類で OpenStack のすべてのサービスと通信します。OpenStack との通信に NetBackup for OpenStack が使用

するエンドポイントの種類は、NetBackup for OpenStack Appliance の構成時に決定されます。

例外: NetBackup for OpenStack Appliance は常に Keystone 管理エンドポイントへのアクセスを必要とします。

この方法では、次のネットワーク要件を特定できます。

- NetBackup for OpenStack Appliance は、管理エンドポイントネットワーク上の Keystone 管理エンドポイントにアクセスする必要があります
- NetBackup for OpenStack Appliance は、1 つの種類のすべてのエンドポイントにアクセスする必要があります

推奨事項: OpenStack エンドポイントの全種類へのアクセスの提供

ベリタスでは、OpenStack の標準とベストプラクティスに従うために、NetBackup for OpenStack アプライアンスにすべての OpenStack エンドポイントへのフルアクセス権を付与することをお勧めします。

NetBackup for OpenStack は独自のエンドポイントも生成します。これらのエンドポイントは、NetBackup for OpenStack Appliance を直接指します。つまり、これらのエンドポイントを使用しても、最初に OpenStack Controller ノードに対する API 呼び出しは送信されず、NetBackup for OpenStack VM に直接送信されます。

したがって、OpenStack の標準とベストプラクティスに従って、NetBackup for OpenStack エンドポイントを既存の OpenStack エンドポイントと同じネットワークに配置することをお勧めします。これにより、各エンドポイントタイプの目的を NetBackup for OpenStack サービスに拡張できます。

- NetBackup for OpenStack CLI または API を使用する場合に OpenStack ユーザーが使用するパブリックエンドポイント
- OpenStack サービスと通信するための内部エンドポイント
- Keystone の必要な管理専用 API を使用する管理エンドポイント

NetBackup for OpenStack で必要なバックアップターゲットアクセス

NetBackup for OpenStack ソリューションでは、バックアップターゲットストレージを使用して、バックアップデータを安全に配置します。NetBackup for OpenStack はバックアップデータを 2 つの部分に分けます。

1. メタデータ
2. ボリュームディスクデータ

最初の種類のデータは、OpenStack エンドポイントとの通信を介して NetBackup for OpenStack Appliance によって生成されます。バックアップと一緒に格納されるすべて

のメタデータは、NetBackup for OpenStack Appliance によって JSON 形式でバックアップターゲットに書き込まれます。

2 番目の種類のデータは、計算ノードで実行されている NetBackup for OpenStack nbosdm サービスによって生成されます。nbosdm サービスは Cinder または Nova ストレージからボリュームデータを読み込み、このデータを qcow2 イメージとしてバックアップターゲットに転送します。各 Datamover サービスは、ここで計算ノードで実行されている VM を担当します。

そのため、ネットワーク要件は次のようになります。

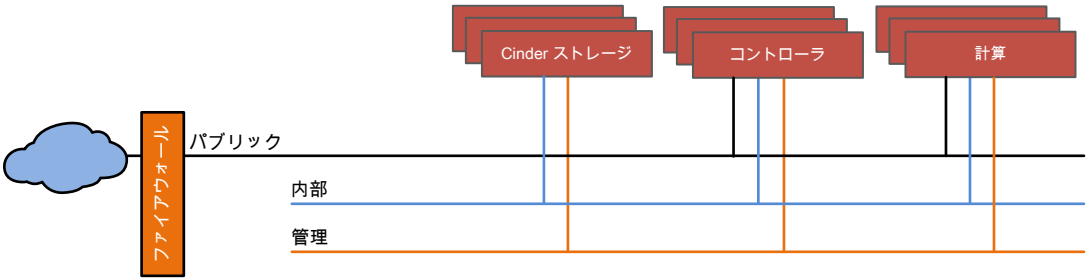
- NetBackup for OpenStack Appliance はバックアップターゲットにアクセスする必要があります
- すべての計算ノードがバックアップターゲットにアクセスする必要があります

一般的な NetBackup for OpenStack ネットワーク統合の例

多くの OpenStack ユーザーは、OpenStack の標準とベストプラクティスに従って、個別のネットワークにパブリックエンドポイント、内部エンドポイント、管理エンドポイントを設定します。また、通常は、目的のバックアップターゲットにアクセスできるネットワークがまだ存在しません。

通常、開始ネットワーク構成は次のようになります。

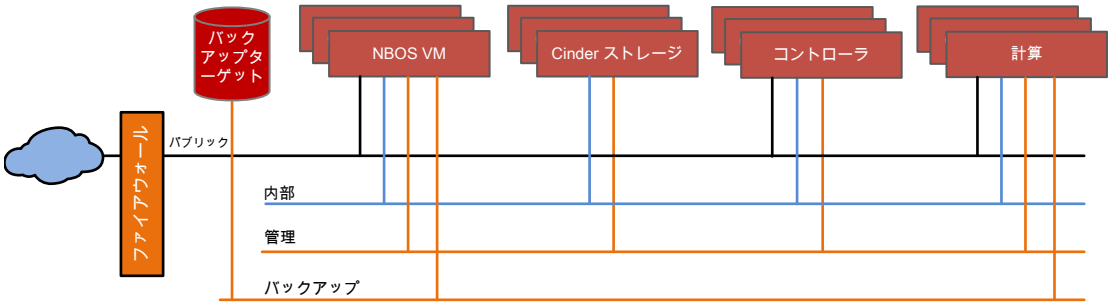
図 2-1 NetBackup for OpenStack のインストール前の標準的な OpenStack ネットワーク構成



OpenStack の標準とベリタスの推奨事項に従って、NetBackup for OpenStack Appliance は、これら 3 つのネットワークすべてに配置されます。さらに、NetBackup for OpenStack Appliance と計算ノードで必要なバックアップターゲットへのアクセスを設定します。ここで、4 番目のネットワークが追加されます。

この結果、ネットワーク構成は次のようになります。

図 **2-2** NetBackup for OpenStack がインストールされた標準的な OpenStack ネットワーク構成



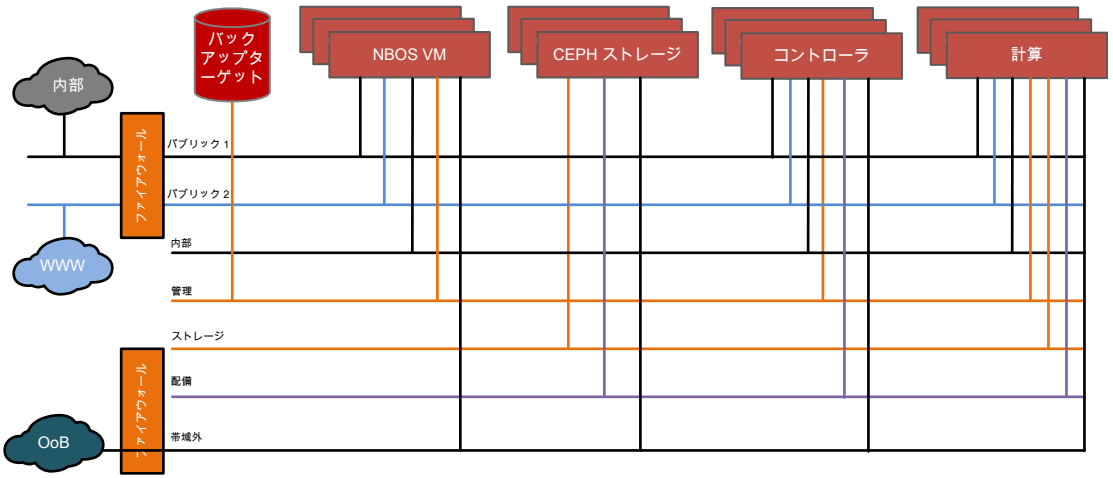
必要に応じてネットワークを組み合わせられます。必要なネットワークアクセスが利用可能であるかぎり、NetBackup for OpenStack は機能します。

NetBackup for OpenStack ネットワーク統合のその他の例

OpenStack はさまざまな方法でインストールされ、ネットワーク構成も異なります。OpenStack ネットワークの構成と、このネットワークへの NetBackup for OpenStack Appliance の実装には、数多くの方法があります。本番環境で見られる 3 つの例を次に示します。

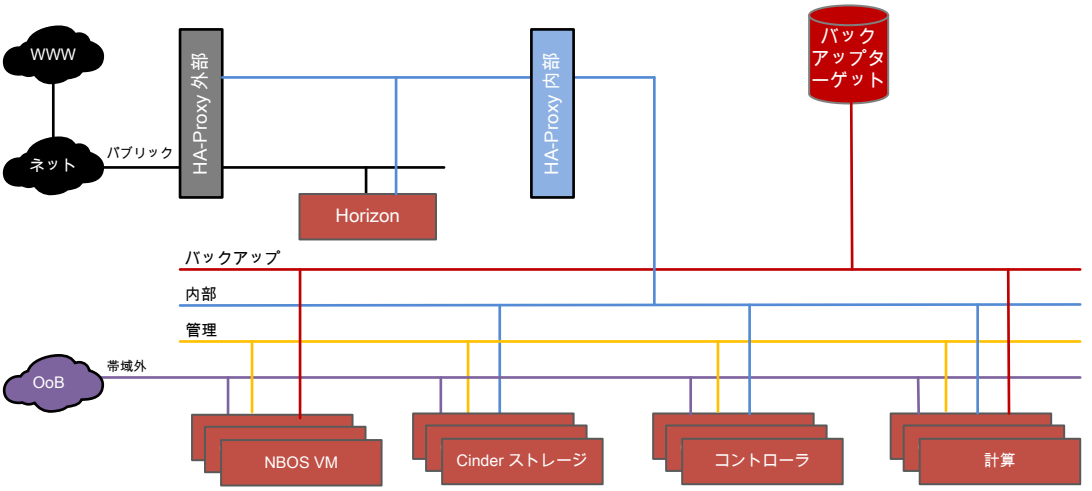
最初の例は、機能別にネットワークを分割する必要がある製造会社で、NetBackup for OpenStack バックアップターゲットを内部ネットワークに配置することにしました。バックアップとリカバリ機能が OpenStack 内部ソリューションとして識別されています。この例は複雑に見えますが、NetBackup for OpenStack が推奨どおりに統合されています。

図 2-3 すべてを分割したネットワークの例



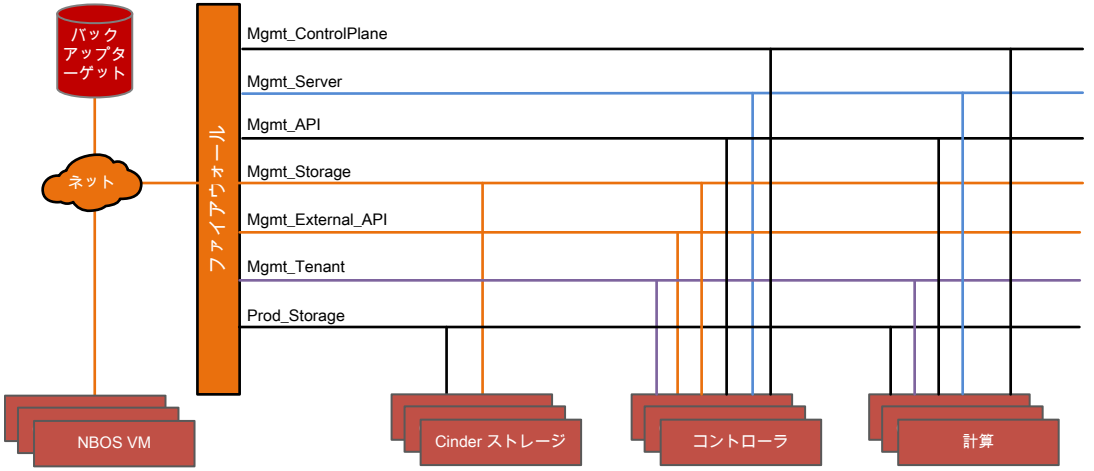
2 つ目の例は、OpenStack ユーザーが OpenStack インフラのネットワークに制御なしで直接アクセスできないようにする必要がある金融機関の例です。この例に従うには、NetBackup for OpenStack に対する API 呼び出しを正確に変換するように内部 HA プロキシを構成する必要があるため、追加の作業が必要になります。

図 2-4 トラストネットワークがない例



3 つ目の例は、OpenStack の外部で仮想マシンを実行する必要があるため、NetBackup for OpenStack を外部のサードパーティソリューションとして強制的に処理せざるを得なかったサービス会社の例です。この種類のネットワーク構成では、NetBackup for OpenStack エンドポイントとファイアウォールルールを十分に計画する必要があります。

図 2-5 サードパーティコンポーネントとしての NetBackup for OpenStack のネットワーク例



インストールの準備

NetBackup for OpenStack のインストールの前に、次の要素について考えることをお勧めします。

テナントクォータ

NetBackup for OpenStack は完全バックアップと増分バックアップの計算に Cinder スナップショットを使用します。完全バックアップの場合、NetBackup for OpenStack は、バックアップジョブのすべてのボリュームに Cinder スナップショットを作成します。その後、次回のバックアップ時に増分バックアップイメージを計算するために、これらの Cinder スナップショットを残します。増分バックアップ操作時に、新しい Cinder スナップショットが作成され、新しいスナップショットと、完全バックアップまたは前回のバックアップ中に残された古いスナップショット間で変更されたブロックが計算されます。その後、古いスナップショットは削除されますが、新しく作成されたスナップショットは残ります。したがって、NetBackup for OpenStack バックアップ機能を利用する各テナントが、これらの追加のスナップショットに対応できる十分な Cinder スナップショットクォータを持っていることが重要です。ガイドラインとしては、バックアップに追加された各ボリューム用に、そのテナントのボリュームスナップショットクォータに 2 つのスナップショットを追加することです。また、バックアップの目的でスナップショットからデータを読み取るために NetBackup for OpenStack でスナップショットからボリューム作成するため、テナントのボリュームクォータを同じ量増やすこともできます。リストア処理中に、NetBackup for OpenStack は追加のインスタンスとCinderボリュームを作成します。リストア操作に対応するために、テナントに Nova インスタンスと Cinder ボリュームの十分なクォータが必要です。不足した場合、リストア操作はエラーになります。

AWS S3 の最終的な一貫性

AWS S3 オブジェクトの一貫性モデルには、次のものが含まれます。

1. read-after-write
2. read-after-update
3. read-after-delete

これらは、作成、更新、または削除された後で、オブジェクトが一貫した状態に達する方法を示します。これらのどの種類でも、強力な一貫性は提供されません。オブジェクトが一貫性のある状態になるまでの遅延時間があります。NetBackup for OpenStack では、AWS S3 の最終的な一貫性の制限を回避するメカニズムを採用していますが、オブジェクトがいつ一貫性のある状態に達するかは確定的ではありません。オブジェクトが一貫性のある状態に達するまでの時間に関して、AWS からの公式な規定はありません。ただし、read-after-write では、他の IO パターンに比べて一貫性に達するまでの時間が短くなります。ベリタスのソリューションは、read-after-write の IO パターンを最大化するように設計されています。オブジェクトが最終的な一貫性に達する時間は、AWS リージョンによっ

ても異なります。たとえば、aws-standard リージョンには、us-east または us-west と比較して強力な一貫性モデルはありません。NetBackup for OpenStack 用の s3 バケットを作成するときに、これらのリージョンを使用することをお勧めします。read-after-update の IO パターンを完全には回避できませんが、オブジェクトへのアクセスに十分な遅延を採用し、オブジェクトが一貫した状態になるのに長い期間がかかるケースに対応しています。ただし、まれにバックアップが失敗し、再起動が必要になる場合があります。

NetBackup for OpenStack クラスタ

NetBackup for OpenStack は単一ノードまたは 3 ノードクラスタとして配備できます。耐障害性と負荷分散のために、3 ノードクラスタとして NetBackup for OpenStack を配備することをお勧めします。NetBackup for OpenStack はクラスタに追加の IP を必要とします。単一ノードと 3 ノードの両方の配備に必要です。クラスタ IP (仮想 IP) は、クラスタの管理に使用され、NetBackup for OpenStack サービスエンドポイントを Keystone サービスカタログに登録するために使用されます。

NetBackup for OpenStack VM のスピンアップ

NetBackup for OpenStack Appliance は、qcow2 イメージとして配信され、KVM ハイパーバイザの上で VM として実行されます。

このガイドでは、RHV クラスタで NetBackup for OpenStack Appliance をスピンアップするためのテスト済みの方法を示します。

cloud-init イメージの作成

NetBackup for OpenStack Appliance は、cloud-init を使用して初期ネットワークとユーザー構成を提供します。

cloud-init は、メタデータサーバーまたは提供された cd イメージから情報を読み込みます。NetBackup for OpenStack は cd イメージを使います。

必要なツール

cloud-init イメージを作成するには、genisoimage を利用できるようにする必要があります。

```
#For RHEL and centos
yum install genisoimage
```

メタデータの提供

cloud-init は、メタデータに 2 つのファイルを使用します。

最初のファイルは meta-data と呼ばれ、ネットワーク構成に関する情報が含まれています。このファイルの例を次に示します。

```
[root@kvm]# cat meta-data
instance-id: NetBackup for OpenStack
network-interfaces: |
   auto ens3
   iface ens3 inet static
   address 158.69.170.20
   netmask 255.255.255.0
   gateway 158.69.170.30

   dns-nameservers 11.11.0.51
local-hostname: nbos-controller.domain.org
```

警告: instance-id は virsh の VM 名と一致する必要があります。

2 番目のファイルは user-data と呼ばれ、スクリプトと、ユーザーパスワードなどの設定情報が含まれています。このファイルの例を次に示します。

```
[root@kvm]# cat user-data
#cloud-config
chpasswd:
  list: |
    root:password1
    stack:password2
  expire: False
```

イメージファイルの作成

機能する cloud-init イメージを作成するために、ファイルメタデータとユーザーデータの両方が必要です。

イメージは、次の一般的なコマンドに従って genisoimage を使用して作成されます。

```
genisoimage -output <name>.iso -volid cidata -joliet -rock
</path/user-data> </path/meta-data>
```

このコマンドの例:

```
genisoimage  -output nbos-firstboot-config.iso -volid cidata
-joliet -rock user-data meta-data
```

NetBackup for OpenStack アプライアンスのスピンアップ

cloud-init イメージが作成された後、NetBackup for OpenStack アプライアンスを目的の KVM サーバーでスピンアップできます。

次のコマンド例は virsh と作成された ISO イメージを使用して NetBackup for OpenStack アプライアンスをスピンアップする方法を示しています。

```
virt-install -n nbosvm  --memory 24576 --vcpus 8 ¥
--os-type linux ¥
--disk nbos-appliance-os-3.0.154.qcow2,device=disk,bus=virtio,size=40
 ¥
--network bridge=virbr0,model=virtio ¥
--network bridge=virbr1,model=virtio ¥
--graphics none ¥
--import ¥
--disk path=nbos-firstboot-config.iso,device=cdrom
```

cloud-init iso イメージなしで NetBackup for OpenStack アプライアンスをスピンアップできます。デフォルト値でスピンアップします。

最初の起動後の cloud-init のアンインストール

初期構成で NetBackup for OpenStack アプライアンスを起動して実行したら、cloud-init をアンインストールすることをお勧めします。

cloud-init がインストールされていない場合は、起動するたびにネットワーク構成が再実行されます。メタデータが指定されていない場合は、ネットワーク構成を DHCP に戻します。

cloud-init をアンインストールするには、次の例に従います。

```
sudo yum  remove cloud-init
```

または

```
touch /etc/cloud/cloud-init.disabled
```

NetBackup for OpenStack バックアップターゲットの形式について

バックアップターゲットストレージは、NetBackup for OpenStack によって取得されたバックアップイメージと構成に必要な詳細を格納するために使用されます。

次のバックアップターゲット形式が NetBackup for OpenStack でサポートされます。いずれか 1 つを選択して準備してから、次の手順に進みます。

- NFS
  NFS 共有パスが必要
- Amazon S3
  - S3 アクセスキー
  - シークレットキー
  - リージョン
  - バケット名
- Ceph ベースの S3 などのその他の S3 互換ストレージ
  - S3 アクセスキー
  - シークレットキー
  - リージョン
  - エンドポイント URL (Amazon S3 以外の S3 で有効)
  - バケット名

NetBackup for OpenStack コンポーネントのインストール

NetBackup for OpenStack VM または NetBackup for OpenStack VM のクラスタがスピンされると、実際のインストール処理を開始できます。この処理は次の手順で行います。

1. NetBackup for OpenStack Datamover API (nbosdmapi) サービスをコントロールプレーンにインストールします。
2. NetBackup for OpenStack Datamover (nbosdm) サービスを計算プレーンにインストールします。
3. Horizon サービスに NetBackup for OpenStack Horizon プラグインをインストールします。

これらの手順の詳細は、OpenStack 配布 NetBackup for OpenStack がインストールされているかどうかによって異なります。サポート対象の各 OpenStack 配布には、独自の配備ツールがあります。NetBackup for OpenStack は、これらの配備ツールに統合され、最初から最後までネイティブ統合を提供します。

RHOSP へのインストール

Red Hat OpenStack Platform Director は、すべての RHOSP インストールを配備して保守するためにサポートおよび推奨される方法です。

NetBackup for OpenStack は、RHOSP Director にネイティブに統合されています。手動による配備方法は、RHOSP ではサポートされません。

次の手順を実行して、NetBackup for OpenStack を RHOSP にインストールします。

表 2-1 RHOSP へのインストール

手順	作業	説明
1	配備を準備します。	p.31 の「配備の準備」を参照してください。
2	NetBackup for OpenStack puppet モジュールをアップロードします。	p.33 の「NetBackup for OpenStack puppet モジュールのアップロード」を参照してください。
3	オーバークラウド役割データファイルを更新して、NetBackup for OpenStack サービスを含めます。	p.33 の「オーバークラウド役割データファイルを更新して NetBackup for OpenStack サービスを含める」を参照してください。
4	NetBackup for OpenStack コンテナイメージを準備します。	p.34 の「NetBackup for OpenStack コンテナイメージの準備」を参照してください。
5	nbos_env.yaml で環境の詳細を指定します。	p.35 の「nbos_env.yaml での環境の詳細の指定」を参照してください。
6	NetBackup for OpenStack 環境を使用してオーバークラウドを配備します。	p.38 の「NetBackup OpenStack 環境でのオーバークラウドの配備」を参照してください。
7	配備を検証します。	p.39 の「配備の検証」を参照してください。
8	NetBackup for OpenStack Appliance で追加手順を実行します。	p.40 の「NetBackup for OpenStack Appliance での追加手順」を参照してください。
9	オーバークラウド配備エラーをトラブルシューティングします。	p.40 の「オーバークラウド配備エラーのトラブルシューティング」を参照してください。

配備の準備

配備を準備するには、次のタスクを実行します。

- NetBackup for OpenStack バックアップターゲットの形式を選択します。

p.29 の「NetBackup for OpenStack バックアップターゲットの形式について」を参照してください。

- アンダークラウドに nbos-cfg-scripts をコピーします。
p.32 の「アンダークラウドへの nbos-cfg-scripts のコピー」を参照してください。
- バックアップターゲットの種類が SSL を使用する Ceph ベースの S3 の場合
p.32 の「バックアップターゲットの種類が SSL を使用する Ceph ベースの S3 の場合」を参照してください。

アンダークラウドへの nbos-cfg-scripts のコピー

インストール済みの RHOSP 環境のアンダークラウドノードで、次の手順を実行します。overcloud deploy コマンドがすでに正常に実行され、オーバークラウドが利用可能である必要があります。

警告: すべてのコマンドは、アンダークラウドノードでユーザー「stack」として実行する必要があります。

次のコマンドを実行して nbos-cfg-scripts をコピーします。

```
cd /home/stack
cp <image location>/nbos-cfg-scripts.tar.gz /home/stack
gunzip /home/stack/nbos-cfg-scripts.tar.gz
tar xvf /home/stack/nbos-cfg-scripts.tar
cd nbos-cfg-scripts/redhat-director-scripts/<RHOSP_RELEASE_DIRECTORY>/
```

利用可能な RHOSP_RELEASE___DIRECTORY 値は次のとおりです。

- `rhosp16.1`
- `rhosp16.2`

バックアップターゲットの種類が SSL を使用する Ceph ベースの S3 の場合

バックアップターゲットが SSL を使用した ceph S3 で、SSL 証明書が自己署名されているか、プライベート CA によって認証されている場合は、SSL 要求を検証するために CA チェーン証明書を指定する必要があります。CA チェーンの cert ファイルの名前を `s3-cert.pem` に変更し、ディレクトリ `nbos-cfg-scripts/redhat-director-scripts/redhat-director-scripts/<RHOSP_RELEASE___Directory/puppet/nbos/files` にコピーする必要があります。

```
cp s3-cert.pem /home/stack/nbos-cfg-scripts/
redhat-director-scripts/<RHOSP_RELEASE_DIRECTORY>/puppet/nbos/files/
```

NetBackup for OpenStack puppet モジュールのアップロード

次のコマンドは、オーバークラウドレジストリに NetBackup for OpenStack puppet モジュールをアップロードします。実際のアップロードは次の配備時に行われます。

```
cd /home/stack/nbos-cfg-scripts/redhat-director-scripts/
<RHOSP_RELEASE_DIRECTORY>/scripts/

./upload_puppet_module.sh
```

オーバークラウド役割データファイルを更新して NetBackup for OpenStack サービスを含める

NetBackup for OpenStack には複数のサービスが含まれています。これらのサービスを `roles_data.yaml` に追加します。

`roles_data.yaml` がカスタマイズされていない場合は、アンダークラウドの次の場所で見つけることができます。

```
/usr/share/openstack-tripleo-heat-templates/roles_data.yaml
```

次のサービスを `roles_data.yaml` に追加します。

メモ: すべてのコマンドは、ユーザー「stack」として実行する必要があります。

役割データファイルへの NetBackup for OpenStack Datamover API サービスの追加

このサービスは、keystone および database サービスと同じ役割を共有する必要があります。事前定義済みの役割の場合、これらのサービスはコントローラの役割で実行されます。カスタムの役割の場合は、OS::TripleO::Services:Keystone サービスがインストールされているのと同じ役割を使用する必要があります。

特定された役割に次の行を追加します。

```
'OS::TripleO::Services::nbosdmapi'
```

役割データファイルへの NetBackup for OpenStack Datamover サービスの追加

このサービスは、nova-compute サービスと同じ役割を共有する必要があります。事前定義済みの役割の場合、nova-compute サービスは計算の役割で実行されます。カスタムで定義された役割の場合は、nova-compute サービスが使用する役割を使用する必要があります。

特定された役割に次の行を追加します。

```
'OS::TripleO::Services::nbosdm'
```

NetBackup for OpenStack コンテナイメージの準備

警告: すべてのコマンドは、ユーザー「stack」として実行する必要があります。

NetBackup for OpenStack はパッケージを収容するためにアンダークラウドのローカルレジストリを使います。

NetBackup for OpenStack は、コンテナをアンダークラウドにプッシュし、nbos_env.yaml を更新するシェルスクリプトを提供します。

```
cd
/home/stack/nbos-cfg-scripts/redhat-director-scripts/<RHOSP_RELEASE_DIRECTORY>//scripts
```

```
sudo ./prepare_nbos_images.sh <UNDERCLOUD_REGISTRY_HOSTNAME>
<IMAGE_SOURCE_FOLDER>
```

次のコマンドを実行して、UNDERCLOUD_REGISTRY_HOSTNAME を見つけます。

次の nbos-undercloud の例では、<UNDERCLOUD_REGISTRY_HOSTNAME> です

```
$ openstack tripleo container image list | grep keystone |
docker://nbos-undercloud:8787/rhosp-rhel8/openstack-keystone:16.0-82
| |
docker://nbos-undercloud:8787/rhosp-rhel8/openstack-barbican-keystone-listener:16.0-84
```

RHOSP16.1 の CONTAINER_TAG 形式: <NBOS_VERSION>-rhosp16.1

RHOSP16.2 の CONTAINER_TAG 形式: <NBOS_VERSION>-rhosp16.2

例:

```
sudo ./prepare_nbos_images.sh nbos-undercloud 9.0.1017-rhosp16.1
/home/stack/nbos/nbos-rhosp16.1-9.0.1017
```

次のコマンドを使用して、変更内容を確認できます。

```
(undercloud) [stack@nbos-undercloud scripts]$ sudo podman images |
grep 9.0.1017-rhosp16.1
localhost/nbos-horizon-plugin 9.0.1017-rhosp16.1 8705f72da6d4
5 days ago 1.16 GB
localhost/nbosdmapi    9.0.1017-rhosp16.1 2da0be5dcacb
5 days ago 1.46 GB
localhost/nbosdm    9.0.1017-rhosp16.1 d6e1168faae2
5 days ago 2.97 GB
```

```
(undercloud) [stack@host scripts]$ grep 'Image'
../environments/nbos_env.yaml
  docker_nbosdm_image: nbos-undercloud:8787/nbosdm:9.0.1017-rhosp16.1

   docker_nbosdmapi_image:
nbos-undercloud:8787/nbosdmapi:9.0.1017-rhosp16.1
   ContainerHorizonImage: nbos-undercloud:8787/nbos-horizon-plugin:
9.0.1017-rhosp16.1
```

nbos_env.yaml での環境の詳細の指定

提供された環境ファイルに、バックアップターゲットの詳細とその他の必要な詳細を指定します。この環境ファイルは、NetBackup for OpenStack コンポーネントを構成するためにオーバークラウド配備で使用されます。コンテナイメージの準備時に、コンテナイメージ名がすでに入力されています。ただし、コンテナの URL を確認することをお勧めします。

さらに、次の情報が必要です。

- nbosdmapi のネットワーク
- nbosdm のパスワード
- バックアップターゲット形式 {nfs/s3}
- NFS の場合
  - NFS 共有のリスト
  - NFS オプション
- S3 の場合
  - S3 形式 {amazon_s3/ceph_s3}
  - S3 アクセスキー
  - S3 シークレットキー
  - S3 リージョン名
  - S3 バケット
  - S3 エンドポイント URL
  - S3 署名バージョン
  - S3 認証バージョン
  - S3 SSL 有効 {true/false}
  - S3 SSL 証明書

メモ: aws S3 以外のバックアップターゲットには、ceph_s3 を使用します。

```
resource_registry:
  OS::TripleO::Services::nbosdm: ../services/nbosdm.yaml
  OS::TripleO::Services::nbosdmapi: ../services/nbosdmapi.yaml
  # NOTE: If there are addition customizations to the endpoint map
(e.g. for
  # other integratiosn), this will need to be regenerated.
  OS::TripleO::EndpointMap: endpoint_map.yaml

parameter_defaults:

   ## Enable NetBackup for OpenStack's quota functionality on horizon

    ExtraConfig:
      horizon::customization_module: 'dashboards.overrides'

   ## Define network map for NetBackup OpenStack Datamover API Service

    ServiceNetMap:
        nbosdmapiNetwork: internal_api

    ## NetBackup for OpenStack Datamover Password for keystone and
database
    nbosdmPassword: "test1234"

    ## NetBackup for OpenStack container pull urls
   docker_nbosdm_image: nbos-undercloud:8787/nbosdm:9.0.1017-rhosp16.1

    docker_nbosdmapi_image:
nbos-undercloud:8787/nbosdmapi:9.0.1017-rhosp16.1

    ## If you do not want NetBackup for OpenStack's horizon plugin
    to replace your horizon container, just comment following line.
    ContainerHorizonImage: nbos-undercloud:8787/nbos-horizon-plugin:
    9.0.1017-rhosp16.1

    ## Backup target type nfs/s3, used to store snapshots taken by
    NetBackup for OpenStack
    BackupTargetType: 'nfs'

    ## For backup target 'nfs'
```

```
  NfsShares: '192.168.122.101:/opt/nbos'
  NfsOptions: 'nolock,soft,timeo=180,intr,lookupcache=none'

  ## For backup target 's3'
  ## S3 type: amazon_s3/ceph_s3
  S3Type: 'amazon_s3'

  ## S3 access key
  S3AccessKey: ''

  ## S3 secret key
  S3SecretKey: ''

  ## S3 region, if your s3 does not have any region, just keep the

  parameter as it is
  S3RegionName: ''

  ## S3 bucket name
  S3Bucket: ''

  ## S3 endpoint url, not required for Amazon S3, keep it as it is
  S3EndpointUrl: ''

  ## S3 signature version
  S3SignatureVersion: 'default'

  ## S3 Auth version
  S3AuthVersion: 'DEFAULT'

 ## If S3 backend is not Amazon S3 and SSL is enabled on S3 endpoint
u
  rl then change it to 'True', otherwise keep it as 'False'
  S3SslEnabled: False

 ## If S3 backend is not Amazon S3 and SSL is enabled on S3 endpoint

  URL and SSL certificates are self signed, then
  ## user need to set this parameter value to:
'/etc/nbosdm/s3-cert.pem', otherwise keep it's value
  as empty string.
  S3SslCert: ''
```

```
## Don't edit following parameter
EnablePackageInstall: True
```

NetBackup OpenStack 環境でのオーバークラウドの配備

オーバークラウド配備コマンドでは、次のヒート環境ファイルと役割データファイルを使用します。

1. nbos_env.yaml
2. roles_data.yaml
3. 利用可能な Keystone エンドポイント構成に従って、正しい NetBackup OpenStack エンドポイントマップファイルを使用します

   tls-endpoints-public-dns.yaml ファイルの代わりに、environments/nbos_env_tls_endpoints_public_dns.yaml を使用します

   tls-endpoints-public-ip.yaml ファイルの代わりに、environments/nbos_env_tls_endpoints_public_ip.yaml を使用します

   tls-everywhere-endpoints-dns.yamlファイルの代わりに、environments/nbos_env_tls_everywhere_dns.yaml を使用します

新しい環境ファイルを含める場合は、-e オプションを使用し、役割のデータファイルの場合は、-r オプションを使用します。

オーバークラウド配備コマンドの例:

```
openstack overcloud deploy --templates ¥
  -e /home/stack/templates/node-info.yaml ¥
  -e /home/stack/templates/overcloud_images.yaml ¥
  -e /home/stack/nbos-cfg-scripts/redhat-director-scripts/
     <RHOSP_RELEASE_DIRECTORY>/environments/nbos_env.yaml ¥
  -e /usr/share/openstack-tripleo-heat-templates/environments/ssl/
     enable-tls.yaml ¥
  -e /usr/share/openstack-tripleo-heat-templates/environments/ssl/
     inject-trust-anchor.yaml ¥
  -e
/home/stack/nbos-cfg-scripts/redhat-director-scripts/<RHOSP_RELEASE_

     DIRECTORY>/environments/nbos_env_tls_endpoints_public_dns.yaml
 ¥
  --ntp-server 192.168.1.34 ¥
  --libvirt-type qemu ¥
  --log-file overcloud_deploy.log ¥
  -r /home/stack/templates/roles_data.yaml
```

配備の検証

警告: コンテナが再起動中の状態にあるか、次のコマンドで一覧表示されない場合、配備は正しく行われていません。マニュアルの内容に従ったかどうかを再度確認してください。

コントローラノード上

NetBackup OpenStack Datamover API と Horizon コンテナが実行状態であり、コントローラノードに他の NetBackup OpenStack コンテナが配備されていないことを確認します。これらのコンテナの役割がコントローラでない場合は、構成された `roles_data.yaml` に従って各ノードを確認します。

```
[root@overcloud-controller-0 heat-admin]# podman ps | grep nbos
26fcb9194566
rhosptrainqa.ctlplane.localdomain:8787/nbosdmapi:9.0-rhosp16.1

kolla_start           5 days ago  Up 5 days ago         nbosdmapi
094971d0f5a9  rhosptrainqa.ctlplane.localdomain:
8787/nbos-horizon-plugin:9.0-rhosp16.1       kolla_start
5 days ago  Up 5 days ago         horizon
```

計算ノード上

NetBackup OpenStack Datamover コンテナが実行状態であり、計算ノードに他の NetBackup OpenStack コンテナが配備されていないことを確認します。

```
[root@overcloud-novacompute-0 heat-admin]# podman ps | grep nbos
b1840444cc59
rhosptrainqa.ctlplane.localdomain:8787/nbosdm:9.0-rhosp16.1

kolla_start           5 days ago  Up 5 days ago         nbosdm
```

Horizon サービスを使用するノード上

Horizon コンテナが実行状態であることを確認します。「Horizon」コンテナは NetBackup for OpenStack Horizon コンテナに置き換えられます。このコンテナには、最新の OpenStack Horizon と NetBackup for OpenStack の Horizon プラグインがあります。

```
[root@overcloud-controller-0 heat-admin]# podman ps | grep horizon
094971d0f5a9  rhosptrainqa.ctlplane.localdomain:
```

```
8787/nbos-horizon-plugin:9.0-rhosp16.1       kolla_start
5 days ago  Up 5 days ago         horizon
```

NetBackup for OpenStack Appliance での追加手順

NetBackup for OpenStack ノードの nova ユーザー ID の変更

RHOSP では、nova-compute docker コンテナの「nova」ユーザー ID は「42436」に設定されます。NetBackup for OpenStack ノードの「nova」ユーザー ID は同じ設定にする必要があります。すべての NetBackup for OpenStack ノードで次の手順を実行します。

1. スクリプトを実行します。
2. nova ユーザーとグループ ID が 42436 に変更されていることを確認します。

```
## Execute the shell script to change 'nova' user and group id to
'42436'
$ ./home/stack/nova_userid.sh

## Ignore any errors and verify that 'nova' user and group id has
changed to '42436'
$ id nova
   uid=42436(nova) gid=42436(nova)
groups=42436(nova),990(libvirt),36(kvm)
```

オーバークラウド配備エラーのトラブルシューティング

NetBackup for OpenStack コンポーネントは、puppet スクリプトを使って展開されます。

オーバークラウド配備が失敗した場合は、次のコマンドを実行してエラーのリストを提供します。次のマニュアルでも有益な洞察を得られます:
https://docs.openstack.org/tripleo-docs/latest/install/troubleshooting/troubleshooting-overcloud.html

```
openstack stack failures list overcloud
heat stack-list --show-nested -f "status=FAILED"
heat resource-list --nested-depth 5 overcloud | grep FAILED

=> If nbosdmapi containers does not start well or in restarting state,

use following logs to debug.
```

```
docker logs nbosdmapi

tail -f /var/log/containers/nbosdmapi/nbosdmapi.log


=> If nbosdm containers does not start well or in restarting state,

use following logs to debug.


docker logs nbosdm

tail -f /var/log/containers/nbosdm/nbosdm.log
```

Ansible OpenStack Ussuri へのインストール

Ansible OpenStack Ussuri に NetBackup for OpenStack をインストールするには、次の手順を実行します。

表 2-2 Ansible OpenStack Ussuri へのインストール

手順	作業	説明
1	ファイルレベルのログが Horizon コンテナの OpenStack コンポーネント用に構成されていることの確認	p.42 の「ファイルレベルのログが Horizon コンテナの OpenStack コンポーネント用に構成されていることの確認」を参照してください。
2	NetBackup for OpenStack ノードの nova ユーザー ID の変更	p.43 の「NetBackup for OpenStack ノードの nova ユーザー ID の変更」を参照してください。
3	配備ホストの準備	p.43 の「配備ホストの準備」を参照してください。
4	NetBackup for OpenStack コンポーネントの配備	p.48 の「NetBackup for OpenStack コンポーネントの配備」を参照してください。
5	NetBackup for OpenStack 配備の検証	p.48 の「NetBackup for OpenStack 配備の検証」を参照してください。

ファイルレベルのログが Horizon コンテナの OpenStack コンポーネント用に構成されていることの確認

NetBackup for OpenStack Horizon プラグインは、OpenStack のログサービスを使用してログを格納します。Horizon コンテナで OpenStack コンポーネントのシステムログを構成することをお勧めします。

ファイルに対して構造化ログ情報を生成するには、ログ作成の次の部分を構成していることを確認します。

設定例:

- フォーマッタ: ログファイルのログ情報の形式を定義します。

```
'verbose': {
   'format': '%(asctime)s %(process)d %(levelname)s %(name)s
%(message)s'
},
```

- ハンドラ: ログファイルにログ情報を書き込むファイルハンドラを追加します。

```
'file': {
    'level': 'DEBUG',
    'class': 'logging.FileHandler',
    'filename': '/var/log/horizon/horizon.log',
    'formatter': 'verbose',
 },
```

- ロガー: ログファイルにファイルハンドラ情報を使用して、使用中の各 OpenStack コンポーネントを更新します。
  たとえば、OpenStack ダッシュボード、Horizon、Nova クライアント、Cinder クライアント、Keystone クライアント、Glance クライアント、Neutron クライアント、OpenStack 認証、Django などがあります。

```
'horizon': {
     'handlers': ['file'],
     'level': 'DEBUG',
     'propagate': False,
}
```

ログのローテーションを有効にして、レコードストアがオーバーフローしないようにログデータのボリュームを制限することをお勧めします。ログ作成とログローテーションの構成について詳しくは、Django のマニュアルを参照してください。

NetBackup for OpenStack ノードの nova ユーザー ID の変更

NetBackup for OpenStack VM は、デフォルトで nova ユーザー ID とグループ ID 162:162 を使用します。Ansible OpenStack は、nova-compute コンテナでは常に nova ユーザー ID 162 とは限りません。NetBackup for OpenStack VM ノードの nova ユーザー ID は nova-compute コンテナと同じである必要があります。nova ID が 162:162 でない場合は、すべての NetBackup for OpenStack VM ノードで次の手順を実行します。

次の手順を実行する前に、ユーザー ID とグループ ID が NetBackup for OpenStack VM の他のどのサービスによっても使用されていないことを確認します。たとえば、計算ノードの nova ID が 997 の場合は、NetBackup for OpenStack VM の他のサービスでユーザー ID が使用されていないことを確認します。`rabbitmq` に 997 のユーザー ID が割り当てられ、NetBackup for OpenStack VM の `SSH` サービスに 997 のグループ ID が割り当てられている場合は、この ID を解放する必要があります。

```
#cat /etc/passwd | grep 997
#pid 997
#ps -ef | grep 997
#usermod -u 900 rabbitmq
#cat /etc/group | grep 997
#groupmod -g 901 ssh_keys
#reboot
```

1. ディレクトリ `/home/stack` に移動します。
2. `nova_userid.sh` ファイルに実行可能権限を割り当てます。

   ```
   #chmod +x nova_userid.sh
   ```

3. 正しい nova ID を使用するようにスクリプトを編集します。
4. スクリプトを実行します。

   ```
   #./nova_userid.sh
   ```

5. nova ユーザーとグループ ID が目的の値に変更されていることを確認します。

   ```
   #id nova
   ```

配備ホストの準備

NetBackup for OpenStack バックアップターゲットのストレージ形式を選択します。

p.29 の「NetBackup for OpenStack バックアップターゲットの形式について」を参照してください。を参照してください。

Ansible の役割と vars を必要な場所にコピーします。

```
cd nbos-cfg-scripts/
cp -R ansible/roles/* /opt/openstack-ansible/playbooks/roles/
cp ansible/main-install.yml   /opt/openstack-ansible/playbooks/
os-nbos-install.yml
cp ansible/environments/group_vars/all/vars.yml /etc/openstack_
deploy/user_nbos_vars.yml
```

ファイルの最後の /opt/openstack-ansible/playbooks/setup-openstack.yml に NetBackup for OpenStack プレイブックを追加します。

```
- import_playbook: os-nbos-install.yml
```

ファイルの最後に次の情報を追加します。/etc/openstack_deploy/user_variables.yml

```
# Datamover haproxy setting
haproxy_extra_services:
  - service:
      haproxy_service_name: nbosdm_service
     haproxy_backend_nodes: "{{ groups['nbosdmapi_all'] | default([])
 }}"
      haproxy_ssl: "{{ haproxy_ssl }}"
      haproxy_port: 8784
      haproxy_balance_type: http
      haproxy_balance_alg: roundrobin
      haproxy_timeout_client: 10m
      haproxy_timeout_server: 10m
      haproxy_backend_options:
       - "httpchk GET / HTTP/1.0¥¥r¥¥nUser-agent:¥¥
osa-haproxy-healthcheck"
```

ファイル /opt/openstack-ansible/inventory/env.d/nbos-nbosdmapi.yml を作成します。

ファイルに次の情報を追加します。

```
cat > /opt/openstack-ansible/inventory/env.d/nbos-nbosdmapi.yml
component_skel:
  nbosdmapi_api:
    belongs_to:
      - nbosdmapi_all
```

```
container_skel:
  nbosdmapi_container:
    belongs_to:
      - nbos-nbosdmapi_containers
    contains:
      - nbosdmapi_api

physical_skel:
  nbos-nbosdmapi_containers:
    belongs_to:
      - all_containers
  nbos-nbosdmapi_hosts:
    belongs_to:
      - hosts
```

次の例に従ってファイル /etc/openstack_deploy/openstack_user_config.yml を編集し、NetBackup for OpenStack コンポーネントのホストエントリを設定します。

```
#nbosdmapi
nbos-nbosdmapi_hosts:     # Add controller details in this section
as
                         # nbos-dmapi is resides on controller nodes.

  infra1:                  # Controller host name
    ip: <controller_ip>    # IP address of controller
  infra2:                  # For multiple controller nodes add
controller node
                          # details in same manner as shown in infra2

    ip: <controller_ip>

#nbos-datamover
nbos_compute_hosts:       # Add compute details in this section as
nbosdm
                          # resides on compute nodes.
  infra-1:                # Compute host name
    ip: <compute_ip>      # IP address of compute
  infra2:                 # For multiple compute nodes add compute
node
                         # details in same manner as shown in infra2
```

```
    ip: <compute_ip>
```

ファイル /etc/openstack_deploy/user_nbos_vars.yml の一般的な編集可能なパラメータセクションを編集します。

NetBackup for OpenStack Appliance の IP アドレス、NetBackup for OpenStack パッケージのバージョン、OpenStack 配布、スナップショットストレージバックエンド、SSL 関連情報などの必要な詳細を追加します。

```
##common editable parameters required for installing
nbos-horizon-plugin,
nbosdm and nbosdmapi
#ip address of nbosvm
IP_ADDRESS: <Nbosvm IP>
##Time Zone
TIME_ZONE: "Etc/UTC"

#Update NBOS package version here, we will install mentioned version

plugins for Example# NBOS_PACKAGE_VERSION: 3.3.36
NBOS_PACKAGE_VERSION: <Build No>
# Update Openstack dist code name like ussuri etc.
OPENSTACK_DIST: ussuri

#Need to add the following statement in nova sudoers file
#nova ALL = (root) NOPASSWD: /home/nbos/.virtenv/bin/privsep-helper
 *
#These changes require for nbosdm, Otherwise nbosdm will not work
#Are you sure? Please set variable to
#  UPDATE_NOVA_SUDOERS_FILE: proceed
#other wise ansible nbosdm installation will exit
UPDATE_NOVA_SUDOERS_FILE: proceed

##### Select snapshot storage type #####
#Details for NFS as snapshot storage , NFS_SHARES should begin with
 "-".
##True/False
NFS: True
NFS_SHARES:
          - sample_nfs_server_ip1:sample_share_path
          - sample_nfs_server_ip2:sample_share_path

#if NFS_OPTS is empty then default value will be
```

```
"nolock,soft,timeo=180,intr,lookupcache=none"
NFS_OPTS: ""

#### Details for S3 as snapshot storage
##True/False
S3: False
VAULT_S3_ACCESS_KEY: sample_s3_access_key
VAULT_S3_SECRET_ACCESS_KEY: sample_s3_secret_access_key
VAULT_S3_REGION_NAME: sample_s3_region_name
VAULT_S3_BUCKET: sample_s3_bucket
VAULT_S3_SIGNATURE_VERSION: default
#### S3 Specific Backend Configurations
#### Provide one of follwoing two values in s3_type variable,
string's case should be match
#Amazon/Other_S3_Compatible
s3_type: sample_s3_type
#### Required field(s) for all S3 backends except Amazon
VAULT_S3_ENDPOINT_URL: ""
#True/False
VAULT_S3_SECURE: True
VAULT_S3_SSL_CERT: ""

###details of nbosdmapi
##If SSL is enabled "NBOSDMAPI_ENABLED_SSL_APIS" value should be
nbosdmapi.
#NBOSDMAPI_ENABLED_SSL_APIS: nbosdmapi
##If SSL is disabled "NBOSDMAPI_ENABLED_SSL_APIS" value should be
empty.
NBOSDMAPI_ENABLED_SSL_APIS: ""
NBOSDMAPI_SSL_CERT: ""
NBOSDMAPI_SSL_KEY: ""

#### Any service is using Ceph Backend then set ceph_backend_enabled

value to True
#True/False
ceph_backend_enabled: False

#Set verbosity level and run playbooks with -vvv option to display
custom debug messages
verbosity_level: 3
```

NetBackup for OpenStack コンポーネントの配備

すでに配備されている Ansible OpenStack の場合は、次のコマンドを実行して NetBackup for OpenStack コンポーネントのみを配備します。

```
cd /opt/openstack-ansible/playbooks

# To create nbosdmapi container
openstack-ansible lxc-containers-create.yml

#To Deploy NetBackup for OpenStack components
openstack-ansible os-nbos-install.yml

#To configure Haproxy for nbosdmapi
openstack-ansible haproxy-install.yml
```

Ansible OpenStack がまだ配備されていない場合は、ネイティブの OpenStack 配備コマンドを実行して、OpenStack と NetBackup for OpenStack コンポーネントを一緒に配備します。ネイティブ配備コマンドの例を次に示します。

```
openstack-ansible setup-infrastructure.yml --syntax-check
openstack-ansible setup-hosts.yml
openstack-ansible setup-infrastructure.yml
openstack-ansible setup-openstack.yml
```

NetBackup for OpenStack 配備の検証

NetBackup for OpenStack datamover api サービスが配備され、開始されていることを確認します。コントローラノードで次のコマンドを実行します。

```
lxc-ls  # Check the nbosdmapi container is present on controller
node.
lxc-info -s controller_nbosdmapi_container-a11984bf
# Confirm running status of the container
```

NetBackup for OpenStack datamover サービスが配備され、計算ノードで開始されていることを確認します。計算ノードで次のコマンドを実行します。

```
systemctl status nbosdm.service
systemctl status nbos-objest-store  # If Storage backend is S3
df -h  # Verify the mount point is mounted on compute node(s)
```

NetBackup for OpenStack Horizon プラグイン、nbosdmclient、nbosjmclient が Horizon コンテナにインストールされていることを確認します。

Horizon コンテナで次のコマンドを実行します。

```
lxc-attach -n controller_horizon_container-1d9c055c

# To login on horizon container
apt list | egrep 'nbos-horizon-plugin|nbosjmclient|nbosdmclient '

# For ubuntu based container
yum list installed |egrep 'nbos-horizon-plugin|nbosjmclient|
nbosdmclient '
# For CentOS based container
```

コントローラノードで次のコマンドを実行して、haproxy の設定を検証します。

```
 haproxy -c -V -f /etc/haproxy/haproxy.cfg # Verify the keyword
nbosdm_service-back is present in output.
```

Kolla Ussuri へのインストール

次の手順を実行して、NetBackup for OpenStack を Kolla Ussuri にインストールします。

表 2-3 Kolla Ussuri へのインストール

手順	作業	説明
1	NetBackup for OpenStack ノードの nova ユーザー ID の変更	p.50 の「NetBackup for OpenStack ノードの nova ユーザー ID の変更」を参照してください。
2	バックアップターゲットの形式の選択	p.29 の「NetBackup for OpenStack バックアップターゲットの形式について」を参照してください。
3	NetBackup for OpenStack 配備スクリプトのコピー	p.51 の「NetBackup for OpenStack 配備スクリプトのコピー」を参照してください。
4	NetBackup for OpenStack 配備スクリプトの Kolla-ansible 配備スクリプトへのコピー	p.52 の「NetBackup for OpenStack 配備スクリプトの Kolla-ansible 配備スクリプトへのコピー」を参照してください。

手順	作業	説明
5	ローカルレジストリへの NetBackup for OpenStack イメージのプッシュ	p.53 の「ローカルレジストリへの NetBackup for OpenStack イメージのプッシュ」を参照してください。
6	NetBackup for OpenStack パラメータを設定するための globals.yml の編集	p.58 の「NetBackup for OpenStack パラメータを設定するための globals.yml の編集」を参照してください。
7	NetBackup for OpenStack スナップショットマウント機能の有効化	p.59 の「NetBackup for OpenStack スナップショットマウント機能の有効化」を参照してください。
8	NetBackup for OpenStack コンテナイメージのプル	p.61 の「NetBackup for OpenStack コンテナイメージのプル」を参照してください。
9	NetBackup for OpenStack コンポーネントの配備	p.62 の「NetBackup for OpenStack コンポーネントの配備」を参照してください。
10	NetBackup for OpenStack 配備の検証	p.62 の「NetBackup for OpenStack 配備の検証」を参照してください。

NetBackup for OpenStack ノードの nova ユーザー ID の変更

NetBackup for OpenStack VM は、デフォルトで nova ユーザー ID とグループ ID 162:162 を使用します。Kolla Ussuri OpenStack は、nova-compute コンテナでは常に nova ユーザー ID 162 とは限りません。NetBackup for OpenStack VM ノードの nova ユーザー ID は nova-compute コンテナと同じである必要があります。nova ID が 162:162 でない場合は、すべての NetBackup for OpenStack VM ノードで次の手順を実行します。

次の手順を実行する前に、ユーザー ID とグループ ID が NetBackup for OpenStack VM の他のどのサービスによっても使用されていないことを確認します。たとえば、計算ノードの nova ID が 997 の場合は、NetBackup for OpenStack VM の他のサービスでユーザー ID が使用されていないことを確認します。`rabbitmq` に 997 のユーザー ID が割り当てられ、NetBackup for OpenStack VM の `SSH` サービスに 997 のグループ ID が割り当てられている場合は、この ID を解放する必要があります。

```
#cat /etc/passwd | grep 997
#pid 997
#ps -ef | grep 997
#usermod -u 900 rabbitmq
#cat /etc/group | grep 997
#groupmod -g 901 ssh_keys
#reboot
```

1. ディレクトリ /home/stack に移動します。
2. nova_userid.sh ファイルに実行可能権限を割り当てます。

   ```
   #chmod +x nova_userid.sh
   ```

3. 正しい nova ID を使用するようにスクリプトを編集します。
4. スクリプトを実行します。

   ```
   #./nova_userid.sh
   ```

5. nova ユーザーとグループ ID が目的の値に変更されていることを確認します。

   ```
   #id nova
   ```

NetBackup for OpenStack 配備スクリプトのコピー

NetBackup for OpenStack 配備スクリプトをコピーする方法

1 nbos-cfg-scripts が /root またはその他のディレクトリの Kolla Ansible サーバーで利用可能であることを確認します。

2 ディレクトリを作成して切り替えて、NetBackup for OpenStack 配備スクリプトを解凍します。

```
mkdir nbos-cfg-scripts

cd nbos-cfg-scripts/
```

3 tar ファイルを解凍します。

```
tar -xvf nbos-cfg-scripts-<NBOS version number>.tar.gz
```

例: `tar -xvf nbos-cfg-scripts-9.1.2.20211021104525.tar.gz`

4 NetBackup for OpenStack Ansible の役割を Kolla-ansible 役割のディレクトリにコピーします。

```
cp -R kolla/roles/NetBackupOpenStack
/path/to/venv/share/kolla-ansible/ansible/roles/
```

NetBackup for OpenStack 配備スクリプトの Kolla-ansible 配備スクリプトへのコピー

NetBackup for OpenStack 配備スクリプトを Kolla-ansible 配備スクリプトにコピーする方法

1 `globals.yml` に NetBackup for OpenStack グローバル変数を追加します。

`globals.yml` のバックアップを作成します。

```
cp /etc/kolla/globals.yml /opt/
```

`globals.yml` に NetBackup for OpenStack グローバル変数を追加します。

```
cat kolla/NetBackupOpenStack_globals.yml >> /etc/kolla/globals.yml
```

2 kolla `passwords.yaml` ファイルに NetBackup for OpenStack パスワードを追加します。

`/etc/kolla/passwords.yml` に `NetBackupOpenStack_passwords.yml` を追加します。パスワードは空です。これらのパスワードを `/etc/kolla/passwords.yml` に手動で設定します。

`passwords.yml` のバックアップを作成します。

```
cp /etc/kolla/passwords.yml /opt/
```

`passwords.yml` に NetBackup for OpenStack グローバル変数を追加します。

```
cat kolla/NetBackupOpenStack_passwords.yml >>
/etc/kolla/passwords.yml
```

`/etc/kolla/passwords.yml` を編集します。ファイルの最後に NetBackup for OpenStack パスワードを設定します。

```
NetBackupOpenStack_keystone_password: <password>
NetBackupOpenStack_database_password: <password>
```

3 NetBackupOpenStack_site.yml コンテンツを kolla ansible の site.yml ファイルに追加します。

site.yml のバックアップを作成します。

```
cp /path/to/venv/share/kolla-ansible/ansible/site.yml /opt/
```

site.yml に NetBackup for OpenStack コードを追加します。

```
cat kolla/NetBackupOpenStack_site.yml >>
/path/to/venv/share/kolla-ansible/ansible/site.yml
```

4 クラウドの kolla-ansible インベントリファイルに NetBackupOpenStack_inventory.txt を追加します。

```
cat kolla/NetBackupOpenStack_inventory.txt >> <your inventory
file name path>
```

次に例を示します。

```
cat kolla/NetBackupOpenStack_inventory.txt >> /root/multinode
```

ローカルレジストリへの NetBackup for OpenStack イメージのプッシュ

ローカルレジストリに NetBackup for OpenStack イメージをプッシュするには、次のタスクを実行します。

表 2-4

手順	作業	説明
1	ローカルレジストリを実行します。	p.53 の「ローカルレジストリの実行」を参照してください。
2	tar からイメージをロードしてローカルリポジトリにプッシュします	p.54 の「tar からのイメージのロードとローカルリポジトリへのプッシュ」を参照してください。

ローカルレジストリの実行

Centos と Ubuntu の NetBackup for OpenStack のコンテナイメージを取得するには、ローカルレジストリを実行します。

ローカルレジストリを実行するには

◆ 配備ノードで次のコマンドを実行して、レジストリコンテナを起動します。

```
docker run -d -p 5001:5000 --restart=always --name
<local_registry_name> registry:2
```

<local_registry_name> レジストリ名。レジストリ名がない場合は、新しい名前を割り当てます。コマンドは、docker.io からレジストリイメージを取得し、そのコンテナを実行します。

tar からのイメージのロードとローカルリポジトリへのプッシュ

配備ノードで nbosdmapi、nbosdm、nbos-horizon-plugin の適切な tar ファイルが利用可能であることを確認します。

NBOS_Version	NetBackup for OpenStack のバージョン番号。
kolla-base-distro	CentOS または Ubuntu
kolla-install-type	バイナリまたはソース
FQDN	kolla 配備サーバーのホスト名。

tar からイメージをロードしてローカルリポジトリにプッシュするには

1 tar ファイルから NetBackup for OpenStack イメージをロードします。

次のコマンドを実行します。

- nbosdmapi

  ```
  docker load --input nbosdmapi-{{ kolla-base-distro }}:{{
  NBOS_version }}-ussuri.tar
  ```

  次に例を示します。

  ```
  docker load --input
  nbosdmapi-ubuntu-9.1.2.20211021104525-ussuri.tar
  ```

- nbosdm

  ```
  docker load i-input nbosdm-{{ kolla-base-distro }}:{{
  NBOS_version }}-ussuri.tar
  ```

  次に例を示します。

  ```
  docker load --input
  nbosdm-ubuntu-9.1.2.20211021104525-ussuri.tar
  ```

- nbos-horizon-plugin

  ```
  docker load --input nbos-horizon-plugin-{{ kolla-install-type
  }}-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri.tar
  ```

  次に例を示します。

```
docker load --input
nbos-horizon-plugin-source-ubuntu-9.1.2.20211021104525-ussuri.tar
```

2 適切な名前で NetBackup for OpenStack イメージにタグを付けます。

次のコマンドを実行します。

- nbosdmapi
  - `docker tag nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri nbos/nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri`
  - `docker tag nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri FQDN:5001/nbos/nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri`

  例:
  - `docker tag nbosdmapi-ubuntu:9.1.2.20211021104525-ussuri nbos/nbosdmapi-ubuntu:9.1.2.20211021104525-ussuri`
  - `docker tag nbosdmapi-ubuntu:9.1.2.20211021104525-ussuri deployment-vm.vxindia.veritas.com:5001/nbos/nbosdmapi-ubuntu:9.1.2.20211021104525-ussuri`
- nbosdm
  - `docker tag nbosdm-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri nbos/nbosdm-<kolla-base-distro>:<NBOS_version>-ussuri`
  - `docker tag nbosdm-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri FQDN:5001/nbos/nbosdm-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri`

  例:
  - `docker tag nbosdm-ubuntu:9.1.2.20211021104525-ussuri nbos/nbosdm-ubuntu:9.1.2.20211021104525-ussuri`
  - `docker tag nbosdm-ubuntu:9.1.2.20211021104525-ussuri deployment-vm.vxindia.veritas.com:5001/nbos/nbosdm-ubuntu:9.1.2.20211021104525-ussuri`
- nbos-horizon-plugin
  - `docker tag nbos-horizon-plugin-{{ kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri nbos/nbos-horion-plugin-{{ kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri`
  - `docker tag nbos-horizon-plugin-{{ kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri`

```
FQDN:5001/nbos/nbos-horizon-plugin-{{ kolla-install-type
}}-{{ kolla-base-distro }}:{{ NBOS_version }}-ussuri
```

例:

- ```
  docker tag
  nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-ussuri
  nbos/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-ussuri
  ```
- ```
  docker tag
  nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-ussuri
  deployment-vm.vxindia.veritas.com:5001/nbos/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-ussuri
  ```

3 タグ付けされたイメージをローカルレジストリにプッシュします。

次のコマンドを実行します。

- nbosdmapi

  ```
  docker push FQDN:5001/nbos/nbosdmapi-{{ kolla-base-distro }}:{{
  NBOS_version }}-ussuri
  ```

  次に例を示します。

  ```
  docker push
  deployment-vm.vxindia.veritas.com:5001/nbos/nbosdmapi-ubuntu:9.1.2.20211021104525-ussuri
  ```

- nbosdm

  ```
  docker push FQDN:5001/nbos/nbosdm-{{ kolla-base-distro }}:{{
  NBOS_version }}-ussuri
  ```

  次に例を示します。

  ```
  docker push
  deployment-vm.vxindia.veritas.com:5001/nbos/nbosdm-ubuntu:9.1.2.20211021104525-ussuri
  ```

- nbos-horizon-plugin

  ```
  docker push FQDN:5001/nbos/nbos-horizon-plugin-{{
  kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version
  }}-ussuri
  ```

  次に例を示します。

  ```
  docker push
  deployment-vm.vxindia.veritas.com:5001/nbos/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-ussuri
  ```

4 すべてのコントローラと計算ノードの /etc/docker/daemon.json に insecure-registries エントリを追加します。

daemon.json ファイルを開き、次のように変更を行います。

```
cat /etc/docker/daemon.json
{
  "log-opts": {
    "max-file": "5",
    "max-size": "50m"
  },
  "registry-mirrors": [
    "http://<deployment node ip>:4000"
  ],
  "insecure-registries": [
    "FQDN:5001"
  ]
}
```

5 配備ノードの /etc/docker/daemon.json に insecure-registries エントリを追加します。

/etc/docker/ ディレクトリが存在しない場合は、作成して daemon.json ファイルを作成します。

daemon.json ファイルを開き、次のように変更を行います。

```
cat /etc/docker/daemon.json
{ "insecure-registries":["FQDN:5001"] }
```

6 Docker を再起動します。

```
systemctl restart docker
```

7 指定したイメージがレジストリにプッシュ済みであることを確認します。

- コントローラと計算ノード: curl -X GET http://FQDN:5001/v2/_catalog
- 配備ノード: docker info

次に例を示します。

```
curl -X GET
http://deployment-vm.vxindia.veritas.com:5001/v2/_catalog
```

次に出力例を示します。

```
curl -X GET http://deployment-vm.vxindia.veritas.com:
5001/v2/_catalog
//Output should look like below:
{"repositories":["nbos/nbos-horizon-plugin-source-centos",
"nbos/nbosdm-centos","nbos/nbosdmapi-centos"]}
```

NetBackup for OpenStack パラメータを設定するための globals.yml の編集

/etc/kolla/globals.yml ファイルを編集して NetBackup for OpenStack バックアップターゲットとビルドの詳細を構成します。NetBackup for OpenStack 関連のパラメータは、globals.yml ファイルの最後にあります。NetBackupOpenStack タグ、バックアップターゲットの種類、バックアップターゲットの詳細などの情報を構成する必要があります。

編集できるパラメータのリストを次に示します。

表 2-5 globals.yml パラメータ

パラメータ	説明
NetBackupOpenStack_tag	コンテナタグ。
horizon_image_full	デフォルトでは、NetBackup for OpenStack Horizon コンテナは配備されません。このパラメータのコメントを解除して、Openstack Horizon コンテナの代わりに NetBackup for OpenStack コンテナを配備します。
NetBackupOpenStack_docker_username	NetBackup for OpenStack のデフォルト Docker ユーザー。(読み取り権限のみ)
NetBackupOpenStack_docker_password	NetBackup for OpenStack のデフォルトの Docker ユーザーのパスワード。
NetBackupOpenStack_docker_registry	NetBackup for OpenStack コンポーネントイメージを含むローカルレジストリ名。
NetBackupOpenStack_backup_target	■ nfs バックアップターゲットが NFS の場合は nfs。 ■ amazon_s3 バックアップターゲットが Amazon S3 の場合は amazon_s3。 ■ ceph_s3 バックアップターゲット形式が S3 で Amazon S3 ではない場合は ceph_s3。

パラメータ	説明
NetBackupOpenStack_nfs_shares	NFS 共有パス。 例: `192.168.145.110:/nfs/nbos`
NetBackupOpenStack_nfs_options	NFS マウントオプションを構成します。
NetBackupOpenStack_s3_access_key	amazon_s3 と ceph_s3 で有効です。
NetBackupOpenStack_s3_secret_key	amazon_s3 と ceph_s3 で有効です。
NetBackupOpenStack_s3_region_name	amazon_s3 と ceph_s3 で有効です。s3 ストレージに region パラメータがない場合は、デフォルト値のままになります。
NetBackupOpenStack_s3_bucket_name	s3 バケットの名前。 amazon_s3 と ceph_s3 で有効です
NetBackupOpenStack_s3_endpoint_url	s3 エンドポイント URL。 ceph_s3 でのみ有効です。
NetBackupOpenStack_s3_ssl_enabled	ceph_s3 でのみ有効です。SSL が有効な S3 エンドポイントの URL の場合は true に設定します。
NetBackupOpenStack_s3_ssl_cert_file_name	SSL が有効で、自己署名証明書がある場合、またはプライベート認証局によって発行された場合にのみ ceph_s3 で有効です。この場合、ceph s3 CA チェーンファイルを、Ansible サーバーの `/etc/kolla/config/nbos/` ディレクトリにコピーします。まだ存在しない場合は、このディレクトリを作成します。
NetBackupOpenStack_copy_ceph_s3_ssl_cert	SSL が有効で自己署名証明書があるか、プライベート認証局によって発行されていて、True に設定されている場合にのみ ceph_s3 で有効です。

NetBackup for OpenStack スナップショットマウント機能の有効化

NetBackup for OpenStack のスナップショットマウント機能を有効にするには、NetBackup for OpenStack バックアップターゲットを nova-compute コンテナと nova-libvirt コンテナで利用できるようにする必要があります。

`/path/to/venv/share/kolla-ansible/ansible/roles/nova-cell/defaults/main.yml` を編集し、`nova_libvirt_default_volumes` 変数を検索します。既存のボリュームの

リストに、NetBackup for OpenStack マウントバインド /var/nbos:/var/nbos:shared を追加します。

デフォルトの Kolla インストールの場合、変数は次のようになります。

```
nova_libvirt_default_volumes:
  - "{{ node_config_directory }}/nova-libvirt/:{{ container_config_
    directory }}/:ro"
  - "/etc/localtime:/etc/localtime:ro"
  - "{{ '/etc/timezone:/etc/timezone:ro' if ansible_os_family
    == 'Debian' else '' }}"
  - "/lib/modules:/lib/modules:ro"
  - "/run/:/run/:shared"
  - "/dev:/dev"
  - "/sys/fs/cgroup:/sys/fs/cgroup"
  - "kolla_logs:/var/log/kolla/"
  - "libvirtd:/var/lib/libvirt"
  - "{{ nova_instance_datadir_volume }}:/var/lib/nova/"
  - "{% if enable_shared_var_lib_nova_mnt | bool %}/var/lib/nova/mnt:

    /var/lib/nova/mnt:shared{% endif %}"
  - "nova_libvirt_qemu:/etc/libvirt/qemu"
  - "{{ kolla_dev_repos_directory ~ '/nova/nova:/var/lib/
     kolla/venv/lib/python' ~ distro_python_version ~ '
     /site-packages/nova' if nova_dev_mode | bool else '' }
  - "/var/nbos:/var/nbos:shared"
```

次に、同じファイル内の変数 nova_compute_default_volumes を検索し、マウントバインド /var/nbos:/var/nbos:shared をリストに追加します。

変更後は、デフォルトの Kolla インストールの場合、変数は次のようになります。

```
nova_compute_default_volumes:
  - "{{ node_config_directory }}/nova-compute/:{{ container_config_
    directory }}/:ro"
  - "/etc/localtime:/etc/localtime:ro"
  - "{{ '/etc/timezone:/etc/timezone:ro' if ansible_os_family
    == 'Debian' else '' }}"
  - "/lib/modules:/lib/modules:ro"
  - "/run:/run:shared"
  - "/dev:/dev"
  - "kolla_logs:/var/log/kolla/"
  - "{% if enable_iscsid | bool %}iscsi_info:/etc/iscsi{% endif %}"
```

```
  - "libvirtd:/var/lib/libvirt"
  - "{{ nova_instance_datadir_volume }}:/var/lib/nova/"
  - "{% if enable_shared_var_lib_nova_mnt | bool %}/var/lib/nova/mnt:/

    var/lib/nova/mnt:shared{% endif %}"
  - "{{ kolla_dev_repos_directory ~ '/nova/nova:/var/lib/kolla/venv/

     lib/python' ~ distro_python_version ~ '/site-packages/nova'
     if nova_dev_mode | bool else '' }}"
  - "/var/nbos:/var/nbos:shared"
```

Ironic 計算ノードを使用する場合は、同じファイルでもう 1 つのエントリを調整する必要があります。変数 `nova_compute_ironic_default_volumes` を検索し、リストに NBOS マウント `/var/nbos:/var/nbos:shared` を追加します。

変更後、変数は次のようになります。

```
nova_compute_ironic_default_volumes:
- "{{ node_config_directory }}/nova-compute-ironic/:{{
container_config_
  directory }}/:ro"
- "/etc/localtime:/etc/localtime:ro"
- "{{ '/etc/timezone:/etc/timezone:ro' if ansible_os_family ==
'Debian'
  else '' }}"
- "kolla_logs:/var/log/kolla/"
- "{{ kolla_dev_repos_directory ~ '/nova/nova:/var/lib/kolla/venv/lib/

   python' ~ distro_python_version ~ '/site-packages/nova' if nova_dev

    _mode | bool else '' }}"
- "/var/nbos:/var/nbos:shared"
```

NetBackup for OpenStack コンテナイメージのプル

既存のインベントリファイルに基づいて dockerhub から NetBackup for OpenStack コンテナのイメージをプルします。

```
kolla-ansible -i <inventory file name> pull --tags NetBackup for
OpenStack
```

次に例を示します。

```
kolla-ansible -i multinode pull --tags netbackup
```

NetBackup for OpenStack コンポーネントの配備

既存のインベントリファイルを使用して、次の配備コマンドを実行します。

```
kolla-ansible -i <inventory file name> deploy
```

次に例を示します。

```
kolla-ansible -i multinode deploy
```

NetBackup for OpenStack 配備の検証

NetBackup for OpenStack コンテナを実行するノードが利用可能で健全であることを確認します。

```
docker ps | grep nbosdmapi
```

次に出力例を示します。

```
3107046dce84   r7515-090-vm51.vxindia.veritas.com:
5001/nbos/nbosdmapi-ubuntu:10.0.0.1.1007-ussuri
"dumb-init --single-…"   9 days ago     Up 9 days
NetBackupOpenStack_datamover_api
```

```
docker ps | grep nbosdm
```

次に出力例を示します。

```
77f22039bd54   r7515-090-vm51.vxindia.veritas.com:
5001/nbos/nbosdm-ubuntu:10.0.0.1.1007-ussuri   "dumb-init
--single-…"   9 days ago     Up 4 days
NetBackupOpenStack_datamover
```

```
docker ps | grep horizon
```

次に出力例を示します。

```
dde1c91ed1a0   r7515-090-vm51.vxindia.veritas.com:
5001/nbos/nbos-horizon-plugin-binary-ubuntu:10.0.0.1.1007-ussuri
"dumb-init --single-…"   7 months ago   Up 7 months
horizon
```

NetBackup for OpenStack の構成

NetBackup for OpenStack 構成プロセスでは、Ansible スクリプトが使用されます。Ansible は、ここ数年で人気が高まった構成管理ツールです。NetBackup for OpenStack では、Ansible プレイブックを大規模に使用して NetBackup for OpenStack クラスタを構成しています。NetBackup for OpenStack 構成の問題をトラブルシューティングするには、Ansible プレイブックの出力に関する基本的な理解が必要です。

Ansible モジュールは本質的にべき等であるため、NetBackup for OpenStack クラスタを変更または再構成するために何度でも NetBackup for OpenStack 構成を実行できます。

VM が起動したら、ブラウザ (Chrome または Firefox) を NetBackup for OpenStack ノードの IP アドレスにポイントします。

これにより、NetBackup for OpenStack コンフィギュレータを含む NetBackup for OpenStack ダッシュボードが表示されます。

ユーザーは admin です。デフォルトのパスワードは password です。

初回ログイン後、admin パスワードの変更が要求されます。

NetBackup for OpenStack ではクラスタを一度設定する必要があり、NetBackup for OpenStack ダッシュボードはクラスタ全体の管理機能を提供します。

NetBackup for OpenStack Appliance に必要な詳細

未構成の NetBackup for OpenStack Appliance にログインすると、表示されるページがコンフィギュレータになります。コンフィギュレータには、NetBackup for OpenStack Appliance、OpenStack、バックアップストレージに関する情報が必要です。

NetBackup for OpenStack クラスタの情報

NetBackup for OpenStack クラスタが正しく動作するには、既存の環境に統合する必要があります。このブロックでは、NetBackup for OpenStack クラスタの動作の詳細に関する情報が求められます。

- コントローラノード
  - これは、NetBackup for OpenStack 仮想アプライアンスの IP アドレスとそのホスト名のリストです。
  - 形式:「=」で組み合わせたペアで構成されるカンマ区切りリスト。このリストの最初のノードはアクティブノードである必要があります。
  - 例:
    172.20.4.151=nbos-104-1,172.20.4.152=nbos-104-2,172.20.4.153=nbos-104-3'

NetBackup for OpenStack クラスタは 1 ノードクラスタと 3 ノードクラスタのみをサポートします。

- 仮想 IP アドレス
  - NetBackup for OpenStack クラスタの IP アドレス (必須)
  - 形式: IP/サブネット
  - 例: 172.20.4.150/24

警告: 仮想 IP は、単一ノードクラスタに対しても必須であり、コントローラノードで指定されたどの IP とも異なる必要があります。

- ネームサーバー
  - ネームサーバーのリスト。主に OpenStack サービスエンドポイントの解決に使用されます。
  - 形式: カンマ区切りリスト
  - 例: 8.8.8.8,172.20.4.1
- ドメイン検索順序
  - NetBackup for OpenStack クラスタが使用するドメイン。
  - 形式: カンマ区切りリスト
  - 例: nbos.io, nbos.demo
- NTP サーバー
  - NetBackup for OpenStack クラスタが使用する NTP サーバー
  - 形式: カンマ区切りリスト
  - 例: 0.pool.ntp.org,10.10.10.10
- タイムゾーン
  - NetBackup for OpenStack クラスタが内部的に使用するタイムゾーン
  - 形式: 事前に入力されたリスト
  - 例: UTC

OpenStack のクレデンシャル情報

NetBackup for OpenStack アプライアンスは 1 つの RHV 環境と統合します。このブロックでは、RHV クラスタへのアクセスと接続に必要な情報が要求されます。

- Keystone URL
  - 構成のための認証のフェッチに使用される Keystone エンドポイント
  - 形式: URL
  - 例: https://keystone.nbos.io:5000/v3
- エンドポイントの種類
  - OpenStack エンドポイントとの通信に使用するエンドポイントの種類を定義します
  - 形式: ラジオボタンの事前定義済みリスト

- 例: Public

Keystone エンドポイントに FQDN を使用する場合は、構成の前に少なくとも 1 つの DNS サーバーを構成する必要があります。

そうしないと、OpenStack クレデンシャルの検証は失敗します。

- ドメイン ID
  - 指定したユーザーとテナントが配置されているドメイン
  - 形式: ID
  - 例: Default
- 管理者
  - ドメイン管理者の役割を持つアカウントのユーザー名
  - 形式: 文字列
  - 例: Admin
- パスワード
  - 以前に指定したユーザーのパスワード
  - 形式: 文字列
  - 例: Password

NetBackup for OpenStack には、ドメイン管理者の役割のアクセス権が必要です。ユーザーにドメイン管理者の役割を提供するには、次のコマンドを使用できます。

```
openstack role add --domain <domain id> --user <username> admin
```

NetBackup for OpenStack コンフィギュレータは、指定されたクレデンシャルを使用して OpenStack にログインできる場合は、各エントリの後で検証します。

この検証は、すべてのエントリが設定されて正しい状態になるまで失敗します。

検証が成功すると、管理テナント、リージョン、およびトラスティの役割をエラーメッセージを表示せずに選択できます。

- 管理テナント
  - 指定したユーザーと一緒に使用するテナント
  - 形式: 事前に入力されたリスト
  - 例: Admin
- リージョン
  - ユーザーとテナントが配置されている OpenStack リージョン
  - 形式: 事前に入力されたリスト

- 例: RegionOne

- トラスティの役割
  - NetBackup for OpenStack 機能を使用するには、OpenStack の役割が必要です
  - 形式: 事前に入力されたリスト
  - 例: _member_

バックアップストレージの構成情報

このブロックは、NetBackup for OpenStack のインストールでバックアップの格納と読み込みに使用されるバックアップターゲットに関する必要な情報を要求します。

- OpenStack 配布
  - 各 OpenStack 配布では、特別なマウントポイントを使用する必要があります
  - 形式: 事前定義済みリスト
  - 配布リスト: RHOSP、Kolla Ansible、およびその他 (Packstack、Openstack-Ansible)
- バックアップストレージ
  - 使用するバックアップストレージプロトコルを定義します
  - 形式: ラジオボタンの事前定義済みリスト
  - 例: NFS

NFS プロトコルの使用

- NFS エクスポート
  - NFS ボリュームを使用するパスが見つかります
  - 形式: NFS ボリュームパスのカンマ区切りリスト
  - 例: 10.10.2.20:/upstream,10.10.5.100:/nfs2
- NFS オプション
  - NFS エクスポートのマウント時に NetBackup for OpenStack クラスタが使用する NFS オプション
  - 形式: NFS オプション
  - 例: nolock,soft,timeo=180,intr,lookupcache=none

事前定義済みの NFS オプションを使用し、変更が必要であることがわかっている場合にのみ変更してください。

NetBackup for OpenStack は事前定義済みの NFS オプションに対してテストしています。

S3 プロトコルの使用

- S3 互換
  - Amazon と他の S3 互換のストレージソリューションの切り替え
  - 形式: 事前定義済みリスト
  - 例: Amazon S3
- (S3 互換) エンドポイント URL
  - 提供された S3 互換ストレージに到達してアクセスするために使用する URL
  - 形式: URL
  - 例: objects.nbos.io
- アクセスキー
  - S3 ストレージにログインするために必要なアクセスキー
  - 形式: アクセスキー
  - 例: SFHSAFHPFFSVVBSVBSZRF
- シークレットキー
  - S3 ストレージにログインするために必要なシークレットキー
  - 形式: シークレットキー
  - 例: bfAEURFGHsnvd3435BdfeF
- リージョン
  - S3 バケットに対して構成されたリージョン (S3 のデフォルトは、リージョンなしで互換性のあるもののままにします)
  - 形式: 文字列
  - 例: us-east-1
- 署名バージョン
  - S3 ストレージへのサインインに使用する S3 署名バージョン
  - 形式: 文字列
  - 例: Default
- バケット名
  - バックアップターゲットとして使用するバケットの名前

- 形式: 文字列
- 例: nbos-backup

ポリシーのインポート

NetBackup for OpenStack Appliance を再初期化または再インストールする場合は、このボックスを選択して、バックアップターゲットにあるすべての一致するポリシーをインポートします。

メモ: 既存のテナントに割り当てられていないポリシーはインポートに失敗し、構成が完了したら手動で再割り当てする必要があります。

詳細設定

コンフィギュレータの最後に、詳細設定をアクティブ化できます。

このオプションをアクティブ化すると、NetBackup for OpenStack Job Manager と NetBackup for OpenStack Datamover API に使用される Keystone エンドポイントの構成が有効になります。

NetBackup for OpenStack Job Manager と NetBackup for OpenStack Datamover API の設定

NetBackup for OpenStack は 2 つのサービスに対して Keystone エンドポイントを生成します。NetBackup for OpenStack Datamover API と NetBackup for OpenStack Job Manager です。

最新の OpenStack インストールでは、エンドポイントの種類が複数のネットワークに分割されます。nbosdmapi エンドポイントと nbosjm エンドポイントの詳細設定によって、それに応じた NetBackup for OpenStack の設定が可能になります。

使用済み IP アドレスは、NetBackup for OpenStack クラスタに追加 VIP として追加されます。

これらのエンドポイントで使用される FQDN の場合、NetBackup for OpenStack コンフィギュレータは FQDN を解決して VIP として設定される IP を学習します。

NetBackup for OpenStack コンポーネントのインストール中に構成された設定に対して nbosdmapi 設定を確認することをお勧めします。

これらのエンドポイントが Keystone にすでに存在する場合、値は事前に入力され、変更できません。変更が必要な場合は、まず古い Keystone エンドポイントを削除します。

https を含む URL を指定すると、TLS が有効な構成が有効になり、証明書と接続された秘密鍵のアップロードが必要になります。

外部データベースの設定

NetBackup for OpenStack では、外部 MySQL または MariaDB データベースを使用できます。

このデータベースは、空の nbosjm データベースを作成し、nbosjm ユーザーを作成し、正しい権限を設定して準備する必要があります。このデータベースを作成するコマンドの例は次のとおりです。

```
create database nbosjm_auto;
CREATE USER 'nbos'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON nbosjm_auto.* TO 'nbos'@'10.10.10.67'
IDENTIFIED BY 'password';
```

NetBackup for OpenStack コンフィギュレータに接続文字列を指定します。

```
mysql://nbos:password@10.10.10.67/nbosjm_auto?charset=utf8
```

この値は、NetBackup for OpenStack ソリューションの初期構成時にのみ設定できます。

クラスタが内部データベースを使うように構成されている場合、接続文字列は次の構成の試行では表示されません。

外部データベースの場合、接続文字列は表示されますが、編集できません。

NetBackup for OpenStack サービスユーザーのパスワードの定義

NetBackup for OpenStack は OpenStack サービスプロジェクトにあるサービスユーザーを使用しています。

このサービスユーザーのパスワードはランダムに生成されるか、詳細設定で定義できます。

コンフィギュレータの起動

すべてのエントリが設定され、すべての検証にエラーがない状態になったら、コンフィギュレータを起動できます。

- ［完了 (Finish)］をクリックします
- 構成を開始するポップアップを再確認します
- コンフィギュレータが終了するまで待機します

コンフィギュレータの一部の要素には時間がかかります。コンフィギュレータが停止しているように見える場合でも、コンフィギュレータが終了するまで待機してください。コンフィギュレータが 6 時間後に終了しない場合は、ベリタスのサポートにお問い合わせください。

コンフィギュレータは Ansible といくつかの NetBackup for OpenStack 内部 API 呼び出しを使用しています。各構成ブロックの後、またはコンフィギュレータの終了後、Ansible 出力にアクセスできます。

構成が正常に終了すると、コンフィギュレータは NBOSVM ダッシュボードを仮想 IP にリダイレクトします。

インストール後の健全性チェック

NetBackup for OpenStack のインストールと構成が成功した後、次の手順を実行して NetBackup for OpenStack のインストールが正常であることを確認できます。

NetBackup for OpenStack Appliance サービスが実行中であることの確認

NetBackup for OpenStack は、NetBackup for OpenStack Appliance で 3 つの主要なサービスを使用します。

- nbosjm-api
- nbosjm-scheduler
- nbosjm-policies

それらは、systemctl status コマンドを使用して起動して実行中であることを確認できます。

```
systemctl status nbosjm-api
######
● nbosjm-api.service - nbosjm api service
   Loaded: loaded (/etc/systemd/system/nbosjm-api.service; disabled;

           vendor preset: disabled)
  Drop-In: /run/systemd/system/nbosjm-api.service.d
           └─50-pacemaker.conf
   Active: active (running) since Wed 2020-04-22 09:17:05 UTC; 1 day
 2h ago
 Main PID: 21265 (python)
    Tasks: 1
   CGroup: /system.slice/nbosjm-api.service
           └─21265 /home/rhv/myansible/bin/python /usr/bin/nbosjm-api

           --config-file=/etc/nbosjm/nbosjm.conf
```

```
systemctl status nbosjm-scheduler
######
● nbosjm-scheduler.service - nbosjm scheduler service
   Loaded: loaded (/etc/systemd/system/nbosjm-scheduler.service;
disabled;
           vendor preset: disabled)
  Drop-In: /run/systemd/system/nbosjm-scheduler.service.d
           └─50-pacemaker.conf
   Active: active (running) since Wed 2020-04-22 09:17:17 UTC; 1 day
 2h ago
 Main PID: 21512 (python)
    Tasks: 1
   CGroup: /system.slice/nbosjm-scheduler.service
           └─21512 /home/rhv/myansible/bin/python
/usr/bin/nbosjm-scheduler
           --config-file=/etc/nbosjm/nbosjm.conf


systemctl status nbosjm-policies
######
● nbosjm-policies.service - nbosjm policies service
   Loaded: loaded (/etc/systemd/system/nbosjm-policies.service;
enabled;
           vendor preset: disabled)
   Active: active (running) since Wed 2020-04-22 09:15:43 UTC; 1 day
 2h ago
 Main PID: 20079 (python)
    Tasks: 33
   CGroup: /system.slice/nbosjm-policies.service
           ├─20079 /home/rhv/myansible/bin/python
/usr/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           ├─20180 /home/rhv/myansible/bin/python
/usr/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           [...]
           ├─20181 /home/rhv/myansible/bin/python
/usr/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           ├─20233 /home/rhv/myansible/bin/python
/usr/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
```

```
           ├─20236 /home/rhv/myansible/bin/python
/usr/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           └─20237 /home/rhv/myansible/bin/python
/usr/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
```

NetBackup for OpenStack ペースメーカーと NGINX クラスタの確認

NetBackup for OpenStack Appliance の健全性を確認する 2 つ目のコンポーネントは、NGINX とペースメーカーのクラスタです。

```
pcs status
######
Cluster name: NetBackup for OpenStack

WARNINGS:
Corosync and pacemaker node names do not match (IPs used in setup?)
Stack: corosync
Current DC: om_nbosvm (version 1.1.19-8.el7_6.1-c3c624ea3d) -
chapterition with quorum
Last updated: Wed Dec 5 12:25:02 2018
Last change: Wed Dec 5 09:20:08 2018 by root via cibadmin on om_nbosvm
1 node configured
4 resources configured

Online: [ om_nbosvm ]
Full list of resources:
virtual_ip (ocf::'heartbeat:IPaddr2): Started om_nbosvm
nbosjm-api (systemd:nbosjm-api): Started om_nbosvm
nbosjm-scheduler (systemd:nbosjm-scheduler): Started om_nbosvm
Clone Set: lb_nginx-clone [lb_nginx]
Started: [ om_nbosvm ]
Daemon Status:
corosync: active/enabled
pacemaker: active/enabled
pcsd: active/enabled
```

NetBackup for OpenStack Appliance の API 接続の検証

選択したエンドポイントで NetBackup for OpenStack API の可用性を確認することをお勧めします。

次の curl コマンドの例では、利用可能なポリシー形式が一覧表示され、接続が利用可能で動作していることを確認できます。

```
curl http://10.10.2.34:8780/v1/8e16700ae3614da4ba80a4e57d60cdb9/
policy_types/detail -X GET -H "X-Auth-Project-Id: admin"
-H "User-Agent: python-nbosjmclient" -H "Accept:
application/json" -H "X-Auth-Token:
gAAAAABe40NVFEtJeePpk1F9QGGh1LiGnHJVLlgZx9t0HRrK9rC5vq
KZJRkpAcW1oPH6Q9K9peuHiQrBHEs1-g75Na4xOEESR0LmQJUZP6n3
7fLfDL_D-hlnjHJZ68iNisIP1fkm9FGSyoyt6IqjO9E7_YVRCTCqNLJ
67ZkqHuJh1CXwShvjvjw
```

その他のコマンドと X-Auth-Token を生成する方法については、API ガイドを参照してください。

nbosdm サービスが起動して実行されていることの検証

nbosdm サービスは、すべての計算ノードにインストールされたデータムーバーです。インストール後に状態を確認することをお勧めします。

```
[root@upstreamcompute1 ~]# systemctl status tripleo-nbosdm.service
● tripleo_nbosdm.service - nbosdm container
   Loaded: loaded (/etc/systemd/system/tripleo_nbosdm.service;
enabled;
           vendor preset: disabled)
   Active: active (running) since Wed 2020-06-10 10:07:28 EDT; 1 day
 19h ago
 Main PID: 10384 (python)
    Tasks: 21
   CGroup: /system.slice/tripleo_nbosdm.service
           └─10384 /usr/bin/python /usr/bin/nbosdm
--config-file=/etc...

Jun 12 03:15:33 upstreamcompute1 python[10384]: libvirt: QEMU Driver

error :...d
Jun 12 03:15:33 upstreamcompute1 python[10384]: libvirt: QEMU Driver

error :...d
Jun 12 03:16:11 upstreamcompute1 python[10384]: libvirt: QEMU Driver

error :...d
```

```
Jun 12 03:16:31 upstreamcompute1 sudo[13977]:     nova : TTY=unknown
 ;
PWD=/...n
Jun 12 03:16:33 upstreamcompute1 sudo[14004]:     nova : TTY=unknown
 ;
PWD=/ ...
Jun 12 05:15:33 upstreamcompute1 python[10384]: libvirt: QEMU Driver

error :...d
Jun 12 05:15:33 upstreamcompute1 python[10384]: libvirt: QEMU Driver

error :...d
Jun 12 05:16:11 upstreamcompute1 python[10384]: libvirt: QEMU Driver

error :...d
Jun 12 05:16:29 upstreamcompute1 sudo[23356]:     nova : TTY=unknown
 ;
PWD=/...n
Jun 12 05:16:32 upstreamcompute1 sudo[23422]:     nova : TTY=unknown
 ;
PWD=/ ...
Hint: Some lines were ellipsized, use -l to show in full.
```

NFS ボリュームが正しくマウントされていることの検証

NetBackup for OpenStack は NFS バックアップターゲットを NetBackup for OpenStack Appliance と計算ノードにマウントします。

これらが正しくマウントされていることを確認するには、次のチェックを行うことをお勧めします。

最初の df -h で /var/NetBackupOpenStack-mounts/<hash-value> を検索します

```
df -h
######
Filesystem                          Size  Used Avail Use% Mounted on
devtmpfs                            63G     0   63G   0% /dev
tmpfs                               63G   16K   63G   1% /dev/shm
tmpfs                               63G   35M   63G   1% /run
tmpfs                               63G     0   63G   0% /sys/fs/cgroup
/dev/mapper/rhvh-rhvh--             7.1T  3.7G  6.8T   1% /
4.3.8.1--0.20200126.0+1
/dev/sda2                           976M  198M  712M  22% /boot
/dev/mapper/rhvh-var                15G  1.9G   12G  14% /var
```

```
/dev/mapper/rhvh-home             976M  2.6M  907M   1% /home
/dev/mapper/rhvh-tmp              976M  2.6M  907M   1% /tmp
/dev/mapper/rhvh-var_log          7.8G  230M  7.2G   4% /var/log
/dev/mapper/rhvh-var_log_audit    2.0G   17M  1.8G   1% /var/log/audit
/dev/mapper/rhvh-var_crash        9.8G   37M  9.2G   1% /var/crash
30.30.1.4:/rhv_backup             2.0T  5.3G  1.9T   1%
/var/NetBackupOpen
Stack-mounts/MzAuMzAuMS40Oi9yaHZfYmFja3Vw
30.30.1.4:/rhv_data               2.0T   37G  2.0T   2%
/rhev/data-center/
mnt/30.30.1.4:_rhv__data
tmpfs                             13G     0   13G   0% /run/user/0
30.30.1.4:/rhv_iso                2.0T   37G  2.0T   2%
/rhev/data-center/
mnt/30.30.1.4:_rhv__iso
```

次に、NetBackup for OpenStack Appliance と RHV ホストからユーザー nova:nova (uid = 36/ gid = 36) として読み取り、書き込み、削除のテストを行います。

```
su nova
######
[nova@nbosvm MTAuMTAuMi4yMDovdXBzdHJlYW0=]$ touch foo
[nova@nbosvm MTAuMTAuMi4yMDovdXBzdHJlYW0=]$ ll
total 24
drwxr-xr-x  3 nova nova 4096 Apr  2 17:27 nbosdm_tasks
-rw-r--r--  1 nova nova    0 Apr 23 12:25 foo
drwxr-xr-x  2 nova nova 4096 Apr  2 15:38 test-cloud-id
drwxr-xr-x 10 nova nova 4096 Apr 22 11:00 policy_1540698c-8e22-4dd1-
a898-8f49cd1a898c
drwxr-xr-x  9 nova nova 4096 Apr  8 15:21 policy_51517816-6d5a-4fce-
9ac7-46ee1e09052c
drwxr-xr-x  6 nova nova 4096 Apr 22 11:30 policy_77fb42d2-8d34-4b8d-
bfd5-4263397b636c
drwxr-xr-x  5 nova nova 4096 Apr 23 06:15 policy_85bf16ed-d4fd-49a6-
a753-98c5ca6e906b
[nova@nbosvm MTAuMTAuMi4yMDovdXBzdHJlYW0=]$ rm foo
[nova@nbosvm MTAuMTAuMi4yMDovdXBzdHJlYW0=]$ ll
total 24
drwxr-xr-x  3 nova nova 4096 Apr  2 17:27 nbosdm_tasks
drwxr-xr-x  2 nova nova 4096 Apr  2 15:38 test-cloud-id
drwxr-xr-x 10 nova nova 4096 Apr 22 11:00 policy_1540698c-8e22-4dd1-
a898-8f49cd1a898c
drwxr-xr-x  9 nova nova 4096 Apr  8 15:21 policy_51517816-6d5a-4fce-
```

```
9ac7-46ee1e09052c
drwxr-xr-x  6 nova nova 4096 Apr 22 11:30 policy_77fb42d2-8d34-4b8d-
bfd5-4263397b636c
drwxr-xr-x  5 nova nova 4096 Apr 23 06:15 policy_85bf16ed-d4fd-49a6-
a753-98c5ca6e906b
```

NetBackup for OpenStack のアンインストール

NetBackup for OpenStack のアンインストールは、インストールされている OpenStack 配布によって異なります。おおまかなプロセスは、すべての配布で同じです。

1. Horizon プラグインまたは NetBackup OpenStack Horizon コンテナをアンインストールします。
2. nbosdmapi コンテナをアンインストールします。
3. nbosdm をアンインストールします。
4. NetBackup for OpenStack クラスタを削除します。

RHOSP からのアンインストール

次の手順を実行して、RHOSP から NetBackup for OpenStack をアンインストールします。

NetBackup for OpenStack Datamover API サービスのクリーニング	p.77 の「NetBackup for OpenStack Datamover API サービスのクリーニング」を参照してください。
NetBackup for OpenStack Datamover サービスのクリーニング	p.78 の「NetBackup for OpenStack Datamover サービスのクリーニング」を参照してください。
NetBackup for OpenStack haproxy リソースのクリーニング	p.79 の「NetBackup for OpenStack haproxy リソースのクリーニング」を参照してください。
NetBackup for OpenStack Keystone リソースのクリーニング	p.80 の「NetBackup for OpenStack Keystone リソースのクリーニング」を参照してください。
NetBackup for OpenStack データベースリソースのクリーニング	p.80 の「NetBackup for OpenStack データベースリソースのクリーニング」を参照してください。
オーバークラウドの配備コマンドを元に戻す	p.81 の「オーバークラウドの配備コマンドを元に戻す」を参照してください。
元の RHOSP Horizon コンテナの復元	p.81 の「元の RHOSP Horizon コンテナの復元」を参照してください。

NetBackup for OpenStack VM クラスタの破棄 p.82 の「NetBackup for OpenStack VM クラスタの破棄」を参照してください。

NetBackup for OpenStack Datamover API サービスのクリーニング

NetBackup for OpenStack Datamover API サービスが実行されているすべてのノードで、次の手順を実行する必要があります。これらのノードは、エントリ `OS::TripleO::Services::nbosdmapi` を含む役割の `roles_data.yaml` を確認することによって識別できます。

NetBackup for OpenStack Datamover API サービスを実行する役割が識別されると、次のコマンドでサービスからノードがクリーンアップされます。

警告: すべてのコマンドを root として、または sudo 権限を持つユーザーとして実行します。

`nbosdmapi` コンテナを停止します。

```
# For RHOSP16.1 onwards
systemctl disable tripleo_nbosdmapi.service
systemctl stop tripleo_nbosdmapi.service
podman stop nbosdmapi
```

`nbosdmapi` コンテナを削除します。

```
# For RHOSP16.1 onwards
podman rm nbosdmapi
podman rm nbosdmapi_init_log
podman rm nbosdmapi_db_sync
```

NetBackup for OpenStack Datamover API サービスの conf ディレクトリをクリーンアップします。

```
rm -rf /var/lib/config-data/puppet-generated/nbosdmapi
rm /var/lib/config-data/puppet-generated/nbosdmapi.md5sum
```

NetBackup for OpenStack Datamover API サービスの log ディレクトリをクリーンアップします。

```
rm -rf /var/log/containers/nbosdmapi/
```

NetBackup for OpenStack Datamover サービスのクリーニング

NetBackup for OpenStack Datamover サービスが実行されているすべてのノードで、次の手順を実行する必要があります。これらのノードは、エントリ `OS::TripleO::Services::nbosdm` を含む役割の `roles_data.yaml` を確認することによって識別できます。

NetBackup for OpenStack Datamover API サービスを実行する役割が識別されると、次のコマンドでサービスからノードがクリーンアップされます。

警告: すべてのコマンドを root として、または sudo 権限を持つユーザーとして実行します。

`nbosdm` コンテナを停止します。

```
# For RHOSP16.1 onwards
systemctl disable tripleo_nbosdm.service
systemctl stop tripleo_nbosdm.service
podman stop nbosdm
```

`nbosdm` コンテナを削除します。

```
# For RHOSP16.1 onwards
podman rm nbosdm
```

計算ホストの NetBackup for OpenStack バックアップターゲットのマウントを解除します。

```
## Following steps applicable for all supported RHOSP releases.

# Check NetBackup for OpenStack backup target mount point
mount | grep NetBackup

# Unmount it
-- If it's NFS  (COPY UUID_DIR from your compute host using above
command)
umount /var/lib/nova/NetBackupOpenStack-mounts/<UUID_DIR>

-- If it's S3
umount /var/lib/nova/NetBackupOpenStack-mounts

# Verify that it's unmounted
```

```
mount | grep NetBackup

df -h  | grep NetBackup

# Remove mount point directory after verifying that backup target
unmounted
successfully.
# Otherwise actual data from backup target may get cleaned.

rm -rf /var/lib/nova/NetBackupOpenStack-mounts
```

NetBackup for OpenStack Datamover サービスの conf ディレクトリをクリーンアップします。

```
rm -rf /var/lib/config-data/puppet-generated/nbosdm/
rm /var/lib/config-data/puppet-generated/nbosdm.md5sum
```

NetBackup for OpenStack Datamover サービスの log ディレクトリをクリーンアップします。

```
rm -rf /var/log/containers/nbosdm/
```

NetBackup for OpenStack haproxy リソースのクリーニング

haproxy サービスが実行されているすべてのノードで、次の手順を実行する必要があります。これらのノードは、エントリ `OS::TripleO::Services::HAproxy` を含む役割の `roles_data.yaml` を確認することによって識別できます。

NetBackup for OpenStack Datamover API サービスを実行する役割が識別されると、次のコマンドですべての NetBackup for OpenStack リソースからノードがクリーンアップされます。

警告: すべてのコマンドを root として、または sudo 権限を持つユーザーとして実行します。

HAProxy ノードで次のファイルを編集し、すべての NetBackup for OpenStack エントリを削除します。

`/var/lib/config-data/puppet-generated/haproxy/etc/haproxy/haproxy.cfg`

これらのエントリの例:

```
listen nbosdmapi
```

```
  bind 172.25.3.60:13784 transparent ssl crt /etc/pki/tls/private/
  overcloud_endpoint.pem
  bind 172.25.3.60:8784 transparent
  http-request set-header X-Forwarded-Proto https if { ssl_fc }
  http-request set-header X-Forwarded-Proto http if !{ ssl_fc }
  http-request set-header X-Forwarded-Port %[dst_port]
  option httpchk
  option httplog
  server overcloud-controller-0.internalapi.localdomain
172.25.3.59:8784
  check fall 5 inter 2000 rise 2
```

すべての編集が完了したら、haproxy コンテナを再起動します。

```
# For RHOSP16.1 onwards
podman restart haproxy-bundle-podman-0
```

NetBackup for OpenStack Keystone リソースのクリーニング

NetBackup for OpenStack は Keystone にサービスとユーザーを登録します。それらを登録解除して削除する必要があります。

```
openstack service delete nbosdmapi
openstack user delete nbosdmapi
```

NetBackup for OpenStack データベースリソースのクリーニング

NetBackup for OpenStack は nbosdmapi サービスのデータベースを作成します。このデータベースはクリーニングする必要があります。

データベースクラスタにログインします。

```
## On RHOSP
podman exec -it galera-bundle-podman-0 mysql -u root
```

次の SQL ステートメントを実行して、データベースをクリーンアップします。

```
## Clean database
DROP DATABASE nbosdmapi;

## Clean nbosdmapi user
```

```
MariaDB [mysql]> select user, host from mysql.user where
user='nbosdmapi';
+-----------+-------------+
| user      | host        |
+-----------+-------------+
| nbosdmapi | 172.25.2.10 |
| nbosdmapi | 172.25.2.8  |
+-----------+-------------+
2 rows in set (0.00 sec)

=> Delete those user accounts
MariaDB [mysql]> DROP USER nbosdmapi@172.25.2.10;
Query OK, 0 rows affected (0.82 sec)

MariaDB [mysql]> DROP USER nbosdmapi@172.25.2.8;
Query OK, 0 rows affected (0.05 sec)

=> Verify that nbosdmapi user got cleaned
MariaDB [mysql]> select user, host from mysql.user where
user='nbosdmapi';
Empty set (0.00 sec)
```

オーバークラウドの配備コマンドを元に戻す

オーバークラウドの配備コマンドで使用されている roles_data.yaml から次のエントリを削除します。

- `OS::TripleO::Services::nbosdmapi`
- `OS::TripleO::Services::nbosdm`

NetBackup for OpenStack の配備前に使用したオーバークラウドの配備コマンドが引き続き利用可能な場合は、それを直接使用できます。

次の手順に従って、すべての NetBackup for OpenStack エントリからオーバークラウドの配備コマンドをクリーンアップします。

1. nbos_env.yaml エントリを削除します。
2. NetBackup OpenStack のエンドポイントのマップファイルを削除します。既存のファイルがある場合は元のマップファイルで置き換えます。

元の RHOSP Horizon コンテナの復元

クリーンアップしたオーバークラウドの配備コマンドを実行します。

NetBackup for OpenStack VM クラスタの破棄

KVM ノードで実行されているすべての VM を一覧表示します

```
virsh list
```

NetBackup for OpenStack VM を破棄します

```
virsh destroy <NetBackup for OpenStack VM Name or ID>
```

NetBackup for OpenStack VM を未定義にします

```
virsh undefine <NetBackup for OpenStack VM name>
```

KVM ホストストレージから NetBackup for OpenStack VM ディスクを削除します

Ansible OpenStack からのアンインストール

NetBackup for OpenStack を Ansible OpenStack からアンインストールするには、次のタスクを実行します。

NetBackup for OpenStack サービスのアンインストール	p.83 の「NetBackup for OpenStack サービスのアンインストール」を参照してください。
NetBackup for OpenStack Datamover API コンテナの破棄	p.83 の「NetBackup for OpenStack Datamover API コンテナの破棄」を参照してください。
openstack_user_config.yml のクリーニング	p.83 の「openstack_user_config.yml のクリーニング」を参照してください。
user_variables.yml の NetBackup for OpenStack haproxy 設定の削除	p.84 の「user_variables.yml の NetBackup for OpenStack haproxy 設定の削除」を参照してください。
NetBackup for OpenStack Datamover API インベントリファイルの削除	p.84 の「NetBackup for OpenStack Datamover API インベントリファイルの削除」を参照してください。
NetBackup for OpenStack Datamover API サービスエンドポイントの削除	p.84 の「NetBackup for OpenStack Datamover API サービスエンドポイントの削除」を参照してください。
NetBackup for OpenStack Datamover API データベースとユーザーの削除	p.85 の「NetBackup for OpenStack Datamover API データベースとユーザーの削除」を参照してください。

rabbitmq コンテナからの nbosdmapi rabbitmq ユーザーの削除	p.85 の「rabbitmq コンテナからの nbosdmapi rabbitmq ユーザーの削除」を参照してください。
haproxy のクリーニング	p.85 の「haproxy のクリーニング」を参照してください。
計算ノードからの証明書の削除	p.86 の「計算ノードからの証明書の削除」を参照してください。
NetBackup for OpenStack VM クラスタの破棄	p.86 の「NetBackup for OpenStack VM クラスタの破棄」を参照してください。

NetBackup for OpenStack サービスのアンインストール

NetBackup for OpenStack Ansible OpenStack プレイブックを実行して、NetBackup for OpenStack サービスをアンインストールできます。

```
cd /opt/openstack-ansible/playbooks
openstack-ansible os-nbos-install.yml --tags "nbos-all-uninstall"
```

NetBackup for OpenStack Datamover API コンテナの破棄

NetBackup for OpenStack Datamover API コンテナを完全に削除するには、次の Ansible プレイブックを実行します。

```
cd /opt/openstack-ansible/playbooks
openstack-ansible lxc-containers-destroy.yml --limit "DMPAI
CONTAINER_NAME"
```

openstack_user_config.yml のクリーニング

`nbosdmapi_hosts` と `nbos_compute_hosts` のエントリを `/etc/openstack_deploy/openstack_user_config.yml` から削除します

```
#nbosdmapi
nbos-nbosdmapi_hosts:
  infra-1:
    ip: 172.26.0.3
  infra-2:
    ip: 172.26.0.4

#nbos-datamover
nbos_compute_hosts:
```

```
  infra-1:
    ip: 172.26.0.7
  infra-2:
    ip: 172.26.0.8
```

user_variables.yml の NetBackup for OpenStack haproxy 設定の削除

/etc/openstack_deploy/user_variables.yml からの NetBackup for OpenStack Datamover API 設定の削除

```
# Datamover haproxy setting
haproxy_extra_services:
  - service:
       haproxy_service_name: nbosdm_service
      haproxy_backend_nodes: "{{ groups['nbosdmapi_all'] | default([])
 }}"
       haproxy_ssl: "{{ haproxy_ssl }}"
       haproxy_port: 8784
       haproxy_balance_type: http
       haproxy_balance_alg: roundrobin
       haproxy_timeout_client: 10m
       haproxy_timeout_server: 10m
       haproxy_backend_options:
         - "httpchk GET / HTTP/1.0¥¥r¥¥nUser-agent:¥¥
osa-haproxy-healthcheck"
```

NetBackup for OpenStack Datamover API インベントリファイルの削除

```
rm /opt/openstack-ansible/inventory/env.d/nbos-nbosdmapi.yml
```

NetBackup for OpenStack Datamover API サービスエンドポイントの削除

```
 source cloudadmin.rc
 openstack endpoint delete "internal datamover service endpoint_id"
 openstack endpoint delete "public datamover service endpoint_id"
 openstack endpoint delete "admin datamover service endpoint_id"
```

NetBackup for OpenStack Datamover API データベースとユーザーの削除

- galera コンテナに入ります。
- mysql データベースエンジンで root ユーザーとしてログインします。
- nbosdmapi データベースを削除します。
- nbosdmapi ユーザーを削除します

```
lxc-attach -n "GALERA CONTAINER NAME"
mysql -u root -p "root password"
DROP DATABASE nbosdmapi;
DROP USER nbosdmapi;
```

rabbitmq コンテナからの nbosdmapi rabbitmq ユーザーの削除

- rabbitmq コンテナに入ります。
- nbosdmapi ユーザーを削除します。
- nbosdmapi vhost を削除します。

```
lxc-attach -n "RABBITMQ CONTAINER NAME"
rabbitmqctl delete_user nbosdmapi
rabbitmqctl delete_vhost /nbosdmapi
```

haproxy のクリーニング

/etc/haproxy/conf.d/nbosdm_service ファイルを削除します。

```
rm  /etc/haproxy/conf.d/nbosdm_service
```

/etc/haproxy/haproxy.cfg ファイルから HAproxy 構成エントリを削除します。

```
frontend nbosdm_service-front-1
    bind hostname:8784 ssl crt /etc/ssl/private/
    haproxy.pem ciphers ECDH+AESGCM:DH+AESGCM:ECDH
    +AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM
    :RSA+AES:!aNULL:!MD5:!DSS
    option httplog
    option forwardfor except 127.0.0.0/8
```

```
    reqadd X-Forwarded-Proto:¥ https
    mode http
    default_backend nbosdm_service-back

frontend nbosdm_service-front-2
    bind 172.26.1.2:8784
    option httplog
    option forwardfor except 127.0.0.0/8
    mode http
    default_backend nbosdm_service-back


backend nbosdm_service-back
    mode http
    balance leastconn
    stick store-request src
    stick-table type ip size 256k expire 30m
    option forwardfor
    option httplog
    option httpchk GET / HTTP/1.0¥r¥nUser-agent:¥
osa-haproxy-healthcheck


    server controller_nbosdmapi_container-bf17d5b3 172.26.1.75:8784

    check port 8784 inter 12000 rise 1 fall 1
```

HAproxy サービスを再起動します。

```
systemctl restart haproxy
```

計算ノードからの証明書の削除

```
rm -rf /opt/config-certs/rabbitmq
rm -rf /opt/config-certs/s3
```

NetBackup for OpenStack VM クラスタの破棄

KVM ノードで実行されているすべての VM を一覧表示します

```
virsh list
```

NetBackup for OpenStack VM を破棄します

```
virsh destroy <NetBackup for OpenStack VM Name or ID>
```

NetBackup for OpenStack VM を未定義にします

```
virsh undefine <NetBackup for OpenStack VM name>
```

KVM ホストストレージから NetBackup for OpenStack VM ディスクを削除します

Kolla Openstack からのアンインストール

NetBackupOpenStack_datamover_api コンテナのクリーニング

コンテナは、NetBackupOpenStack_datamover_api コンテナが実行されているすべてのノードでクリーニングする必要があります。Kolla Openstack インベントリファイルは、サービスでノードを識別するのに役立ちます。

NetBackupOpenStack_datamover_api コンテナをクリーニングするには、次の手順を実行する必要があります。

NetBackupOpenStack_datamover_api コンテナをクリーニングする方法

1. NetBackupOpenStack_datamover_api コンテナを停止します。

   ```
   docker stop NetBackupOpenStack_datamover_api
   ```

2. NetBackupOpenStack_datamover_api コンテナを削除します。

   ```
   docker rm NetBackupOpenStack_datamover_api
   ```

3. /etc/kolla/nbosdmapi ディレクトリをクリーニングします。

   ```
   rm -rf /etc/kolla/nbosdmapi
   ```

4. NetBackupOpenStack_datamover_api コンテナのログディレクトリをクリーニングします。

   ```
   rm -rf /var/log/kolla/nbosdmapi/
   ```

NetBackupOpenStack_datamover コンテナのクリーニング

コンテナは、NetBackupOpenStack_datamover コンテナが実行されているすべてのノードでクリーニングする必要があります。Kolla Openstack インベントリファイルは、サービスでノードを識別するのに役立ちます。

NetBackupOpenStack_datamover コンテナをクリーニングする方法

1. NetBackupOpenStack_datamover コンテナを停止します。

   ```
   docker stop NetBackupOpenStack_datamover
   ```

2. NetBackupOpenStack_datamover コンテナを削除します。

   ```
   docker rm NetBackupOpenStack_datamover
   ```

3. /etc/kolla/nbosdm ディレクトリをクリーニングします。

   ```
   rm -rf /etc/kolla/nbosdm
   ```

4. NetBackupOpenStack_datamover コンテナのログディレクトリをクリーニングします。

   ```
   rm -rf /var/log/kolla/nbosdm/
   ```

NetBackupOpenStack Datamover API の haproxy のクリーニング

NetBackupOpenStack Datamover API エントリは、すべての haproxy ノードでクリーニングする必要があります。Kolla Openstack インベントリファイルは、サービスでノードを識別するのに役立ちます。

NetBackupOpenStack Datamover API の haproxy をクリーニングする方法

1. `rm /etc/kolla/haproxy/services.d/nbosdmapi.cfg`
2. `docker restart haproxy`

Kolla Ansible 配備のクリーニング手順

次の場所からすべての NetBackup for OpenStack 関連エントリを削除します。

- /path/to/venv/share/kolla-ansible/ansible/roles/ 役割 NetBackup for OpenStack があります。
- /etc/kolla/globals.yml ファイルの最後に NetBackup for OpenStack エントリが追加されます。
- /etc/kolla/passwords.yml ファイルの最後に NetBackup for OpenStack エントリが追加されていました。
- /path/to/venv/share/kolla-ansible/ansible/site.yml ファイルの最後に NetBackup for OpenStack エントリが追加されていました。
- /root/multinode このサンプルインベントリファイルの最後に NetBackup for OpenStack エントリが追加されます。

元の Horizon コンテナへの復帰

NetBackup for OpenStack Horizon コンテナを元の Kolla Ansible Horizon コンテナに置き換えるには、配備コマンドを実行します。

```
kolla-ansible -i multinode deploy
```

Keystone リソースのクリーニング

NetBackup for OpenStack は nbosdmapi ユーザーで nbosdmapi サービスを作成しました。次のコマンドを実行して、Keystone リソースをクリーニングします。

```
openstack service delete nbosdmapi
```

```
openstack user delete nbosdmapi
```

NetBackup for OpenStack データベースリソースのクリーニング

NetBackup for OpenStack Datamover API サービスには、OpenStack データベース内に独自のデータベースがあります。

NetBackup for OpenStack データベースリソースをクリーニングする方法

1. root ユーザーまたは同様の権限を持つユーザーとして Openstack データベースにログインします。

   ```
   mysql -u root -p
   ```

2. nbosdmapi データベースとユーザーを削除します。

   ```
   DROP DATABASE nbosdmapi;
   ```

   ```
   DROP USER nbosdmapi;
   ```

NetBackup for OpenStack VM クラスタの破棄

NetBackup for OpenStack VM クラスタを破棄する方法

1. KVM ノードで実行されているすべての VM を一覧表示します

   ```
   virsh list
   ```

2. NetBackup for OpenStack VM を破棄します

   ```
   virsh destroy <NetBackup for OpenStack VM Name or ID>
   ```

3 NetBackup for OpenStack VM を未定義にします

```
virsh undefine <NetBackup for OpenStack VM name>
```

4 KVM ホストストレージから NetBackup for OpenStack VM ディスクを削除します。

nbosjm CLI クライアントのインストール

nbosjm CLI クライアントについて

nbosjm CLI クライアントは rpm および deb パッケージとして提供されます。

次のオペレーティングシステムでテストしています。

- CentOS7、CentOS8

nbosjm クライアントをインストールすると、必要なすべての OpenStack クライアントも自動的にインストールされます。

nbosjm クライアントをインストールすると、クライアントはグローバルな OpenStack Python クライアント (利用可能な場合) に統合されます。

必要な接続文字列とパッケージ名は、[ダウンロード (Downloads)]タブの NetBackup for OpenStack ダッシュボードにあります。

nbosjm クライアントのインストール

RPM ベースのオペレーティングシステム

nbosjm CLI クライアントは Python2 と Python3 で利用可能です

Python2 の場合は次を実行します。

```
yum install nbosjmclient-9.0.999-9.0.noarch.rpm
```

Python3 の場合は次を実行します。

```
yum install nbosjmclient-py3-el8-9.0.999-9.0.noarch.rpm
```

deb ベースのオペレーティングシステム

nbosjm CLI クライアントは Python2 と Python3 で利用可能です

Python2 の場合は次を実行します。

```
apt-get install nbosjmclient_9.0.999_all.deb
```

Python3 の場合は次を実行します。

```
apt-get install nbosjmclient-py3_9.0.999_all.deb
```

NetBackup for OpenStack のログローテーションについて

ログローテーションを使用すると、多数のログファイルを生成するシステムの管理が容易になります。ログファイルの自動ローテーション、圧縮、削除、メール送信が可能です。各ログファイルの処理は、毎日、毎週、毎月、または大きくなりすぎたときに実行できます。

logrotate は、スケジュールされた cron ジョブとして実行される Linux のユーティリティです。これは、設定ファイルから情報を読み込みます。これらの設定ファイルを更新することで、ログローテーションを構成できます。

RHOSP プラットフォームでは、ログローテーションの構成変更後に、変更を有効にするために設定全体を再配備する必要があります。

空の VxMS ログファイルは、8 日後に自動的にクリーンアップされます。

表 2-6 に、Kolla と Ansible のログローテーションを構成するために使用されるデフォルトオプションを示します。

表 **2-6** Kolla と Ansible のログローテーションのデフォルトオプション

コンポーネント	ログローテーションのデフォルトオプション

NBOSJM	設定ファイル: /etc/logrotate.d/nbosjm
	
	/var/log/nbosjm/*.log {
	missingok
	notifempty
	copytruncate
	size 25M
	rotate 30
	compress
	dateformat -%Y%m%d-%H
	}
	
	/var/NetBackupOpenStack-mounts/*/*/*.log {
	su root nova
	missingok
	compress
	delaycompress
	notifempty
	copytruncate
	size 25M
	rotate 30
	dateformat -%Y%m%d-%H
	}
	
	/var/NetBackupOpenStack-mounts/*/*.log {
	su root nova
	missingok
	compress
	delaycompress
	notifempty
	copytruncate
	size 25M
	rotate 30
	dateformat -%Y%m%d-%H
	}

コンポーネント	ログローテーションのデフォルトオプション

NBOSDMAPI	設定ファイル: /etc/logrotate.d/nbosdmapi
	
	/var/log/kolla/nbosdmapi/nbosdmapi.log {
	daily
	missingok
	notifempty
	copytruncate
	size=25M
	rotate 30
	maxage 30
	compress
	dateformat -%Y%m%d-%H
	}

VxMS と NBOSDM	設定ファイル: /etc/logrotate.d/nbosdm
	
	/var/log/kolla/nbosdm/nbosdm.log {
	daily
	missingok
	notifempty
	copytruncate
	size=25M
	rotate 30
	maxage 30
	compress
	dateformat -%Y%m%d-%H
	}
	
	/usr/openv/netbackup/logs/vxms/*.log {
	daily
	missingok
	notifempty
	copytruncate
	size=1M
	rotate 5
	postrotate
	find -daystart -mtime +30 -delete
	find -daystart -mtime +7 -size 0 -delete
	endscript
	compress
	dateformat -%Y%m%d-%H
	}

表 2-7 に、RHOSP のログローテーションを構成するために使用されるデフォルトオプションを示します。

表 2-7 RHOSP のログローテーションのデフォルトオプション

コンポーネント	ログローテーションのデフォルトオプション

NBOSJM	設定ファイル: /etc/logrotate.d/nbosjm
	
	/var/log/nbosjm/*.log {
	missingok
	notifempty
	copytruncate
	size 25M
	rotate 30
	compress
	dateformat -%Y%m%d-%H
	}
	
	/var/NetBackupOpenStack-mounts/*/*/*.log {
	su root nova
	missingok
	compress
	delaycompress
	notifempty
	copytruncate
	size 25M
	rotate 30
	dateformat -%Y%m%d-%H
	}
	
	/var/NetBackupOpenStack-mounts/*/*.log {
	su root nova
	missingok
	compress
	delaycompress
	notifempty
	copytruncate
	size 25M
	rotate 30
	dateformat -%Y%m%d-%H
	}

NBOSDM と NBOSDMAPI	ディレクタノードで次のファイルを参照してください。/home/stack/openstack-tripleo-heat-templates/deployment/logrotate/logrotate-crond-container-puppet.yaml

コンポーネント	ログローテーションのデフォルトオプション

VxMS	設定ファイル: /etc/logrotate.d/nbosdm
	
	/etc/logrotate.d/vxms
	
	/var/log/vxms/*.log {
	daily
	missingok
	notifempty
	copytruncate
	size=1M
	rotate 5
	postrotate
	find -daystart -mtime +30 -delete
	find -daystart -mtime +7 -size 0 -delete
	endscript
	compress
	dateformat -%Y%m%d-%H
	}

3

NetBackup OpenStack Appliance の構成

この章では以下の項目について説明しています。

NetBackup for OpenStack クラスタの再構成

NetBackup for OpenStack アプライアンスは、OpenStack 環境または一般的なバックアップソリューションの変更に合わせて、いつでも再構成して NetBackup for OpenStack クラスタを調整できます。

NetBackup for OpenStack クラスタを再構成するには、[構成 (Configure)]に移動します。構成ページには、nbosvm クラスタの現在の構成が表示されます。

この構成ページでは、最後に成功した構成の Ansible プレイブックにもアクセスできます。

NetBackup for OpenStack クラスタの再構成を開始するには、表の最後にある[再構成 (Reconfigure)]をクリックします。

その後、NetBackup for OpenStack の構成ガイドに従ってください。

NetBackup for OpenStack コンフィギュレータが開始されたら、NetBackup for OpenStack を使用し続けるために正常に実行する必要があります。

エラーが発生した場合、クラスタは最新の動作状態にロールバックしません。

NetBackup マスターサーバーの詳細の構成

NetBackup for OpenStack VM でマスターサーバーの詳細を構成する必要があります。NetBackup for OpenStack コンフィギュレータ UI のこの構成は、ライセンスチェック、容量レポート、および証明書の配備のための通信に必要です。

マスターサーバーの詳細を構成する方法

1. NetBackup for OpenStack コンフィギュレータ UI にログオンします。
2. マスターサーバーのホスト名を入力します。
3. 証明書の種類から 1 つを選択します。

NBCA	NetBackup CA が発行した証明書は、NetBackup CA が署名した証明書、または NetBackup 証明書と呼ばれます。 p.98 の「NetBackup のセキュリティ管理と証明書について」を参照してください。
外部 CA	NetBackup CA 以外の CA が発行した証明書は、外部 CA が署名した証明書、または外部証明書と呼ばれます。 p.98 の「NetBackup のセキュリティ管理と証明書について」を参照してください。

4. [SHA-256 指紋 (SHA-256 fingerprint)]に入力します。NetBackup Web UI に表示される NetBackup 認証局の詳細から、SHA-256 指紋を表示してコピーできます。

   『NetBackup Web UI 管理者ガイド』の「NetBackup 認証局の詳細と指紋の表示」を参照してください。

   コマンドラインを使用して SHA-256 指紋を参照することもできます。NetBackup プライマリサーバーで次のコマンドを実行します。

   ```
   /usr/openv/netbackup/bin/nbcertcmd -listCACertDetails
   ```

   『NetBackup コマンドリファレンスガイド』を参照してください。

5. 証明書タイプ NBCA を選択し、マスターサーバーのセキュリティ設定が[最高 (Very High)]として構成されている場合は、トークンを指定する必要があります。

   3 台の VM を使用して NetBackup for OpenStack クラスタを作成する場合は、2 つの引用符 ("") を使用して空白のセキュリティトークンを指定し、マスターサーバーのセキュリティを[高 (High)]に構成する必要があります。

6 証明書の種類で[外部 CA (External CA)]を選択する場合は、次の情報を入力する必要があります。

証明書ファイル (Certificate file)	証明書ファイルのパスを指定します。
トラストストアの場所 (Trust store location)	トラストストアの場所を指定します。
秘密鍵 (Private key)	秘密鍵を入力します。
パスフレーズファイル (Passphrase file)(オプション)	秘密鍵が暗号化されている場合は、パスフレーズファイルを指定します。
CRL を使用 (Use CRL)	証明書で定義されている CRL (証明書失効リスト) を使用する場合は、[証明書から (From certificate)]を選択します。 別のファイルで定義されている CRL を使用し、ファイルの場所を指定する場合は、[次のパスから: (From the following path:)]を選択します。 CRL を使用しない場合は、[CRL は使用しない (Do not use CRL)]を選択します。

7 [送信 (Submit)]をクリックします。

8 [Ansible 出力 (Ansible Output)]タブでは、NetBackup マスターサーバーの有効なホストとして自身を登録する、NetBackup OpenStack VM の新しい証明書などの詳細を確認できます。

NetBackup のセキュリティ管理と証明書について

NetBackup は、セキュリティ証明書を使って NetBackup ホストを認証します。これらの証明書は X.509 公開鍵基盤 (PKI) 標準に適合している必要があります。安全に通信するために、NetBackup 証明書または外部証明書を使用できます。

NetBackup 証明書はデフォルトでホストに対して発行され、NetBackup マスターサーバーは CA として動作し、CRL (証明書失効リスト) を管理します。NetBackup 証明書の配備のセキュリティレベルにより、証明書が NetBackup ホストに配備される方法と、各ホストで CRL が更新される頻度が決定されます。ホストに新しい証明書が必要な場合 (元の証明書の期限切れまたは無効化などの場合) は、NetBackup 認証トークンを使って証明書を再発行できます。

外部証明書とは、信頼できる外部 CA が署名した証明書です。外部証明書を使うように NetBackup を構成すると、NetBackup ドメイン内のマスターサーバー、メディアサーバー、クライアントは、外部証明書を安全な通信のために使用します。さらに、NetBackup Web サーバーもこれらの証明書を NetBackup Web UI と NetBackup ホスト間の通信に使用

します。外部証明書の配備、外部証明書の更新と置換、外部 CA の CRL の管理は、NetBackup 以外で管理されます。

外部証明書について詳しくは、『NetBackup セキュリティと暗号化ガイド』を参照してください。

NetBackup for OpenStack ダッシュボードのパスワードの変更

NetBackup for OpenStack GUI のパスワードを変更するには、次の手順を実行します。

- NetBackup for OpenStack ダッシュボードにログオンします。
- 右上隅の［管理 (Admin)］をクリックしてサブメニューを開きます。
- ［パスワードのリセット (Reset Password)］を選択します。
- 新しい NetBackup for OpenStack のパスワードを設定します。

NetBackup for OpenStack ダッシュボードのパスワードのリセット

- 次に移動します。`/home/stack/myansible/lib/python3.6/site-packages/nbos_configurator/`
- 次を実行します。`/home/stack/myansible/bin/python recreate_conf.py`
- nbos-config サービスを再起動します。`systemctl restart nbos-config`

NetBackup for OpenStack の再初期化

NetBackup for OpenStack Appliance を再初期化すると、すべてのポリシー関連の値が NetBackup for OpenStack データベースから削除されます。

NetBackup for OpenStack Appliance を再初期化するには、次の手順を実行します。

- NetBackup for OpenStack ダッシュボードにログオンします。
- 右上隅の［管理 (Admin)］をクリックしてサブメニューを開きます。
- ［再初期化 (Reinitialize)］を選択します。
- NetBackup for OpenStack を再初期化することを確認します。

NetBackup for OpenStack ログのダウンロード

NetBackup for OpenStack Web GUI を介して NetBackup for OpenStack ログを直接ダウンロードできます。

NetBackup for OpenStack Web GUI を介してログをダウンロードするには、次の操作を実行します。

- NetBackup for OpenStack Web GUI にログオンします。
- ［ログ (Logs)］に移動します。
- ダウンロードするログを選択します。
  - 各 NetBackup for OpenStack Appliance のログは個別にダウンロードできます。
  - または、すべてのログファイルが含まれる zip を作成してダウンロードできます。

これにより、現在のログファイルがダウンロードされます。すでにローテーションされているログは、NetBackup for OpenStack アプライアンスから SSH を介して直接ダウンロードする必要があります。ローテーションされた古いログを含むすべてのログは、次の場所にあります。

```
/var/logs/nbosjm/
```

4

NetBackup マスターサーバーの構成

この章では以下の項目について説明しています。

- NetBackup 用 OpenStack プラグインのライセンス
- NetBackup マスターサーバーでの NetBackup for OpenStack VM の許可
- NetBackup Web UI からの OpenStack Horizon UI の起動について

NetBackup 用 OpenStack プラグインのライセンス

次のテクニカルノートを確認し、適切なライセンスを適用します。

https://www.veritas.com/content/support/en_US/article.100040155.html

ライセンスの追加方法について詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

NetBackup マスターサーバーでの NetBackup for OpenStack VM の許可

NetBackup for OpenStack VM を使用するには、マスターサーバーを使用して構成する必要があります。NetBackup マスターサーバーで、NetBackup for OpenStack VM との通信を許可するための手順を実行します。

これは、ソフトウェアまたはアプリケーションが安全な実行を承認されていないかぎり、それらを実行しないようにシステムを制限するセキュリティ手法です。

NetBackup マスターサーバーで NetBackup for OpenStack VM を許可するには

◆ NetBackup マスターサーバー上で次のコマンドを実行します。

- UNIX の場合

```
bpsetconfig -h masterserver
bpsetconfig> APP_PROXY_SERVER = nbosvm1.domain.org
bpsetconfig> APP_PROXY_SERVER = nbosvm2.domain.org
bpsetconfig> APP_PROXY_SERVER = nbosvm3.domain.org
bpsetconfig>
UNIX systems: <ctl-D>
```

- Windows の場合

```
bpsetconfig -h masterserver
bpsetconfig> APP_PROXY_SERVER = nbosvm1.domain.org
bpsetconfig> APP_PROXY_SERVER = nbosvm2.domain.org
bpsetconfig> APP_PROXY_SERVER = nbosvm3.domain.org
bpsetconfig>
Windows systems: <ctl-Z>
```

メモ: NetBackup for OpenStack VM が 3 ノードクラスタの場合は、マスターサーバーに 3 つのノードすべてを追加する必要があります。

このコマンドは APP_PROXY_SERVER = clientname エントリをバックアップ構成 (bp.conf) ファイルに設定します。

APP_PROXY_SERVER = clientname について詳しくは、『NetBackup 管理者ガイド Vol. 1』の「NetBackup クライアントの構成オプション」のセクションを参照してください。

NetBackup Web UI からの OpenStack Horizon UI の起動について

Horizon UI にアクセスするには、アドレスバーに Horizon インスタンスの IP アドレスまたはホスト名を入力します。

また、NetBackup Web UI で Horizon インスタンスの詳細を構成して OpenStack Horizon UI を起動することもできます。

表 4-1 OpenStack Horizon UI の起動

手順	作業	説明
1	NetBackup Web UI で OpenStack Horizon インスタンスを追加します。	p.103 の「NetBackup Web UI での OpenStack Horizon インスタンスの追加」を参照してください。

手順	作業	説明
2	RBAC を構成します。 ■ OpenStack 管理者用のカスタム役割を作成します。 ■ 役割にユーザーを追加します。	p.103 の「NetBackup for OpenStack 管理者用のカスタム役割の作成」を参照してください。
3	役割でログオンし、Horizon UI を起動します。	p.104 の「NetBackup Web UI からの Horizon UI の起動」を参照してください。

NetBackup Web UI での OpenStack Horizon インスタンスの追加

NetBackup Web UI で OpenStack Horizon インスタンスを追加し、Web UI から Horizon UI を起動できます。

NetBackup Web UI で OpenStack Horizon インスタンスを追加する方法

1. Web UI で、[作業負荷 (Workload)]の下にある[OpenStack]をクリックします。
2. [追加 (Add)]をクリックします。
3. [Horizon インスタンスのリンクを追加 (Add Horizon instance link)]ボックスで、ホスト名/IP アドレスとポート番号を入力します。
4. [保存 (Save)]をクリックします。

NetBackup for OpenStack 管理者用のカスタム役割の作成

NetBackup Web ユーザーインターフェースは、NetBackup 環境に役割に基づくアクセス制御を適用する機能を提供します。RBAC を使用して、現在 NetBackup へのアクセス権を持たないユーザーにアクセス権を提供します。または、現在管理者アクセス権を持っている NetBackup ユーザーに対して、組織内の役割に基づいて制限されたアクセス権を提供できます。

RBAC の構成について詳しくは、『NetBackup™ Web UI 管理者ガイド』を参照してください。

NetBackup for OpenStack 管理者のカスタム役割を追加する方法

1. 左側で、[セキュリティ (Security)]、[RBAC]の順に選択します。
2. [ロール (Roles)]タブを選択し、[追加 (Add)]をクリックします。
3. [カスタム役割 (Custom role)]を選択し、[次へ (Next)]をクリックします。
4. [役割名 (Role name)]と説明を指定します。たとえば、特定の部署や地域のバックアップ管理者であるすべてのユーザー向けのロールであることを示す場合が考えられます。

5 ［ロールのアクセス権 (Role permissions)］で、そのロールを持つユーザーに、各アクセス権の種類に対して付与するアクセス権またはアクセスの種類を選択します。

6 ［役割の追加 (Add role)］をクリックします。

NetBackup Web UI からの Horizon UI の起動

カスタム役割を作成してユーザーを役割に追加すると、カスタム役割を持つユーザーは Horizon UI にログオンできます。

NetBackup Web UI から Horizon UI を起動する方法

1 NetBackup Web UI にログオンします。

2 Web UI で、［作業負荷 (Workload)］の下にある［OpenStack］をクリックします。

3 URL をクリックします。

4 Horizon UI にログオンします。

5

NetBackup for OpenStack のポリシー

この章では以下の項目について説明しています。

ポリシーについて

ポリシーは、構成に従って 1 つ以上の仮想マシンを保護するバックアップジョブです。必要な数のポリシーを作成できます。ただし、各 VM は 1 つのポリシーにのみ属することができます。

ポリシーのリスト

Horizon の使用

Horizon でプロジェクトのすべての利用可能なポリシーを表示する方法

- Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。

Horizon の概要には、すべてのポリシーが次の追加情報と一緒に一覧表示されます。

- 作成時刻
- ポリシー名
- ポリシーの説明
- このポリシー内のスナップショットの合計
  - 成功したスナップショットの合計数
  - 失敗したスナップショットの合計数
- ポリシー形式
- ポリシーの状態

CLI の使用

```
nbosjm policy-list [--all {True,False}] [--nfsshare <nfsshare>]
```

- `--all {True,False}` すべてのプロジェクトのすべてのポリシーを一覧表示します (管理者ユーザーのみに有効)。
- `--nfsshare <nfsshare>` NFS 共有のすべてのポリシーを一覧表示します (管理者ユーザーのみに有効)。

ポリシーの作成

Horizon の使用

Horizon 内にポリシーを作成するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. [ポリシーの作成 (Create Policy)]をクリックします。
3. [詳細 (Details)]タブで、ポリシー名、説明、およびポリシー形式 (シリアルまたはパラレル) を指定します。

4 [ポリシーメンバー (Policy Members)]タブで、保護する VM を選択します。

5 [スケジュール (Schedule)]タブで、[スケジューラを有効にする (Enable Scheduler)]をクリックしてバックアップをスケジュールします。

スケジュールで、開始日、終了日、開始時刻、バックアップを繰り返す必要がある時間数を指定します。

6 [ポリシー属性 (Policy Attributes)]タブで保持ポリシーを指定します。

7 [ポリシー属性 (Policy Attributes)]タブで完全バックアップの間隔を選択します。

8 必要に応じて、[オプション (Options)]タブで[VM を一時停止 (Pause VM)]を選択します。

9 [作成 (Create)]をクリックします。

作成されたポリシーは数秒後に利用可能になり、指定されたスケジュールとポリシーに従ってバックアップの作成を開始します。

CLI の使用

```
nbosjm policy-create --instance <instance-id=instance-uuid>
                            [--display-name <display-name>]
                            [--display-description
<display-description>]
                            [--policy-type-id <policy-type-id>]
                            [--source-platform <source-platform>]
                            [--jobschedule <key=key-name>]
                            [--metadata <key=key-name>]
                            [--policy-attribute-id
<policy_attribute_id>]
```

- `--display-name` オプションのポリシー名。(デフォルト = なし)
- `--display-description` オプションのポリシーの説明。(デフォルト = なし)
- `--policy-type-id` ポリシー形式 ID が必要です
- `--source-platform` ポリシーソースプラットフォームが必要です。サポート対象のプラットフォームは「openstack」
- `--instance` ポリシーに含めるインスタンスを指定します。複数のインスタンスを含める場合は、オプションを複数回指定します。Instance-id: この UUID を持つインスタンスを含めます。
- `--jobschedule` ジョブスケジュールに次のキーと値のペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。"start_date" : "06/05/2014" "end_date" : "07/15/2014" "start_time" : "2:30 PM" "interval" : "1 hr" "snapshots_to_retain" : "2"

- `--metadata` ポリシー形式のメタデータに含めるキーと値のペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。key=value
- `--policy-attribute-id` ポリシーに割り当てるポリシー属性の ID。

ポリシーの概要

ポリシーに関する情報をポリシーの概要に表示します。

Horizon の使用

Horizon 内にポリシーの概要を入力するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 表示するポリシーを特定します。
3. ポリシー名をクリックすると、ポリシーの概要が表示されます。

詳細 (Details)	[ポリシーの詳細 (Policy Details)]タブには、ポリシーに関する最も重要な情報が表示されます。 ■ 名前 (Name) ■ 説明 (Description) ■ 可用性ゾーン (Availability Zone) ■ qemu ゲストエージェントの可用性の情報を含む保護対象 VM のリスト qemu-guest-agent の状態は、qemu ゲストエージェントの統合を提供するためにこの VM に必要な OpenStack 構成が行われているかどうかを示します。qemu ゲストエージェントが VM にインストールされ構成されているかどうかは確認されません。 保護対象の VM のリストから、保護対象の VM に直接移動できます。
スナップショット (Snapshots)	[スナップショット (Snapshots)]タブには、選択したポリシーで利用可能なすべてのスナップショットのリストが表示されます。 ここから、スナップショットを操作し、オンデマンドでスナップショットを作成し、リストアを開始できます。 p.114 の「スナップショットについて」を参照してください。

ポリシー属性 (Policy Attributes)	[ポリシー属性 (Policy Attributes)]タブには、現在構成されているスケジューラと保持ポリシーの概要が表示されます。次の要素が表示されます。 ■ スケジューラの状態 (有効または無効) ■ 開始日時 ■ 終了日時 ■ RPO ■ 次回のスナップショット実行までの時間 ■ 保持ポリシーと値 ■ 完全バックアップ間隔のポリシーと値
ファイル検索	[ファイル検索 (File Search)]タブは、リストアを必要とせずにスナップショット上のファイルとフォルダを検索できる強力な検索エンジンへのアクセスを提供します。 p.138 の「ファイル検索について」を参照してください。
その他	[その他 (Miscellaneous)]タブには、ポリシーの残りのメタデータが表示されます。次の情報が表示されます。 ■ 作成時刻 ■ 最終更新時刻 ■ ポリシー ID ■ ポリシー形式 ID ■ ポリシー属性 ID ■ プロジェクト ID ■ ユーザー ID

CLI の使用

```
nbosjm policy-show <policy-id> [--verbose <verbose>]
```

- `<policy-id>` 表示するポリシーの ID/名前。
- `--verbose` ポリシーについての追加情報を表示するオプション。

ポリシーの編集

変更するニーズに合わせて、すべてのコンポーネントでポリシーを変更できます。

メモ: ポリシーを編集すると、ユーザーが新しい所有者として設定されます。

Horizon の使用

Horizon でポリシーを編集するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 変更するポリシーを識別します。
3. [スナップショットの作成 (Create Snapshot)]ドロップダウンをクリックします。
4. [ポリシーの編集 (Edit Policy)]をクリックします。
5. 必要に応じてポリシーを修正します。ポリシー形式を除くすべてのパラメータを変更できます。
6. [更新 (Update)]をクリックします。

CLI の使用

```
usage: nbosjm
policy-modify [--display-name <display-name>]
                [--display-description <display-description>]
                [--instance <instance-id=instance-uuid>]
                [--jobschedule <key=key-name>]
                [--metadata <key=key-name>]
                [--policy_attribute_id <policy_attribute_id>]
                <policy-id>
```

- `--display-name` オプションのポリシー名。(デフォルト = なし)
- `--display-description` オプションのポリシーの説明。(デフォルト = なし)
- `--instance <instance-id=instance-uuid>` ポリシーに含めるインスタンスを指定します。複数のインスタンスを含める場合は、オプションを複数回指定します。Instance-id: この UUID を持つインスタンスを含めます
- `--jobschedule <key=key-name>` ジョブスケジュールに次のキー値ペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。タイムゾーンを指定しない場合、デフォルトでは、ローカルコンピュータのタイムゾーンが使用されます。"start_date" : "06/05/2014" "end_date" : "07/15/2014" "start_time" : "2:30 PM" "interval" : "1 hr" "retention_policy_type" : 「保持するスナップショットの数」または「スナップショットを保持する日数」"retention_policy_value" : "30"
- `--metadata <key=key-name>` ポリシー形式のメタデータに含めるキー値のペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。
- `--policy-attribute-id <policy_attribute_id>` 割り当てるポリシー属性の ID。

- <policy-id> 編集するポリシーの ID。

ポリシーの削除

不要になったポリシーは安全に削除できます。ポリシーを削除する前に、すべてのスナップショットを削除する必要があります。

p.114 の「スナップショットについて」を参照してください。

Horizon の使用

ポリシーを削除するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 削除するポリシーを識別します。
3. [スナップショットの作成 (Create Snapshot)]ドロップダウンをクリックします。
4. [ポリシーの削除 (Delete Policy)]をクリックします。
5. もう一度[ポリシーの削除 (Delete Policy)]をクリックして確定します。

CLI の使用

```
nbosjm policy-delete [--database_only <True/False>] <policy-id>
```

- <policy-id> 削除するポリシーの ID/名前。
- --database_only <True/False> データベースからのみ削除する場合は True のままにします。(デフォルトは False)

ポリシーのロック解除

バックアップまたはリストアをアクティブに実行しているポリシーは、以降のタスクでロックされます。必要に応じて強制的にポリシーのロックを解除できます。

バックアップまたはリストアが失敗することなく停止したり、バックアップの実行中にリストアが必要な場合は、この機能を最後の手段としてのみ使用することをお勧めします。

Horizon の使用

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. ロック解除するポリシーを識別します。
3. [スナップショットの作成 (Create Snapshot)]ドロップダウンをクリックします。

4. ［ポリシーのロック解除 (Unlock Policy)］をクリックします。
5. もう一度［ポリシーの解除 (Unlock Policy)］をクリックして確定します。

CLI の使用

```
nbosjm policy-unlock <policy-id>
```

- <policy-id> ロック解除するポリシーの ID。

ポリシーのリセット

まれに、作成したバックアップの品質を確保するためにバックアップチェーンのやり直しが必要になる場合があります。ポリシーの再作成を回避する場合は、ポリシーをリセットできます。

ポリシーをリセットすると、次の処理が実行されます。

- 進行中のすべてのタスクがキャンセルされます。
- 保護対象の VM からすべての既存の NetBackup for OpenStack スナップショットが削除されます。
- 次のスナップショット時刻が再計算されます。
- 次回のスナップショットで完全バックアップが作成されます。

Horizon の使用

ポリシーをリセットするには、次の手順を実行します。

1. Horizon コンソールで、［NBOS バックアップ (NBOS Backups)］、［ポリシー (Policies)］の順に移動します。
2. リセットするポリシーを識別します。
3. ［スナップショットの作成 (Create Snapshot)］ドロップダウンをクリックします。
4. ［ポリシーのリセット (Reset Policy)］をクリックします。
5. もう一度［ポリシーのリセット (Reset Policy)］をクリックして確定します。

CLI の使用

```
nbosjm policy-reset <policy-id>
```

- <policy-id> リセットするポリシーの ID/名前。

6

OpenStack のバックアップとリストアの実行

この章では以下の項目について説明しています。

スナップショットについて

スナップショットは、すべてのデータとメタデータを含むポリシーの単一の NetBackup for OpenStack バックアップです。ポリシーが保護するすべての VM の情報が含まれます。

スナップショットのリスト

Horizon の使用

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 詳細を表示するポリシーを特定します。

3. ポリシーの概要を入力するポリシー名をクリックします。
4. ［スナップショット (Snapshots)］タブに移動します。

選択したポリシーのスナップショットのリストには、次の追加情報が含まれています。

- 作成時刻
- スナップショットの名前
- スナップショットの説明
- このスナップショットからのリストアの総数
  - 成功したリストアの総数
  - 失敗したリストアの総数
- スナップショット形式
- スナップショットのサイズ
- スナップショットの状態

CLI の使用

```
nbosjm snapshot-list [--policy-id <policy-id>]
                          [--nbos_node <host>]
                          [--date_from <date_from>]
                          [--date_to <date_to>]
                          [--all {True,False}]
```

- `--policy-id <policy-id>` policy-id (ポリシー ID) によって結果をフィルタ処理します。
- `--nbos_node <host>` nbos ノードでスケジュールされているすべてのスナップショット操作を一覧表示します (デフォルト = なし)。
- `--date_from <date_from>`「YYYY-MM-DDTHH:MM:SS」の形式の開始日付 (2016-10-10T00:00:00 などの形式で)。時間を指定しない場合は、デフォルトで 00:00 になります。
- `--date_to <date_to>`「YYYY-MM-DDTHH:MM:SS」の形式の終了日付 (デフォルトは現在の日付)。date_from と date_to の同じ日付の結果を含めてまたは除外してスナップショットを取得するには、HH:MM:SS を指定します。
- `--all {True,False}` すべてのプロジェクトのすべてのスナップショットを一覧表示します (管理者ユーザーのみに有効)。

スナップショットの作成

スナップショットは、NetBackup for OpenStack スケジューラによって自動的に作成されます。必要な場合、またはスケジューラを無効にした場合は、オンデマンドでスナップショットを作成できます。

メモ: NetBackup for OpenStack では、スワップディスクとエフェメラルディスクのバックアップはサポートされていません。

Horizon の使用

オンデマンドでスナップショットを作成するには、2 つの可能性があります。

可能性 1: ポリシーの概要から

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. スナップショットを作成するポリシーを特定します。
3. [スナップショットの作成 (Create Snapshot)]をクリックします。
4. スナップショットの名前と説明を入力します。
5. 完全スナップショットと増分スナップショットのどちらにするかを決定します。
6. [作成 (Create)]をクリックします。

可能性 2: ポリシーのスナップショットリストから

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. スナップショットを作成するポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. [スナップショットの作成 (Create Snapshot)]をクリックします。
6. スナップショットの名前と説明を入力します。
7. 完全スナップショットと増分スナップショットのどちらにするかを決定します。
8. [作成 (Create)]をクリックします。

CLI の使用

```
nbosjm policy-snapshot [--full] [--display-name <display-name>]
                                [--display-description
```

```
<display-description>]
                                    <policy-id>
```

- <policy-id> スナップショットを作成するポリシーの ID。
- --full 完全スナップショットが必要かどうかを指定します。
- --display-name <display-name> オプションのスナップショット名。(デフォルト = なし)
- --display-description <display-description> オプションのスナップショットの説明。(デフォルト = なし)

スナップショットの概要

各スナップショットには、バックアップについての多くの情報が含まれています。この情報は、スナップショットの概要で確認できます。

Horizon の使用

スナップショットの概要を表示するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 表示するスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します
6. スナップショット名をクリックします。

詳細

[スナップショットの詳細 (Snapshot Details)]タブには、スナップショットに関する最も重要な情報が表示されます。

- スナップショット ID、名前、説明
- スナップショット形式
- 所要時間
- サイズ
- 状態
- スナップショットに含まれる VM
- スナップショットの各 VM に対して
  - インスタンス情報 - 名前と状態
  - セキュリティグループ - 名前、種類
  - フレーバー - vCPU、ディスク、RAM
  - ネットワーク - IP、ネットワーク名、Mac アドレス
  - 接続されたボリューム - 名前、種類、サイズ (GB)、マウントポイント、リストアサイズ
  - その他 - VM の元の ID

リストア

[スナップショットのリストア (Snapshot Restores)]タブには、選択したスナップショットから開始されたリストアのリストが表示されます。ここからリストアを開始できます。

p.121 の「リストアについて」を参照してください。

その他

[スナップショットのその他 (Snapshot Miscellaneous)]タブには、スナップショットに関する残りのメタデータ情報が表示されます。

- 作成時刻
- 最終更新時刻
- スナップショット ID
- スナップショットを含んでいるポリシーのポリシー ID

CLI の使用

```
nbosjm snapshot-show [--output <output>] <snapshot_id>
```

- `<snapshot_id>` 表示されるスナップショットの ID。
- `--output <output>` スナップショットの追加の詳細を取得するオプション。スナップショットメタデータには –output metadata を指定し、スナップショット VM ネットワークには –output networks を指定し、スナップショット VM ディスクには –output disks を指定します。

メモ: OpenStack では、ネットワークインターフェースなしでインスタンスを起動できません。ネットワークインターフェースが接続されていないインスタンスのスナップショットは、選択的リストアまたはワンクリックリストアオプションを使用してリストアすることはできません。ただし、インプレースリストアは使用できます。この場合、インスタンスは起動されません。

スナップショットの削除

不要になったスナップショットは、ポリシーから安全に削除できます。

保持ポリシーは、構成されたポリシーに従って最も古いスナップショットを自動的に削除します。

ポリシーを削除できるようにするには、すべてのスナップショットを削除する必要があります。

NetBackup for OpenStack スナップショットを削除しても、OpenStack Cinder スナップショットは削除されません。必要に応じて個別に削除する必要があります。

Horizon の使用

スナップショットを削除するには、2 つの可能性があります。

可能性 1: サブメニューを使用した単一のスナップショットの削除

サブメニューを介して単一のスナップショットを削除するには、次の手順に従います。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 削除するスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します
6. [処理 (Actions)]列のドロップダウンをクリックします。
7. [スナップショットの削除 (Delete Snapshot)]をクリックします。
8. [削除 (Delete)]をクリックして確定します。

可能性 2: スナップショットの概要のチェックボックスを使用した複数のスナップショットの削除

スナップショットの概要から 1 つ以上のスナップショットを削除するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 表示するスナップショットを含むポリシーを特定します。

3. ポリシーの概要を入力するポリシー名をクリックします
4. ［スナップショット (Snapshots)］タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します。
6. 削除する各スナップショットのチェックボックスにチェックマークを付けます。
7. ［スナップショットの削除 (Delete Snapshots)］をクリックします。
8. ［削除 (Delete)］をクリックして確定します。

CLI の使用

```
nbosjm snapshot-delete <snapshot_id>
```

- <snapshot_id> 削除するスナップショットの ID。

ボリュームスナップショットのクリーンアップ

スナップショット ID またはポリシー ID を使用して、失敗またはエラーの状態にあるボリュームスナップショットをクリーンアップできます。

CLI の使用

```
nbosjm volume-snapshot-cleanup --snapshot_id <snapshot_id>
nbosjm volume-snapshot-cleanup --policy <policy_id>
```

- <snapshot_id> クリーンアップするポリシースナップショットの ID。
- <policy_id> 失敗またはエラー状態のボリュームスナップショットがあり、クリーンアップする必要があるポリシーの ID。

メモ: snapshot_id オプションと policy_id オプションの両方を使用する場合、スナップショット ID がポリシーに関連付けられている必要があります。

スナップショットのキャンセル

進行中のスナップショットはキャンセルできます。

キャンセルしたスナップショットは、エラーが発生したスナップショットと同様に処理されます。

Horizon の使用

1. Horizon コンソールで、［NBOS バックアップ (NBOS Backups)］、［ポリシー (Policies)］の順に移動します。

2. キャンセルするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします
4. ［スナップショット (Snapshots)］タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します
6. 特定されたスナップショットと同じ行の［キャンセル (Cancel)］をクリックします。
7. ［キャンセル (Cancel)］をクリックして確定します。

CLI の使用

```
nbosjm snapshot-cancel <snapshot_id>
```

- `<snapshot_id>` キャンセルするスナップショットの ID。

リストアについて

リストアは、バックアップされた VM を NetBackup for OpenStack スナップショットから戻すワークフローです。

マルチ接続ボリュームのリストアについて

NetBackup for OpenStack は、バックアップとリストアのためにマルチ接続ボリュームをサポートします。この機能を使うと、1 つのボリュームを複数の VM と共有できます。マルチ接続ボリュームについて詳しくは、OpenStack のマニュアルを参照してください。

マルチ接続ボリュームが含まれる VM のバックアップ中、各 VM は個別にバックアップされます。そのため、マルチ接続ボリュームを持つ VM に対するリストア操作を実行すると、リストアされたボリュームはマルチ接続のプロパティセットを持ちますが、デフォルトでは共有されません。

たとえば、同じポリシーによって保護されている 4 台の VM に接続されたマルチ接続ボリュームがあるとします。このポリシーで 4 台の VM のバックアップを作成します。スナップショットをリストアすると、マルチ接続のプロパティが設定された 4 つの別々のボリュームを持つ 4 台の VM がリストアされます。

リストアのリスト

Horizon の使用

スナップショットのリストアリストにアクセスするには、次の手順を実行します。

1. Horizon コンソールで、［NBOS バックアップ (NBOS Backups)］、［ポリシー (Policies)］の順に移動します。

2. 表示するスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. ［スナップショット (Snapshots)］タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します。
6. スナップショット名をクリックします。
7. ［リストア (Restores)］タブに移動します。

CLI の使用

```
nbosjm restore-list [--snapshot_id <snapshot_id>]
```

- `--snapshot_id <snapshot_id>` リストアを表示するスナップショットの ID

リストアの概要

Horizon の使用

詳細なリストアの概要を表示するには、次の手順を実行します。

1. Horizon コンソールで、［NBOS バックアップ (NBOS Backups)］、［ポリシー (Policies)］の順に移動します。
2. 表示するスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします
4. ［スナップショット (Snapshots)］タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します。
6. スナップショット名をクリックします。
7. ［リストア (Restores)］タブに移動します。
8. 表示するリストアを特定します。
9. リストア名をクリックします。

詳細

[リストアの詳細 (Restore Details)]タブには、リストアに関する最も重要な情報が表示されます。

- 名前
- 説明
- リストア形式
- 状態
- 所要時間
- サイズ
- 進捗を示すメッセージ
- 進捗状況
- ホスト
- リストアオプション

リストアオプションは、NetBackup for OpenStack に提供される restore.json です。

- リストアされる VM のリスト
  - リストアされる VM 名
  - リストアされる VM の状態
  - リストアされる VM ID

その他

[その他 (Misc)]タブには、追加のメタデータ情報が表示されます。

- 作成時刻
- リストア ID
- リストアを含むスナップショットの ID
- ポリシー

CLI の使用

```
nbosjm restore-show [--output <output>] <restore_id>
```

- `<restore_id>` 表示されるリストアの ID
- `--output <output>` 追加のリストア詳細を取得するオプション、リストアメタデータには –output metadata を指定します、–output networks –output subnets –output routers –output flavors

リストアの削除

不要になったリストアは、ポリシーから安全に削除できます。

リストアを削除すると、このリストアに関する NetBackup for OpenStack の情報のみが削除されます。OpenStack リソースは削除されません。

Horizon の使用

リストアを削除するには、2 つの可能性があります。

可能性 1: サブメニューを使用した単一のリストアの削除

サブメニューを介して単一のリストアを削除するには、次の手順に従います。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 削除するスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します。
6. スナップショット名をクリックします。
7. [リストア (Restore)]タブに移動します。
8. 対象のリストアの行で[リストアの削除 (Delete Restore)]をクリックします。
9. 再び[リストアの削除 (Delete Restore)]をクリックして確定します。

可能性 2: スナップショットの概要のチェックボックスを使用した複数のリストアの削除

リストアリストから 1 つ以上のリストアを削除するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 表示するスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します。
6. スナップショット名をクリックして、スナップショットを入力します。
7. [リストア (Restore)]タブに移動します。
8. 削除する各リストアのチェックボックスにチェックマークを付けます。
9. [リストアの削除 (Delete Restore)]をクリックします。
10. 再び[リストアの削除 (Delete Restore)]をクリックして確定します。

CLI の使用

```
nbosjm restore-delete <restores_id>
```

- `<restore_id>` 削除するリストアの ID

リストアのキャンセル

進行中のリストアはキャンセルできます。

Horizon の使用

Horizon でリストアをキャンセルするには、次の手順に従います。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 削除するスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します。
6. スナップショット名をクリックします。
7. [リストア (Restore)]タブに移動します。
8. 進行中のリストアを特定します。
9. 対象のリストアの行で[リストアのキャンセル (Cancel Restore)]をクリックします。
10. 再び[リストアのキャンセル (Cancel Restore)]をクリックして確定します。

CLI の使用

```
nbosjm restore-cancel <restore_id>
```

- `<restore_id>` 削除するリストアの ID

ワンクリックリストア

ワンクリックリストアは、バックアップされたときと同じ状態のスナップショットからすべての VM を戻します。これらは次のようになります。

- 同じデータセンター内の同じクラスタに配置されます
- 同じストレージドメインを使用します
- 同じネットワークに接続されます
- 同じフレーバーを持ちます

ユーザーはメタデータを変更できません。

ワンクリックリストアでは、バックアップされた元の VM が削除されている必要があります。そうでないと、失われます。1 つの VM がまだ実行されていても、ワンクリックリストアは失敗します。

ワンクリックリストアは、リストアされた VM を保護するためにポリシーを自動的に更新します。

Horizon の使用

ワンクリックリストアを開始するには、2 つの可能性があります。

可能性 1: スナップショットリストから

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. リストアするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. リストアするスナップショットを特定します。
6. 特定されたスナップショットと同じ行の[ワンクリックリストア (One-Click Restore)]をクリックします。
7. (オプション) 名前と説明を入力します。
8. [作成 (Create)]をクリックします。

可能性 2: スナップショットの概要から

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. リストアするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. リストアするスナップショットを特定します。
6. スナップショット名をクリックします。
7. [リストア (Restores)]タブに移動します。
8. [ワンクリックリストア (One-Click Restore)]をクリックします。
9. (省略可能) 名前と説明を入力します。
10. [作成 (Create)]をクリックします。

CLI の使用

```
nbosjm snapshot-oneclick-restore [--display-name <display-name>]
                        [--display-description <display-description>]

                          <snapshot_id>
```

- `<snapshot_id>` リストアするスナップショットの ID。
- `--display-name <display-name>` リストアの省略可能な名前。
- `--display-description <display-description>` リストアの省略可能な説明。

選択的リストア

選択的リストアは、NetBackup for OpenStack が提供する最も複雑なリストアです。これにより、リストアされた VM をユーザーのニーズに正確に適応できます。

選択的リストアを使用すると、次の処理を変更できます。

- リストア対象の VM
- リストアされた VM の名前
- 接続するネットワーク
- 使用するストレージドメイン
- リストア先のデータセンターまたはクラスタ
- リストアされた VM が使用するフレーバー

選択的リストアは常に利用可能で、事前の要件はありません。

Horizon の使用

選択的リストアを開始するには、2 つの可能性があります。

可能性 1: スナップショットリストから

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. リストアするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. リストアするスナップショットを特定します。

6. ［処理 (Actions)］列のドロップダウンメニューから、［選択的リストア (Selective Restore)］を選択します。
7. 必要に応じて選択的リストアを構成します。
8. ［リストア (Restore)］をクリックします。

可能性 2: スナップショットの概要から

1. Horizon コンソールで、［NBOS バックアップ (NBOS Backups)］、［ポリシー (Policies)］の順に移動します。
2. リストアするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. ［スナップショット (Snapshots)］タブに移動します。
5. リストアするスナップショットを特定します。
6. スナップショット名をクリックします。
7. ［リストア (Restores)］タブに移動します。
8. ［選択的リストア (Selective Restore)］をクリックします。
9. 必要に応じて選択的リストアを構成します。
10. ［リストア (Restore)］をクリックします。

CLI の使用

```
nbosjm snapshot-selective-restore [--display-name <display-name>]
                        [--display-description <display-description>]

                          [--filename <filename>]
                          <snapshot_id>
```

- `<snapshot_id>` リストアするスナップショットの ID。
- `--display-name <display-name>` リストアの省略可能な名前。
- `--display-description <display-description>` リストアの省略可能な説明。
- `--filename <filename>` ファイル名を含むファイルパス (相対パスまたは絶対パス) を指定します。デフォルトでは、ファイル /usr/lib/python2.7/site-packages/nbosjmclient/input-files/restore.json が読み込まれます。これを使用して、値を参照したり、このファイルの値を置き換えたりできます。

インプレースリストア

インプレースリストアは、VM とそのボリュームがまだ利用可能であるが、データが破損したり、他の理由でロールバックする必要があるようなユースケースを対象としています。

これにより、バックアップの一部である、選択したボリュームのデータのみをリストアできます。

インプレースリストアは、元の VM と元のボリュームがまだ利用可能で接続されている場合にのみ機能します。NetBackup for OpenStack は保存されたオブジェクト ID でこれを確認しています。

インプレースリストアでは、新しい RHV リソースは作成されません。新しいボリュームまたは VM が必要な場合は、他のいずれかのリストアオプションを使用してください。

インプレースリストアではインスタンスが再起動されます。

Horizon の使用

インプレースリストアを開始するには、2 つの可能性があります。

可能性 1: スナップショットリストから

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. リストアするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. リストアするスナップショットを特定します。
6. [処理 (Actions)]列のドロップダウンから、[インプレースリストア (Inplace Restore)]を選択します。
7. 必要に応じてインプレースリストアを構成します。
8. [リストア (Restore)]をクリックします。

可能性 2: スナップショットの概要から

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. リストアするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. リストアするスナップショットを特定します。
6. スナップショット名をクリックします。

7. ［リストア (Restores)］タブに移動します。
8. ［インプレースリストア (Inplace Restore)］をクリックします。
9. 必要に応じてインプレースリストアを構成します。
10. ［リストア (Restore)］をクリックします。

CLI の使用

```
nbosjm snapshot-inplace-restore [--display-name <display-name>]
                        [--display-description <display-description>]

                         [--filename <filename>]
                         <snapshot_id>
```

- `<snapshot_id>` リストアするスナップショットの ID。
- `--display-name <display-name>` リストアの省略可能な名前。
- `--display-description <display-description>` リストアの省略可能な説明。
- `--filename <filename>` ファイル名を含むファイルパス (相対パスまたは絶対パス) を指定します。デフォルトでは、ファイル /usr/lib/python2.7/site-packages/nbosjmclient/input-files/restore.json が読み込まれます。これは、値を参照したり、このファイルの値を置き換えるために使用できます。

CLI に必要な restore.json

nbosjm クライアントの CLI は、restore.json ファイルを使用して、選択的リストアとインプレースリストアのリストアパラメータを定義します。

この restore.json の選択的リストアの例を次に示します。詳細な分析と説明は後述します。

restore.json には、バックアップされたリソースに関する情報が必要です。必要なすべての情報をスナップショットの概要に収集できます。

```
{
    name: getjson,
    description: -,
    oneclickrestore: False,
    restore_type: selective,
    type: openstack,
    openstack:
```

```
        {
            instances:
                [
                    {
                        include: True,
                        id: 890888bc-a001-4b62-a25b-484b34ac6e7e,

                        name: cdcentOS-1,
                        availability_zone:,
                        nics: [],
                        vdisks:
                            [
                                {
                                  id:
4cc2b474-1f1b-4054-a922-497ef5564624,
                                  new_volume_type:,
                                  availability_zone: nova
                                }
                            ],
                        flavor:
                            {
                                ram: 512,
                                ephemeral: 0,
                                vcpus: 1,
                                swap:,
                                disk: 1,
                                id: 1
                            }
                    }
                ],
            restore_topology: True,
            networks_mapping:
                {
                    networks: []
                }
        }
}
```

必要な一般的な情報

リストアの正確な詳細を指定する前に、リストアの一般的なメタデータを提供する必要があります。

- name リストアの名前。

- description リストアの説明。
- oneclickrestore <True/False> リストアがワンクリックリストアかどうか。この設定を True に設定すると、他のすべての設定が上書きされ、ワンクリックリストアが開始されます。
- restore_type <oneclick/selective/inplace> 目的のリストアを定義します。
- type openstack OpenStack クラウドへのリストアを定義します。
- openstack リストアの正確な定義を開始します。

選択的リストアに必要な情報

選択的リストアでは、必要なリストアを実行するために多くの情報が必要です。

この情報は、次の 3 つのコンポーネントに分かれています。

- インスタンス
- restore_topology
- networks_mapping

インスタンスに必要な情報

この部分には、リストアするスナップショットに含まれるすべてのインスタンスとそのリストア方法に関するすべての情報が含まれます。

VM をリストアしない場合でも、リストアを問題なく実行するには restore.json 内に VM が必要です。

各インスタンスには、次の情報が必要です

- id インスタンスの元の ID
- include <True/False> インスタンスをリストアする場合は True を設定します

これ以降のすべての情報は、インスタンスがリストアに含まれる場合にのみ必要です。

- name インスタンスの新しい名前
- availability_zone インスタンスのリストア先となる Nova 可用性ゾーン。「任意の可用性ゾーン」の場合は空のままにします
- Nics インスタンスに接続する OpenStack Neutron ポートのリスト。各 Neutron ポートは次のもので構成されています。
  - id 使用する Neutron ポートの ID
  - mac_address Neutron ポートの Mac アドレス
  - ip_address Neutron ポートの IP アドレス

- network ポートが割り当てられているネットワーク。次の情報が含まれます。
  - id Neutron ポートが含まれるネットワークの ID
  - subnet ポートが割り当てられているサブネット。次の情報が含まれます。
    - id Neutron ポートが含まれるネットワークの ID

次に利用可能な空き IP を使用するには、Nics を空のリスト [ ] に設定します

Nic の空のリストをネットワークトポロジーリストアと組み合わせて使用して、リストアジョブはインスタンスの元の IP アドレスを設定します。

- vdisks インスタンスに含まれるすべてのボリュームのリスト。各ボリュームには、次の情報が必要です。
  - id ボリュームの元の ID。
  - new_volume_type リストアされたボリュームに使用するボリューム形式。「ボリューム形式なし」の場合は空のままにします。
  - availability_zone ボリュームに使用する Cinder 可用性ゾーン。Cinder のデフォルトの可用性ゾーンは Nova です。
- flavor リストアされたインスタンスに使用するフレーバーを定義します。次の情報が含まれます。
  - ram リストアされたインスタンスの RAM 容量 (MB)。
  - ephemeralインスタンスのエフェメラルディスクの大きさ (GB)。
  - vcpus リストアされたインスタンスが利用可能な vcpu の数。
  - swap リストアされたインスタンスのスワップの大きさ (MB)。なしの場合は空のままにします。
  - disk インスタンスがブートする root ディスクのサイズ。
  - id 指定された情報と一致するフレーバーの ID。

警告: root ディスクは、少なくともバックアップされたインスタンスのルートディスクと同じ大きさである必要があります。

次の例では、すべての値を持つ単一インスタンスについて説明します。

```
'instances':[
  {
     'name':'cdcentOS-1-selective',
     'availability_zone':'US-East',
     'nics':[
```

```
        {
           'mac_address':'fa:16:3e:00:bd:60',
           'ip_address':'192.168.0.100',
           'id':'8b871820-f92e-41f6-80b4-00555a649b4c',
           'network':{
              'subnet':{
                 'id':'2b1506f4-2a7a-4602-a8b9-b7e8a49f95b8'
              },
              'id':'d5047e84-077e-4b38-bc43-e3360b0ad174'
           }
        }
     ],
     'vdisks':[
        {
           'id':'4cc2b474-1f1b-4054-a922-497ef5564624',
           'new_volume_type':'ceph',
           'availability_zone':'nova'
        }
     ],
     'flavor':{
        'ram':2048,
        'ephemeral':0,
        'vcpus':1,
        'swap':'',
        'disk':20,
        'id':'2'
     },
     'include':True,
     'id':'890888bc-a001-4b62-a25b-484b34ac6e7e'
  }
]
```

ネットワークトポロジーのリストアまたはネットワークマッピングに必要な情報

警告: ネットワークトポロジーのリストアとネットワークマッピングは混在させないでください。

ネットワークトポロジーのリストアセットをアクティブ化するには:

```
restore_topology:True
```

ネットワークマッピングセットをアクティブ化するには:

```
restore_topology:False
```

ネットワークマッピングをアクティブ化するときに、networks_mapping ブロックの一部であるマッピングの詳細を提供する必要があります。

- networks snapshot_network と target_network のペアのリスト。
  - snapshot_network スナップショットでバックアップされたネットワーク。次の情報が含まれます。
    - id バックアップされたネットワークの元の ID。
    - subnet スナップショットでバックアップされたネットワークのサブネット。次の情報が含まれます。
      - id バックアップされたサブネットの元の ID。
  - target_network マッピングする既存のネットワーク。次の情報が含まれます。
    - id マッピングするネットワークの ID。
    - subnet スナップショットでバックアップされたネットワークのサブネット。次の情報が含まれます。
      - id マッピングするサブネットの ID。

選択的リストアの完全な例

```
{
   'description':u   '-',
   'oneclickrestore':False,
   'openstack':{
      'instances':[
         {
            'name':'cdcentOS-1-selective',
            'availability_zone':'US-East',
            'nics':[
               {
                  'mac_address':'fa:16:3e:00:bd:60',
                  'ip_address':'192.168.0.100',
                  'id':'8b871820-f92e-41f6-80b4-00555a649b4c',
                  'network':{
                     'subnet':{
                        'id':'2b1506f4-2a7a-4602-a8b9-b7e8a49f95b8'
```

```
                },
                'id':'d5047e84-077e-4b38-bc43-e3360b0ad174'
             }
          }
       ],
       'vdisks':[
          {
             'id':'4cc2b474-1f1b-4054-a922-497ef5564624',
             'new_volume_type':'ceph',
             'availability_zone':'nova'
          }
       ],
       'flavor':{
          'ram':2048,
          'ephemeral':0,
          'vcpus':1,
          'swap':'',
          'disk':20,
          'id':'2'
       },
       'include':True,
       'id':'890888bc-a001-4b62-a25b-484b34ac6e7e'
    }
 ],
 'restore_topology':False,
 'networks_mapping':{
    'networks':[
       {
          'snapshot_network':{
             'subnet':{
                'id':'8b609440-4abf-4acf-a36b-9a0fa70c383c'
             },
             'id':'8b871820-f92e-41f6-80b4-00555a649b4c'
          },
          'target_network':{
             'subnet':{
                'id':'2b1506f4-2a7a-4602-a8b9-b7e8a49f95b8'
             },
             'id':'d5047e84-077e-4b38-bc43-e3360b0ad174',
             'name':'internal'
          }
       }
    ]
```

```
        }
    },
    'restore_type':'selective',
    'type':'openstack',
    'name':'getjson2'
}
```

インプレースリストアに必要な情報

インプレースリストアは、選択的リストアより必要な情報が少なくて済みます。リストアするインスタンスとボリュームに関するいくつかの情報を含むベースファイルのみが必要です。

インスタンスに必要な情報

- `id` スナップショット内のインスタンスの ID。
- `restore_boot_disk` その VM のブートディスクをリストアする場合は、True に設定します。

ブートディスクが Cinder ディスクでもある場合は、両方の値を true に設定する必要があります。

- `include` このインスタンスの少なくとも 1 つのボリュームをリストアする場合は、True に設定します。
- `vdisks` インスタンスに接続されているディスクのリスト。各ディスクには次が含まれます。
  - `id` ボリュームの元の ID。
  - `restore_cinder_volume` ボリュームをリストアする場合は、True に設定します。
  - `new_volume_type` リストアされたボリュームのボリューム形式。元のボリュームと同じ値に設定します。

ネットワークマッピングに必要な情報

ネットワーク情報は必要ありませんが、リストアを機能させるにはフィールドの値が空である必要があります。

インプレースリストアの完全な例

```
{
    'description':u   '-',
    'name':'Inplace Restore',
    'zone':'',
```

```
   'oneclickrestore':False,
   'restore_type':u   'inplace',
   'type':u   'openstack',
   'openstack':{
      'instances':[
         {
            'restore_boot_disk':True,
            'include':True,
            'id':'ba8c27ab-06ed-4451-9922-d919171078de',
            'vdisks':[
               {
                  'restore_cinder_volume':True,
                  'id':'04d66b70-6d7c-4d1b-98e0-11059b89cba6',
                  'new_volume_type':'ceph'
               }
            ]
         }
      ],
      'restore_topology':False,
      'networks_mapping':{
         'networks':[
         ]
      }
   }
}
```

ファイル検索について

ファイル検索機能を使用すると、1 つ以上のバックアップでポリシー内の選択した VM に存在するファイルとフォルダを検索できます。

Horizon のファイル検索タブへのナビゲート

ファイル検索タブはすべてのポリシー概要に含まれます。これを表示するには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. ファイル検索を実行するポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [ファイル検索 (File Search)]をクリックして、ファイル検索タブで値を入力します。

Horizon でのファイル検索の構成と開始

ファイル検索は、指定された検索文字列を使用して、選択したバックアップのサブセットの単一の仮想マシンに対して実行されます。

ファイル検索を実行するには、次の要素を決定して構成する必要があります。

ファイル検索を実行する VM の選択

[VM 名/ID (VM Name/ID)]で、検索が行われる VM を選択します。ドロップダウンメニューには、ポリシーのスナップショットに含まれるすべての VM のリストが表示されます。

ポリシーによるアクティブな保護対象ではなくなったが既存のスナップショットに含まれる VM は赤で一覧表示されます。

ファイルパスの設定

ファイルパスは、選択した VM とスナップショットに対して実行される検索文字列を定義します。この検索文字列は基本の RegEx をサポートします。

ファイルパスは「/」で始まる必要があります。

Windows パーティションは完全にサポートされます。各パーティションは独自の root を持つ独自のボリュームです。「C:」の代わりに「/Windows」を使用します。

ファイル検索は、常にファイルパスに指定されたディレクトリに対して実行され、それより深いディレクトリに対しては行われません。

/etc 内のすべてのファイルのファイルパスの例: /etc/*

検索するスナップショットの定義

「スナップショットのフィルタ基準」は、設定する必要がある 3 番目および最後のコンポーネントです。これにより、検索するスナップショットが定義されます。

事前フィルタリングには、次の 3 つのオプションがあります。

1. すべてのスナップショット: 利用可能なすべてのスナップショットから、選択した VM を含むすべてのスナップショットを一覧表示します。
2. 最後のスナップショット: 最後の 10、25、50、またはカスタムの個数のスナップショットを選択し、[適用 (Apply)]をクリックして、選択した VM 内の条件に一致する利用可能なスナップショットのリストを取得します。
3. 日付範囲: 開始日と終了日を設定し、[適用 (Apply)]をクリックして、選択した VM 内の設定した日付に含まれる利用可能なすべてのスナップショットのリストを取得します。

事前フィルタリングが完了すると、一致するすべてのスナップショットが事前に自動的に選択されます。検索対象にしないスナップショットがある場合はそのチェックマークをはずします。

メモ: スナップショットが選択されていないと、ファイル検索は開始されません。

Horizon でのファイル検索の開始と結果の取得

ファイル検索を開始するには、次の要素を設定する必要があります。

- 検索する VM の選択
- 有効なファイルパスの指定
- 検索する 1 つ以上のスナップショットの選択

これらを設定したら、[検索 (Search)]をクリックしてファイル検索を開始します。

警告: ファイル検索を開始した後、他の Horizon タブまたは Web サイトに移動しないでください。失われた結果を再取得するには、検索を繰り返す必要があります。

しばらくすると結果が表示されます。結果は、スナップショットとスナップショット内のボリューム別にグループ化された表形式で表示されます。

見つかった各ファイルまたはフォルダについて、次の情報が提供されます。

- POSIX 権限
- ファイルまたはフォルダを指すリンクの量
- ファイルまたはフォルダを所有するユーザー ID
- ファイルまたはフォルダに割り当てられたグループ ID
- ファイルまたはフォルダの実際のサイズ (バイト単位)
- 作成時刻
- 前回の変更時刻
- 最終アクセス時刻
- 見つかったファイルまたはフォルダへの絶対パス

目的のスナップショットが特定されると、表の上部にある[スナップショットの表示 (View Snapshot)]オプションを使用してスナップショットに直接移動できます。また、表の最後にある[スナップショットのマウント (Mount Snapshot)]ボタンを使用して、スナップショットを直接マウントすることもできます。

CLI ファイル検索の実行

```
nbosjm filepath-search [--snapshotids <snapshotid>]
                            [--end_filter <end_filter>]
                            [--start_filter <start_filter>]
                            [--date_from <date_from>]
                            [--date_to <date_to>]
                            <vm_id> <file_path>
```

- <vm_id> 検索する VM の ID
- <file_path> 検索するファイルのパス
- --snapshotids <snapshotid> 指定されたスナップショット ID (snapshotid) でのみ検索します。この UUID を持つインスタンスを含めます
- --end_filter <end_filter> 最後のスナップショット (最後の 10 個のスナップショットなど) を表示します。デフォルトの 0 はすべてのスナップショットを表示することを意味します
- --start_filter <start_filter> 5 つ目のスナップショットから、など、指定されたスナップショットから表示します。デフォルトの 0 は最初のスナップショットから開始することを意味します
- --date_from <date_from> 「YYYY-MM-DDTHH:MM:SS」の形式の開始日付 (2016-10-10T00:00:00 など)。時間を指定しない場合は、デフォルトで 00:00 になります
- --date_to <date_to> 「YYYY-MM-DDTHH:MM:SS」の形式の終了日付 (デフォルトは現在の日付)。date_from と date_to の同じ日付の結果を含めてまたは除外してスナップショットを取得するには、HH:MM:SS を指定します。

スナップショットのマウントについて

NetBackup for OpenStack では、スナップショットからファイルを表示またはダウンロードできます。スナップショットがマウントされた時にファイルまたはディレクトリに加えられた変更は一時的なものとなり、スナップショットのマウントが解除されると破棄されます。マウントは、1 つまたは複数のファイルをリストアするためのより簡単な方法です。スナップショットをマウントするには、次の手順に従います。

ファイルリカバリマネージャインスタンスの作成

Ubuntu、CentOS、RHEL などの Linux ベースのクラウドイメージを使用して OpenStack イメージを作成します。次のメタデータパラメータを追加し、クラウドイメージを Glance にアップロードします。

```
--file <File Manager Image Path> ¥
--container-format bare ¥
--disk-format qcow2 ¥
--public ¥
--property hw_qemu_guest_agent=yes ¥
--property nbos_recovery_manager=yes ¥
--property hw_disk_bus=virtio ¥
nbos-file-manager
```

そのイメージからインスタンスをスピンアップします。マウント操作には少なくとも 8 GB の RAM を使用することをお勧めします。より大きいスナップショットはより多くの RAM を必要とすることがあります。

CentOS と RHEL クラウドイメージへの適用手順

1. qemu-guest-agent をインストールしてアクティブ化します。
2. BLACKLIST_RPC セクションで次のように、`/etc/sysconfig/qemu-ga` を編集して削除します。

   ```
   guest-file-read
   guest-file-write
   guest-file-open
   guest-file-close
   ```

3. /etc/sysconfig/selinux で SELINUX を無効にします。

   ```
   SELINUX=disabled
   ```

4. Python 3 をインストールします。

   ```
   yum install python3
   ```

5. lvm2 をインストールします。

   ```
   yum install lvm2
   ```

6. インスタンスを再起動します。

Ubuntu クラウドイメージへの適用手順

1. qemu-guest-agent をインストールしてアクティブ化します。
2. `/etc/init.d/qemu-guest-agent` を編集し、daemon args に Freeze-Hook ファイルパスを追加します。

   ```
   DAEMON_ARGS="-F/etc/qemu/fsfreeze-hook
   ```

3. qemu-guest-agent サービスを再起動します。
4. Python 3 をインストールします。

   ```
   apt-get install python3
   ```

5. インスタンスを再起動します。

スナップショットのマウント

File Recovery Manager にスナップショットをマウントすると、マウントされたスナップショットにあるすべてのデータに対する読み取りアクセスが可能になります。

マウントされたスナップショットをマウントし続ける必要がなくなったら、マウント解除します。マウントされたスナップショットは、保持ポリシーによってパージされません。

任意の OpenStack インスタンスに対してマウントプロセスを実行できます。この処理中、インスタンスは再起動されます。

スナップショットは、常に File Recovery Manager インスタンスにのみマウントします。

Horizon の使用

Horizon でのスナップショットのマウントには、2 つの可能性があります。

スナップショットリストの使用

スナップショットリストを使用してスナップショットをマウントするには、次の手順に従います。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. マウントするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. スナップショットリストで検索したスナップショットを特定します。
6. [処理 (Actions)]列のドロップダウンから、[ワンクリックリストア (OneClick Restore)]を選択します。
7. [スナップショットのマウント (Mount Snapshot)]をクリックします。

8. マウントする File Recovery Manager インスタンスを選択します。
9. ［マウント (Mount)］をクリックして確認します。

プロジェクトのすべてのインスタンスが一覧表示され、File Recovery Manager インスタンスがあるはずです。File Recovery Manager イメージに次のプロパティセットがあることを管理者として確認します。

```
nbos_recovery_manager=yes
```

ファイル検索結果の使用

ファイル検索結果を使用してスナップショットをマウントするには、次の手順に従います。

1. Horizon コンソールで、［NBOS バックアップ (NBOS Backups)］、［ポリシー (Policies)］の順に移動します。
2. マウントするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. ［ファイル検索 (File Search)］タブに移動します。
5. ファイル検索を実行します。
6. マウントするスナップショットを特定します。
7. 選択したスナップショットの［スナップショットのマウント (Mount Snapshot)］をクリックします。
8. マウントする File Recovery Manager インスタンスを選択します。
9. ［マウント (Mount)］をクリックします。

プロジェクトのすべてのインスタンスが一覧表示され、File Recovery Manager インスタンスがあるはずです。File Recovery Manager イメージに次のプロパティセットがあることを管理者として確認します。

```
nbos_recovery_manager=yes
```

CLI の使用

```
nbosjm snapshot-mount <snapshot_id> <mount_vm_id>
```

- <snapshot_id> マウントするスナップショットの ID
- <mount_vm_id> スナップショットをマウントする File Recovery Manager インスタンスの ID。

File Recovery Manager へのアクセス

File Recovery Manager は、通常の Linux ベースの OpenStack インスタンスです。

SSH または、FileZila や WinSCP などの SSH ベースのツールを介してアクセスできます。

多くの場合、クラウドイメージでは SSH ログインはデフォルトでは無効になっています。必要に応じて SSH ログインを有効にします。

マウントされたスナップショットは次のパスにあります。

```
/home/ubuntu/nbos-mounts/mounts/
```

スナップショット内の各 VM には、識別子として VM_ID を使用する独自のディレクトリがあります。

マウントされたスナップショットの識別

スナップショットが長期間マウントされる場合があるため、識別することが重要です。

Horizon の使用

Horizon 内でマウントされたスナップショットの識別には、2 つの可能性があります。

File Recovery Manager インスタンスのメタデータから

1. Horizon コンソールで、[計算 (Compute)]、[インスタンス (Instances)]の順に移動します。
2. File Recovery Manager インスタンスを特定します。
3. File Recovery Manager インスタンスの名前をクリックして、その詳細を表示します。
4. [概要 (Overview)]タブで、メタデータを検索します。
5. `mounted_snapshot_url` の値を特定します

`mounted_snapshot_url` には、最後にマウントされたスナップショットのスナップショット ID が含まれます。

メモ: この値は、新しいスナップショットがマウントされたときにのみ更新されます。

スナップショットリストから

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. マウントするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. [スナップショットをマウント解除 (Unmount Snapshot)]オプションがあるスナップショットを検索します。

CLI の使用

```
nbosjm snapshot-mounted-list [--policyid <policyid>]
```

- `--policyid <policyid>` 指定されたポリシーのスナップショットにリストを制限します

スナップショットのマウント解除

マウントされたスナップショットが不要になったら、スナップショットをマウント解除することをお勧めします。

スナップショットをマウント解除すると、次のスナップショットをマウントするために File Recovery Manager インスタンスが解放され、NetBackup for OpenStack 保持ポリシーで以前にマウントされたスナップショットがパージされます。

警告: File Recovery Manager インスタンスを削除しても NetBackup for OpenStack アプライアンスは更新されません。スナップショットは、マウント解除コマンドを受信するまでマウントされたと見なされます。

Horizon の使用

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. マウントするスナップショットを含むポリシーを特定します。
3. ポリシーの概要を入力するポリシー名をクリックします。
4. [スナップショット (Snapshots)]タブに移動します。
5. [スナップショットをマウント解除 (Unmount Snapshot)]オプションがあるスナップショットを検索します。
6. [スナップショットをマウント解除 (Unmount Snapshot)]をクリックします。

CLI の使用

```
nbosjm snapshot-dismount <snapshot_id>
```

- `<snapshot_id>` マウント解除するスナップショットの ID。

スケジューラについて

すべてのポリシーに独自のスケジュールがあります。これらのスケジュールは、有効化、無効化、変更できます。

スケジュールは次によって定義されます。

- 状態 (有効/無効)
- 開始日/時刻
- 終了日
- 2 つのスナップショット間の時間

スケジュールの無効化

Horizon の使用

Horizon で単一ポリシーのスケジューラを無効にするには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 変更するポリシーを識別します。
3. [処理 (Actions)]列のドロップダウンから、[ポリシーの編集 (Edit Policy)]を選択します。
4. [スケジュール (Schedule)]タブに移動します。
5. [有効 (Enabled)]のチェックマークをはずします。
6. [更新 (Update)]をクリックします。

CLI の使用

```
nbosjm disable-scheduler --policyids <policyid>
```

- `--policyid <policyid>` 少なくとも 1 つのポリシー ID が必要です。スケジューラを無効にするポリシーの ID を指定します。複数のポリシーを含める場合は、オプションを複数回指定します。`--policyids <policyid> --policyids <policyid>`

スケジュールの有効化

Horizon の使用

Horizon で単一ポリシーのスケジューラを有効にするには、次の手順を実行します。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[ポリシー (Policies)]の順に移動します。
2. 変更するポリシーを識別します。
3. [処理 (Actions)]列のドロップダウンから、[ポリシーの編集 (Edit Policy)]を選択します。
4. [スケジュール (Schedule)]タブに移動します。
5. [有効 (Enabled)]を選択します。
6. [更新 (Update)]をクリックします。

CLI の使用

```
nbosjm enable-scheduler --policyids <policyid>
```

- `--policyid <policyid>` 少なくとも 1 つのポリシー ID が必要です。スケジューラを有効にするポリシーの ID を指定します。複数のポリシーを含める場合は、オプションを複数回指定します。`--policyids <policyid> --policyids <policyid>`

スケジュールの変更

スケジュールを変更するには、ポリシー自体を変更する必要があります。

p.109 の「ポリシーの編集」を参照してください。

電子メール通知について

NetBackup for OpenStack では、バックアップとリストアのたびに電子メールを介してユーザーに通知できます。

電子メールはポリシーの所有者に送信されます。

電子メール通知をアクティブ化するための要件

電子メール通知を使用するには、2 つの要件を満たす必要があります。

どちらの要件も、OpenStack 管理者が設定または構成する必要があります。要件を確認するには、OpenStack 管理者にお問い合わせください。

- 割り当てられたユーザー電子メール
  電子メールがポリシーの所有者に送信されるため、ポリシーを作成した OpenStack ユーザーに電子メールアドレスが関連付けられている必要があります。
- 構成済み NetBackup for OpenStack 電子メールサーバー

NetBackup for OpenStack は、電子メール通知の送信に使用する電子メールサーバーを把握している必要があります。バックアップ管理者は、Horizon 内の特定の領域でこれを実行できます。

電子メール通知のアクティブ化または非アクティブ化

電子メール通知はテナント全体でアクティブ化されます。テナントで電子メール通知機能をアクティブ化するには、次の手順に従います。

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[設定 (Settings)] の順に移動します。
2. [電子メールアラートの有効化 (Enable Email Alerts)]チェックボックスにチェックマークを付けるか、はずします。

7

バックアップ管理タスクの実行

この章では以下の項目について説明しています。

NBOS バックアップ管理領域

NetBackup for OpenStack はサービスとしてのバックアップを提供します。これにより、OpenStack ユーザーは自分のバックアップ自体を管理および制御できます。これにより、バックアップソリューションの全体像を把握する、バックアップ管理者の必要性がなくなることはありません。

バックアップ管理者に必要なツールを提供するために、NetBackup for OpenStack は、API と CLI に加えて Horizon の NBOS バックアップ管理領域も提供します。

NBOS バックアップ管理領域へのアクセス

NBOS バックアップ管理領域にアクセスするには、次の手順に従います。

1. 管理者ユーザーを使用して Horizon にログオンします。

2. ［管理 (Admin)］、［NBOS バックアップ管理 (NBOS Backup Admin)］、［NetBackupOpenStack］の順に移動します。

［NBOS バックアップ管理 (NBOS Backup Admin)］領域には次の機能があります。

特定のテナントの情報をフィルタ処理して表示することもできます。

状態の概要

状態の概要は、常に［NBOS バックアップ管理 (NBOS Backup Admin)］領域に表示されます。次のような、最も必要な情報を一目で確認できます。

- ストレージ使用状況 (NFS のみ)
- 既存の VM 数と比較した保護対象 VM の数
- 現在実行中のスナップショットの数
- NBOS ノードの状態
- NBOSDM サービスの状態

サービスが実行中で状態が良好なときに、ノードの状態が表示されます。

［ポリシー (Policies)］タブ

このタブには、その時点に存在するすべてのポリシーに関する情報が表示されます。これは、すべてのバックアップ管理者にとって最も重要な概要タブであるため、NBOS バックアップ管理領域を開いたときのデフォルトのタブとして表示されます。

次の情報が表示されます。

- ポリシーを所有するユーザーの ID
- ポリシーを含むプロジェクト
- ポリシー名
- ポリシー形式
- 可用性ゾーン
- 保護対象の VM の数
- 直近の 30 個のバックアップに関するパフォーマンス情報
  - バックアップされたデータの量 (緑色のバー)
  - バックアップにかかった時間 (赤い線)
- 増分 (赤) バックアップと比較した完全 (青) バックアップの数を示す円グラフ
- 成功したバックアップの数

- 失敗したバックアップの数
- そのポリシーによって使われるストレージ
- 使用されるバックアップターゲット
- 次回のスナップショット実行のタイミング
- ポリシーの一般的な間隔
- ポリシーを無効化または有効化するためのスイッチを含むスケジューラの状態

[使用状況 (Usage)]タブ

管理者は多くの場合、大量のリソースが使用されている場所を把握する必要があります。また、課金システムに使用状況の情報をすばやく提供する必要があります。このタブは次の情報を提供して、これらのタスクで役立ちます。

- テナントが使用するストレージ
- テナントによって保護される VM

ドリルダウンすると、ポリシー別に、さらに保護された VM 別に同じ情報を表示できます。

[使用状況 (Usage)]タブには、テナントによってアクティブに使用されなくなったが、バックアップターゲット上に存在するポリシーと VM が表示されます。

[ノード (Nodes)]タブ

このタブには、NetBackup for OpenStack クラスタノードに関する情報が表示されます。次の情報が表示されます。

- ノード名
- ノード ID
- ノードの NetBackup for OpenStack バージョン
- IP アドレス
- アクティブコントローラノード (True/False)
- ノードの状態

仮想 IP は独自のノードとして表示されます。これは通常、現在アクティブなコントローラノードの直下に表示されます。

[NBOSDM]タブ (NetBackup for OpenStack Datamover サービス)

このタブには、NetBackup for OpenStack Datamover サービスに関する情報が表示されます。次の情報が表示されます。

- サービス名
- サービスが実行されている計算ノード
- ゾーン
- OpenStack の観点から見たサービスの状態 (有効または無効)
- サービスのバージョン
- 一般的な状態
- 状態が最後に更新された時間

[ストレージ (Storage)]タブ

このタブには、バックアップターゲットストレージに関する情報が表示されます。ここには、次の情報が含まれます。

- ストレージ名

ストレージ名をクリックすると、そのストレージに格納されているすべてのポリシーの概要が表示されます。

- ストレージの容量
- ストレージの総利用率
- ストレージの状態
- 統計情報
  - すべてのストレージが使用されている割合
  - 完全バックアップに使用されるストレージの割合
  - 完全バックアップと増分バックアップの数

[監査 (Audit)]タブ

監査ログは、ポリシーの作成、スナップショットの作成など、ユーザーが実行するポリシー関連の一連のアクティビティを提供します。次の情報が表示されます。

- エントリの日時
- 実行されたタスク
- タスクが実行されたプロジェクト
- タスクを実行したユーザー

監査ログでは、特定のユーザーが実行したエントリのみなど、検索する文字列に対して検索を実行できます。

また、必要に応じて、表示される時間枠を変更できます。

[ポリシー属性 (Policy Attributes)]タブ

[ポリシー属性 (Policy Attributes)]タブを使用すると、管理者はポリシー属性を操作できます。

p.151 の「[ポリシー (Policies)]タブ」を参照してください。

[設定 (Settings)]タブ

このタブは、クラウド全体のすべてのグローバル設定を管理します。NetBackup for OpenStack には 2 種類の設定があります。

1. 電子メールの設定
2. ジョブスケジューラの設定。

電子メールの設定

これらの設定は、ユーザーにスナップショットとリストアの電子メールレポートを送信するために NetBackup for OpenStack で使用されます。

電子メールの設定は、OpenStack ユーザーに電子メール通知を提供するために必要です。

電子メールを設定するには、次の情報が必要です。

- SMTP サーバー
- SMTP ユーザー名
- SMTP パスワード
- SMTP ポート
- SMTP タイムアウト
- 送信者の電子メールアドレス

テスト電子メールは構成ページから直接送信できます。

CLI を使用して電子メール設定を操作するには、次のコマンドを使用します。

電子メール設定を初めてまたは削除後に設定するには、次のコマンドを使用します。

```
nbosjm setting-create [--description <description>]
                            [--category <category>]
                            [--type <type>]
                            [--is-public {True,False}]
```

```
                                [--is-hidden {True,False}]
                                [--metadata <key=value>]
                                <name> <value>
```

- --description 省略可能な説明 (デフォルト = なし)。電子メールの設定には必要ありません。
- --category 省略可能な設定カテゴリ (デフォルト = なし)。電子メールの設定には必要ありません。
- --type 設定の種類。email_settings に設定します
- --is-public 設定を一般公開するかどうかを設定します。False に設定します。
- --is-hidden 設定を常に非表示にするかどうかを設定します。False に設定します。
- --metadata 設定を一般公開するかどうかを設定します。電子メールの設定には必要ありません。
- <name> 設定の名前。
- <value> 設定の値。

すでに設定されている電子メール設定を CLI を介して更新するには、次を使用します。

```
nbosjm setting-update [--description <description>]
                              [--category <category>]
                              [--type <type>]
                              [--is-public {True,False}]
                              [--is-hidden {True,False}]
                              [--metadata <key=value>]
                              <name> <value>
```

- --description 省略可能な説明 (デフォルト = なし)。電子メールの設定には必要ありません。
- --category 省略可能な設定カテゴリ (デフォルト = なし)。電子メールの設定には必要ありません。
- --type 設定の種類。email_settings に設定します。
- --is-public 設定を一般公開するかどうかを設定します。False に設定します。
- --is-hidden 設定を常に非表示にするかどうかを設定します。False に設定します。
- --metadata 設定を一般公開するかどうかを設定します。電子メールの設定には必要ありません。
- <name> 設定の名前。
- <value> 設定の値。

すでに設定されている電子メール設定を表示するには、次を使用します。

```
nbosjm setting-show [--get_hidden {True,False}] <setting_name>
```

- `--get_hidden` 非表示の設定 (True) または表示 (False)。電子メールの設定には必要ありません。設定する場合は `False` を使用します。
- `<setting_name>` 表示する設定の名前。

設定した電子メール設定を削除するには、次を使用します。

```
nbosjm setting-delete <setting_name>
```

- `<setting_name>` 削除する設定の名前。

設定名	値の種類	例
smtp_default___recipient	文字列	admin@example.net
smtp_default___sender	文字列	admin@example.net
smtp_port	整数	587
smtp_server_name	文字列	Mailserver_A
smtp_server_username	文字列	admin
smtp_server_password	文字列	password
smtp_timeout	整数	10
smtp_email_enable	ブール値	True

ジョブスケジューラの無効化または有効化

グローバルジョブスケジューラを使用すると、スケジュールされたポリシーを 1 つずつ変更せずにすべてを無効化できます。

バックアップ管理の領域でグローバルジョブスケジューラを無効または有効にするには、次の手順を実行します。

1. 管理者ユーザーを使用して Horizon にログオンします。
2. [管理 (Admin)]、[NBOS バックアップ管理 (NBOS Backup Admin)]、[NetBackupOpenStack]、[設定 (Settings)]の順に移動します。
3. [ジョブスケジューラの無効化または有効化 (Disable/Enable Job Scheduler)]をクリックします。

4. ［ジョブスケジューラの有効化 (Job Scheduler Enabled)］ボックスを選択またはクリアします。
5. ［変更 (Change)］をクリックして確定します。

グローバルジョブスケジューラは CLI でも制御できます。

グローバルジョブスケジューラの状態を取得するには、次を使用します。

```
nbosjm get-global-job-scheduler
```

グローバルジョブスケジューラを無効にするには、次を使用します。

```
nbosjm disable-global-job-scheduler
```

グローバルジョブスケジューラを有効にするには、次を使用します。

```
nbosjm enable-global-job-scheduler
```

ポリシー属性

NetBackup for OpenStack のテナント主導のバックアップサービスにより、テナントはバックアップポリシーを制御できます。ただし、テナントに必要な制御を超えているために、場合によっては、クラウド管理者がテナントに許可するポリシーを制限することが必要です。たとえば、テナントが頻繁に完全バックアップを実行したためにクォータを超過する場合があります。すべてのテナントがそのようなバックアップポリシーに従った場合、クラウドインフラに設定されているリソース制限に影響する可能性があります。代わりに、クラウド管理者が事前定義済みのバックアップポリシーを定義でき、各テナントがそれらのポリシーのみに制限されている場合、クラウド管理者はバックアップサービスをより適切に制御できます。

ポリシーは、テナントが任意のインスタンスを作成できない nova フレーバーに似ています。代わりに、各テナントは管理者が公開した nova フレーバーのみを使用できます。

利用可能なポリシーの一覧表示

Horizon の使用

Horizon で利用可能なすべてのポリシーを表示するには、次の手順に従います。

1. 管理者ユーザーを使用して Horizon にログオンします。
2. ［管理 (Admin)］、［NBOS バックアップ管理 (NBOS Backup Admin)］、［NetBackupOpenStack］、［ポリシー属性 (Policy Attributes)］の順に移動します。

次の情報が、利用可能な各ポリシーのポリシータブに表示されます。

- 作成時刻
- 名前
- 説明
- 状態
- 設定された間隔
- 設定された保持形式
- 設定された保持の値
- 完全バックアップ間隔
- 処理

CLI の使用

```
nbosjm policy-list
```

```
nbosjm policy-show <policy_attribute_id>
```

- `<policy_attribute_id>` 表示するポリシーの ID。

ポリシー属性の作成

Horizon の使用

Horizon でポリシー属性を作成するには、次の手順に従います。

1. 管理者ユーザーを使用して Horizon にログオンします。
2. [管理 (Admin)]、[NBOS バックアップ管理 (NBOS Backup Admin)]、[NetBackupOpenStack]、[ポリシー属性 (Policy Attributes)]の順に移動します。
3. [新しいポリシー属性 (New Policy Attributes)]をクリックします。
4. [詳細 (Details)]タブで、ポリシー属性名と説明を指定します。
5. [繰り返し間隔 (Hrs) (Repeat Every (Hrs))] フィールドで、バックアップを繰り返す時間数を指定します。
6. [スナップショット保持形式 (Snapshot Retention Type)]を選択し、値を入力します。
   - 保持するスナップショットの数
   - スナップショットを保持する日数

7. ［完全バックアップ間隔 (Full Backup Interval)］のオプションのいずれかを選択します。
   - 常時 (Always)
   - スナップショット数 (Number of Snapshots)
8. ［作成 (Create)］をクリックします。

CLI の使用

```
nbosjm policy-create --policy-attribute-fields <key=key-name>
                          [--display-description
<display_description>]
                          [--metadata <key=key-name>]
                          [--display-name <display-name>]
```

- `--policy-attribute-fields <key=key-name>` ポリシー属性フィールドに次のキーと値のペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。
  - `interval` バックアップを繰り返す時間数を指定します。
    指定可能な値: 1 から 24
    デフォルト値: 1
  - `retention_policy_type` スナップショットの保持形式を指定します。
    指定可能な値: 保持するスナップショットの数またはスナップショットを保持する日数
    デフォルト値: 保持するスナップショットの数
  - `retention_policy_value` 保持するスナップショットの数またはスナップショットを保持する日数を指定します。
    指定可能な値: 1 から 365
    デフォルト値: 30
  - `fullbackup_interval` 完全バックアップを作成するまでの増分バックアップの数を指定します。
    指定可能な値: 0 から 999。常に完全バックアップを作成するには、0 を指定します。
    デフォルト値: 5

  次に例を示します。

  ```
  nbosjm policy-create –policy-attribute-fields interval="1 hr"
  –policy-attribute-fields retention_policy_type="Number of Snapshots
  to Keep" –policy-attribute-attribute-fields
  ```

```
retention_policy_value="30" -policy-attribute-fields
fullbackup_interval="2"
```

- --display-description <display_description> オプションのポリシーの説明。(デフォルト = 説明なし)
- --metadata <key=keyname> ポリシー形式のメタデータに含めるキーと値のペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。
- --display-name <display-name> ポリシーの名前を指定します。

ポリシー属性の編集

Horizon の使用

Horizon でポリシーを編集するには、次の手順を実行します。

1. 管理者ユーザーを使用して Horizon にログオンします。
2. [管理 (Admin)]、[NBOS バックアップ管理 (NBOS Backup Admin)]、[NetBackupOpenStack]、[ポリシー属性 (Policy Attributes)]の順に移動します。
3. 編集するポリシーを識別します。
4. 選択したポリシーの行の最後にある[ポリシー属性の編集 (Edit Policy Attribute)]をクリックします。
5. 必要に応じてポリシー属性を編集します。すべての値を変更できます。
6. [更新 (Update)]をクリックします。

CLI の使用

```
nbosjm policy-update [--display-name <display-name>]
                          [--display-description
<display-description>]
                         [--policy-attribute-fields <key=key-name>]

                          [--metadata <key=key-name>]
                          <policy_attribute_id>
```

- --display-name <display-name> ポリシー属性の名前。
- --display-description <display_description> 省略可能なポリシー属性の説明。(デフォルト = 説明なし)
- --policy-attribute-fields <key=key-name> ポリシー属性フィールドに次のキーと値のペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。

- interval バックアップを繰り返す時間数を指定します。
  指定可能な値: 1 から 24
  デフォルト値: 1
- retention_policy_type スナップショットの保持形式を指定します。
  指定可能な値: 保持するスナップショットの数またはスナップショットを保持する日数
  デフォルト値: 保持するスナップショットの数
- retention_policy_value 保持するスナップショットの数またはスナップショットを保持する日数を指定します。
  指定可能な値: 1 から 365
  デフォルト値: 30
- fullbackup_interval 完全バックアップを作成するまでの増分バックアップの数を指定します。
  指定可能な値: 0 から 999。常に完全バックアップを作成するには、0 を指定します。
  デフォルト値: 5

次に例を示します。

```
nbosjm policy-create -policy-attribute-fields interval="1 hr"
-policy-attribute-fields retention_policy_type="Number of Snapshots
to Keep" -policy-attribute-attribute-fields
retention_policy_value="30" -policy-attribute-fields
fullbackup_interval="2"
```

- --metadata <key=keyname> ポリシー形式のメタデータに含めるキーと値のペアを指定します。複数のキーを含める場合は、オプションを複数回指定します。key=value
- <policy_attribute_id> ポリシーの名前。

ポリシーの割り当てまたは削除

Horizon の使用

Horizon でポリシーを割り当てるまたは削除するには、次の手順を実行します。

1. 管理者ユーザーを使用して Horizon にログオンします。
2. [管理 (Admin)]、[NBOS バックアップ管理 (NBOS Backup Admin)]、[NetBackupOpenStack]、[ポリシー属性 (Policy Attributes)]の順に移動します。
3. 割り当てるまたは削除するポリシー属性を特定します。
4. 選択したポリシーの行の最後にあるドロップダウンをクリックします。
5. [プロジェクトの追加と削除 (Add/Remove Projects)] をクリックします。

6. プラスオプションまたはマイナスオプションを使用して、追加または削除するプロジェクトを選択します。
7. ［適用 (Apply)］をクリックします。

CLI の使用

```
nbosjm policy-assign [--add_project <project_id>]
                          [--remove_project <project_id>]
                          <policy_attribute_id>
```

- `--add_project <project_id>` ポリシーを割り当てるプロジェクトの ID。複数のプロジェクトを割り当てるには、複数回使用します。
- `--remove_project <project_id>` ポリシーを削除するプロジェクトの ID。複数のプロジェクトを削除するには、複数回使用します。
- `<policy_attribute_id>` 割り当てる、または削除するポリシー

ポリシーの削除

Horizon の使用

Horizon でポリシーを削除するには、次の手順を実行します。

1. 管理者ユーザーを使用して Horizon にログオンします。
2. ［管理 (Admin)］、［NBOS バックアップ管理 (NBOS Backup Admin)］、［NetBackupOpenStack］、［ポリシー属性 (Policy Attributes)］の順に移動します。
3. 割り当てるまたは削除するポリシーを特定します。
4. 選択したポリシーの行の最後にあるドロップダウンをクリックします。
5. ［ポリシーの削除 (Delete Policy)］をクリックします
6. ［削除 (Delete)］をクリックして確定します。

CLI の使用

```
nbosjm policy-delete <policy_attribute_id>
```

- `<policy_attribute_id>` 削除するポリシーの ID。

ポリシークォータ

NetBackup for OpenStack を使用すると、OpenStack 管理者は、プロジェクトクォータを NetBackup for OpenStack の使用状況に合わせて設定できます。

次のクォータを設定できます。

- プロジェクトで許可されるポリシーの数
- プロジェクトで許可されるスナップショットの数
- プロジェクトで保護が許可される VM の数
- プロジェクトがバックアップターゲットで使用を許可されるストレージの量

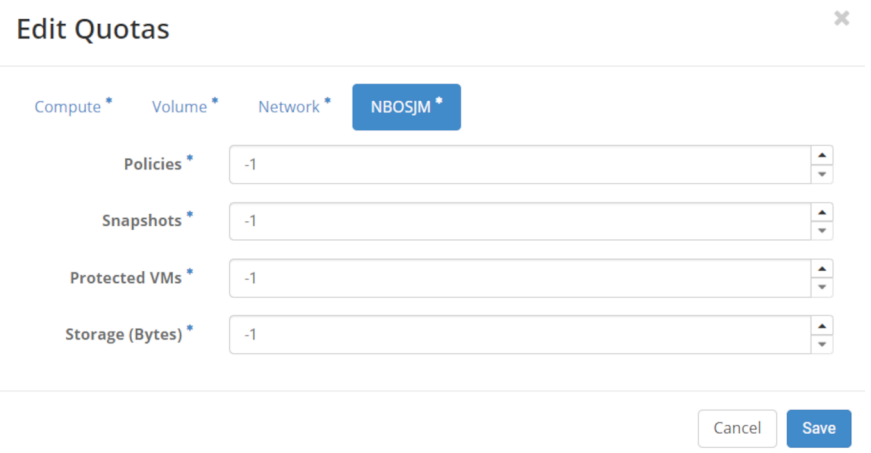
Horizon 経由のポリシークォータの操作

NetBackup for OpenStack のクォータ機能は、サポート対象のすべての OpenStack バージョンと配布で利用可能ですが、クォータ機能の Horizon 統合は、Train 以上のリリースにのみ含まれています。

ポリシークォータは、他のプロジェクトクォータと同様に管理されます。

1. 管理者ユーザーを使用して Horizon にログオンします。
2. [資格情報 (Identity)]、[プロジェクト (Projects)]の順に移動します。
3. クォータを変更または表示するプロジェクトを特定します。
4. 選択したプロジェクトの行の最後にあるドロップダウンをクリックします。
5. [クォータの変更 (Modify Quotas)]をクリックします。
6. Policy Manager に移動します。
7. 必要に応じてクォータを編集します。
8. [保存 (Save)]をクリックします。

図 7-1 Policy Manager クォータの Horizon への統合



CLI 経由のポリシークォータの操作

利用可能なクォータの種類の一覧表示

NetBackup for OpenStack は複数の異なるクォータを提供しています。次のコマンドを実行すると、それらを一覧表示できます。

メモ: NetBackup for OpenStack 9.0.0.1 には、クォータタイプのボリュームはまだ統合されていません。これを使用しても、テナントが適用する必要があるクォータは生成されません。

```
nbosjm project-quota-type-list
```

クォータの種類に関する詳細の表示

次のコマンドは、指定されたクォータの種類の詳細を表示します。

```
nbosjm project-quota-type-show <quota_type_id>
```

- `<quota_type_id>` 表示するクォータの種類の ID。

クォータの作成

次のコマンドは、特定のプロジェクトのクォータを作成し、指定した値を設定します。

```
nbosjm project-allowed-quota-create --quota-type-id quota_type_id
                                    --allowed-value allowed_value

                                      --high-watermark
high_watermark
                                      --project-id project_id
```

- `<quota_type_id>` 作成するクォータの種類の ID。
- `<allowed_value>` このクォータの種類に設定する値。
- `<high_watermark>` 高水準点の警告に設定する値。
- `<project_id>` クォータを割り当てるプロジェクト。

Horizon 経由で設定すると、高水準点は許容値の 80% に自動的に設定されます。

作成されたクォータは、独自の ID を持つ allowed_quota_object を生成します。この ID は、作成されたクォータを引き続き使用する場合に必要です。

許可されたクォータの一覧表示

次のコマンドは、特定のプロジェクトに設定されているすべての NetBackup for OpenStack クォータを一覧表示します。

```
nbosjm project-allowed-quota-list <project_id>
```

- <project_id> 一覧表示するクォータが含まれるプロジェクト。

許可されたクォータの表示

次のコマンドは、指定の許可されたクォータに関する詳細を表示します。

```
nbosjm project-allowed-quota-show <allowed_quota_id>
```

- <allowed_quota_id> 表示する許可されたクォータの ID。

許可されたクォータの更新

次のコマンドは、既存の許可されたクォータの値を更新する方法を示します。

```
nbosjm project-allowed-quota-update [--allowed-value <allowed_value>]

                                          [--high-watermark
<high_watermark>]
                                         [--project-id <project_id>]

                                          <allowed_quota_id>
```

- <allowed_value> このクォータの種類に設定する値。
- <high_watermark> 高水準点の警告に設定する値。
- <project_id> クォータを割り当てるプロジェクト。
- <allowed_quota_id> 更新する許可されたクォータの ID。

許可されたクォータの削除

次のコマンドは、許可されたクォータを削除し、影響を受けるプロジェクトの接続済みクォータの種類の値を無制限に設定します。

```
nbosjm project-allowed-quota-delete <allowed_quota_id>
```

- <allowed_quota_id> 削除する許可されたクォータの ID。

信頼の管理

NetBackup for OpenStack は、NetBackup for OpenStack サービスユーザーが別の OpenStack ユーザーの名前で処理できるようにする OpenStack Keystone Trust システムを使用しています。

このシステムは、すべてのバックアップおよびリストア機能で使用されます。

OpenStack 管理者は、作成された信頼を直接操作する必要はありません。NetBackup for OpenStack の構成中にクラウドの信頼が作成され、ポリシーの作成または変更時に必要に応じてさらに信頼が作成されます。

信頼は CLI を介してのみ使用できます

すべての信頼の一覧表示

```
nbosjm trust-list
```

信頼の表示

```
nbosjm trust-show <trust_id>
```

- <trust_id> 表示する信頼の ID。

信頼の作成

```
nbosjm trust-create [--is_cloud_trust {True,False}] <role_name>
```

- <role_name> 信頼が作成される役割の名前。
- --is_cloud_trust {True,False} クラウド管理者の信頼を作成する場合は、true に設定します。クラウドの信頼を作成するときは、NetBackup for OpenStack を構成するために使用されたのと同じユーザーとテナントを使用し、管理者の役割を維持します。

信頼の削除

```
nbosjm trust-delete <trust_id>
```

- <trust_id> 削除する信頼の ID。

ポリシーのインポートと移行

各 NetBackup for OpenStack ポリシーには専用の所有者が存在します。ポリシーの所有権は次によって定義されます。

- OpenStack ユーザー: ポリシーに割り当てられた OpenStack ユーザー ID。
- OpenStack プロジェクト: ポリシーに割り当てられた OpenStack プロジェクト ID。
- OpenStack クラウド: ポリシーに割り当てられた NetBackup for OpenStack のサービスユーザー ID。

OpenStack ユーザーは、ポリシーを変更することで、ポリシーのユーザー所有権を更新できます。

この所有権は、ポリシーの所有者のみがポリシーを操作できることを保証します。

OpenStack 管理者は、古い NetBackup for OpenStack インストールからポリシーを再割り当てするか、ポリシーを再インポートできます。

ポリシーのインポート

ポリシーのインポートでは、バックアップターゲット上に存在するポリシーを NetBackup for OpenStack データベースにインポートできます。

ポリシーのインポートは、OpenStack Cloud が所有するポリシーをインポートするように設計されています。別のクラウドが所有するポリシーはインポートまたは一覧表示されません。

インポート可能なポリシーのリストを取得するには、次の CLI コマンドを使用します。

```
nbosjm policy-get-importpolicies-list [--project_id <project_id>]
```

- --project_id <project_id> 特定のプロジェクトのみに属するポリシーを一覧表示します。

ポリシーを NetBackup for OpenStack データベースにインポートするには、次の CLI コマンドを使用します。

```
nbosjm policy-importpolicies [--policies <policyid>]
```

- --policyids <policyid> インポートするポリシー ID を指定します。複数のポリシーに対してオプションを繰り返します。

孤立したポリシー

孤立したポリシーは、特定の NetBackup for OpenStack インストールの観点から定義されます。バックアップターゲットストレージにあるが、NetBackup for OpenStack インストールで認識されていないポリシーは孤立していると見なされます。

さらに、以前に同じクラウド内のプロジェクトまたはユーザーが所有していたポリシー間で分割されたり、異なるクラウドから移行された場合も同様に認識されます。

次の CLI コマンドは孤立したポリシーのリストを提供します。

```
nbosjm policy-get-orphaned-policies-list [--migrate_cloud
{True,False}]
[--generate_yaml {True,False}]
```

- `--migrate_cloud {True,False}` 他のクラウドのポリシーも一覧表示する場合は、True に設定します。デフォルトは False です。
- `--generate_yaml {True,False}` ポリシー再割り当て API の入力として使用する yaml 形式で出力ファイルを生成する場合は、True に設定します。

多くのポリシーを含むバックアップターゲットに対してこのコマンドを実行すると、少し時間がかかることがあります。NetBackup for OpenStack は完全なストレージを読み込み、データベースで認識されているポリシーに対して見つかったすべてのポリシーを検証します。

ポリシーの再割り当て

OpenStack 管理者は、ポリシーを新しい所有者に再割り当てできます。これには、あるクラウドから別のクラウドまたはプロジェクト間でポリシーを移行する可能性が含まれます。

警告: ポリシーを再割り当てすると、ターゲット NetBackup for OpenStack インストールのデータベースのみが変更されます。異なる NetBackup インストールによって管理されるようになったため、元のソースインストールは更新されません。

次の CLI コマンドを使ってポリシーを再割り当てします。

```
nbosjm policy-reassign-policies
[--old_tenant_ids <old_tenant_id>]
[--new_tenant_id <new_tenant_id>]
[--policy_ids <policy-id>]
[--user_id <user_id>]
[--migrate_cloud {True,False}]
```

```
[--map_file <map_file>]
```

- `--old_tenant_ids <old_tenant_id>` ポリシーを新しいテナントに再割り当てする必要がある古いテナント ID を指定します。複数のテナントからポリシーを選択するには、複数回指定します。
- `--new_tenant_id <new_tenant_id>` ポリシーを古いテナントから再割り当てする必要がある新しいテナント ID を指定します。1 つの対象テナントのみを指定できます。
- `--policy_ids <policy-id>` 新しいテナントに再割り当てする必要があるポリシーの ID を指定します。指定されない場合は、古いテナントのすべてのポリシーが新しいテナントに再割り当てされます。複数のポリシーを含める場合は、複数回指定します。
- `--user_id <user_id>` 古いテナントからポリシーを再割り当てする必要があるユーザー ID を指定します。1 人の対象ユーザーのみを指定できます。
- `--migrate_cloud {True,False}` 他のクラウドのポリシーも再割り当てする場合は、True に設定します。デフォルトは False です。
- `--map_file` 再割り当てマップファイルのファイル名を含むファイルパス (相対パスまたは絶対パス) を指定します。新しいテナントにマップされた古いポリシーのリストを提供します。このファイルの形式は YAML です。

説明付きのマッピングファイルの例を次に示します。

```
reassign_mappings:
- old_tenant_ids: [] #user can provide list of old_tenant_ids or
policy_ids
new_tenant_id: new_tenant_id
user_id: user_id
policy_ids: [] #user can provide list of old_tenant_ids or policy_ids
migrate_cloud: True/False #Set to True if want to reassign policies
 from
# other clouds as well. Default is False

- old_tenant_ids: [] #user can provide list of old_tenant_ids or
policy_ids
new_tenant_id: new_tenant_id
user_id: user_id
policy_ids: [] #user can provide list of old_tenant_ids or policy_ids
migrate_cloud: True/False #Set to True if want to reassign policies
 from
```

```
# other clouds as well. Default is False
```

ディザスタリカバリ

NetBackup for OpenStack ポリシーは、NetBackup for OpenStack データベースをバックアップせずにディザスタリカバリを実行できるように設計されています。

NetBackup for OpenStack ポリシーがバックアップターゲットストレージに存在し、NetBackup for OpenStack インストールがそれらへのアクセス権を持つ限り、ポリシーをリストアできます。

ディザスタリカバリプロセス

1. ターゲットクラウド用に NetBackup for OpenStack をインストールおよび構成します。

   p.30 の「NetBackup for OpenStack コンポーネントのインストール」を参照してください。

2. 必要なマウントパスを確認し、必要に応じて作成します。

   p.170 の「マウントパス」を参照してください。

3. ポリシーを再割り当てします。

   p.168 の「ポリシーの再割り当て」を参照してください。

4. 利用可能なポリシーをユーザーに通知します。

この手順は、NetBackup for OpenStack を使用してすべての OpenStack インストールに適用されるように設計されています。これは、特定の環境の正確なディザスタリカバリプロセスを開発するための開始点として使用されます。

ユーザーに通知するのではなく、リストアに必要な権限を持つ各プロジェクトにユーザーが含まれるように、ポリシーを必要に応じてリストアする必要があります。

マウントパス

NetBackup for OpenStack 増分スナップショットには、以前に取得されたバックアップのバッキングファイルが含まれるため、NetBackup for OpenStack 増分バックアップはすべて合成完全バックアップになります。

NetBackup for OpenStack は、この機能に qcow2 バッキングファイルを使用しています。

```
qemu-img info 85b645c5-c1ea-4628-b5d8-1faea0e9d549
image: 85b645c5-c1ea-4628-b5d8-1faea0e9d549
```

```
file format: qcow2
virtual size: 1.0G (1073741824 bytes)
disk size: 21M
cluster_size: 65536
backing file:
/var/NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW0=
/policy_3c2fbee5-ad90-4448-b009-5047bcffc2ea/snapshot_f4874ed7-fe85-
4d7d-b22b-082a2e068010/vm_id_9894f013-77dd-4514-8e65-818f4ae91d1f/
vm_res_id_9ae3a6e7-dffe-4424-badc-bc4de1a18b40_vda/a6289269-3e72-4085-
adca-e228ba656984
Format specific information:
    compat: 1.1
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
```

例に示すように、バッキングファイルは絶対パスであるため、バッキングファイルにアクセスできるようにするために、このパスが存在する必要があります。

NetBackup for OpenStack は、複数の NFS ボリュームを同時に構成できるように、NFS マウントパスに base64 ハッシュアルゴリズムを使用しています。ハッシュ値は、指定された NFS パスを使用して計算されます。

```
# echo -n 10.10.2.20:/upstream | base64
MTAuMTAuMi4yMDovdXBzdHJlYW0=
```

バッキングファイルのパスが NetBackup for OpenStack VM と計算ノードで利用できない場合、増分バックアップのリストアは失敗します。

バッキングファイルを利用可能にするための推奨されるテスト済みの方法は、必要なディレクトリパスを作成し、mount --bind を使用して、そのパスをバックアップに使用できるようにすることです。

```
#mount --bind <mount-path1> <mount-path2>
```

mount –bind コマンドを実行すると、次の再ブートまで必要なパスが利用可能になります。再ブート後にパスにアクセスする必要がある場合は、fstab を編集する必要があります。

```
#vi /etc/fstab
<mount-path1> <mount-path2> none bind   0 0
```

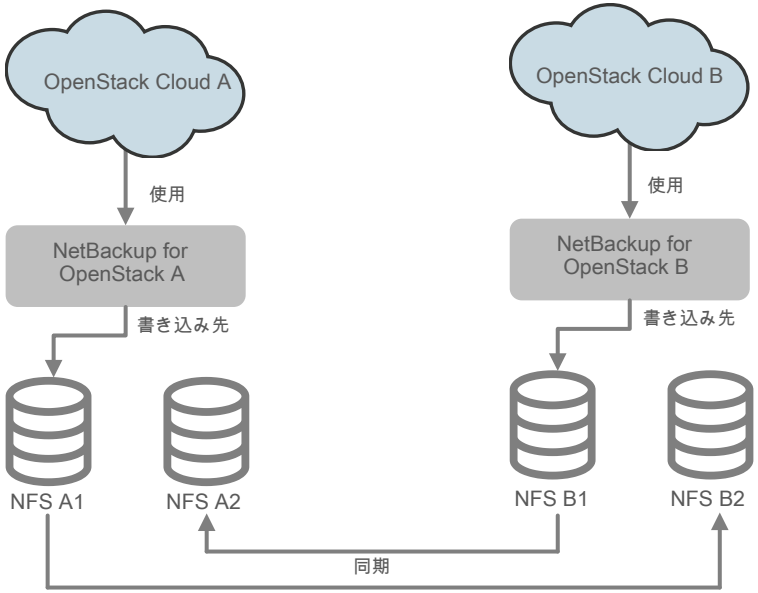
NFS を使用したディザスタリカバリのランブックの例

このランブックでは、特定のシナリオで NetBackup for OpenStack を使用したディザスタリカバリを設定する方法を示します。

シナリオ

OpenStack Cloud A と OpenStack Cloud B の 2 つの利用可能な OpenStack クラウドがあります。OpenStack Cloud B は、OpenStack Cloud A のディザスタリカバリリストアポイントです。その逆も同様です。どちらのクラウドにも独立した NetBackup for OpenStack インストールが統合されています。これらの NetBackup for OpenStack インストールは NFS ターゲットにバックアップを書き込みます。「NetBackup for OpenStack A」は「NFS A1」に書き込み、「NetBackup for OpenStack B」は「NFS B1」に書き込んでいます。使用されている NFS ボリュームは、もう一方の NFS ボリュームと同期されています。「NFS A1」は「NFS B2」と同期されていて、「NFS B1」は「NFS A2」と同期されています。同期プロセスは、NetBackup for OpenStack から独立して設定されており、常に新しいデータセットが優先されます。

図 7-2 ディザスタリカバリのシナリオ



ディザスタリカバリのシナリオ

このシナリオでは、単一のポリシーと完全なクラウドのディザスタリカバリについて説明します。すべてのプロセスは OpenStack 管理者として実行されます。

ディザスタリカバリプロセスの前提条件

このランブックでは、次のことが当てはまると想定しています。

- OpenStack Cloud A と OpenStack Cloud B の両方に有効なライセンスを持つアクティブな NetBackup for OpenStack インストールがあります
- OpenStack Cloud A と OpenStack Cloud B には、追加の VM をホストするための空きリソースがあります
- OpenStack Cloud A と OpenStack Cloud B で利用可能なテナントまたはプロジェクトは、もう一方のテナントまたはプロジェクトの指定されたリストアポイントです
- ドメインレベルで管理者役割の権限を持つユーザーにアクセス権を付与します
- OpenStack クラウドの 1 つが停止または消失しています

OpenStack Cloud A が停止しており、ポリシーが OpenStack Cloud B にリストアされると想定しています。

浮動 IP を超えて、共有テナントネットワークを使用する場合、次の追加要件があります。すべてのテナントネットワーク、ルーター、ポート、浮動 IP、DNS ゾーンが作成されています。

単一のポリシーのディザスタリカバリ

このシナリオでは、1 つのポリシーでディザスタリカバリを実行できますが、どちらのクラウドもアクティブな状態のままです。これを行うには、次に示すおおまかなプロセスに従う必要があります。

1. 構成済みの NFS ボリュームにポリシーディレクトリをコピーします。
2. 正しいマウントパスを利用可能にします。
3. ポリシーを再割り当てします。
4. ポリシーをリストアします。
5. クリーンアップします。

構成済みの NFS ボリュームへのポリシーディレクトリのコピー

メモ: このプロセスでは、OpenStack Cloud A から OpenStack Cloud B にポリシーを取得する方法のみを示します。その逆の処理も同様です。

単一のポリシーのみをリカバリするため、「NetBackup for OpenStack B」によって使用される NFS B1 ボリュームにその単一のポリシーのデータをコピーする方が効率的です。

NFS B2 ボリュームの NetBackup for OpenStack VM へのマウント

NetBackup for OpenStack VM で nova ユーザーが利用可能であるため、両方の NFS ボリューム間のコネクタとして NetBackup for OpenStack VM を使用することをお勧めします。

```
# mount <NFS B2-IP/NFS B2-FQDN>:/<VOL-Path> /mnt
```

NFS B2 ボリュームのポリシーの特定

NetBackup for OpenStack は ID によって識別され、バックアップターゲットに格納されます。次の例を参照してください。

```
policy_ac9cae9b-5e1b-4899-930c-6aa0600a2105
```

ポリシー ID が不明な場合は、ポリシーディレクトリ内のバックアップメタデータで利用可能です。

```
/…/policy_<id>/policy_db <<< Contains User ID and Project ID
of policy owner
/…/policy_<id>/policy_vms_db <<< Contains VM IDs and VM Names
of all VMs actively protected be the policy
```

ポリシーのコピー

特定されたポリシーは、すべてのサブディレクトリとファイルとともにコピーする必要があります。その後、適切な権限で nova:nova に所有権を調整する必要があります。

```
# cp /mnt/policy_ac9cae9b-5e1b-4899-930c-6aa0600a2105 /var/
NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW0=/
policy_ac9cae9b-5e1b-4899-930c-6aa0600a2105
# chown -R nova:nova /var/NetBackupOpenStack-mounts/
MTAuMTAuMi4yMDovdXBzdHJlYW0=/policy_ac9cae9b-5e1b-4899-
930c-6aa0600a2105
# chmod -R 644 /var/NetBackupOpenStack-mounts/
MTAuMTAuMi4yMDovdXBzdHJlYW0=/policy_ac9cae9b-5e1b-
4899-930c-6aa0600a2105
```

マウントパスを利用可能にする

NetBackup for OpenStack バックアップは qcow2 バッキングファイルを使用しており、増分バックアップはすべて完全合成バックアップになります。これらのバッキングファイルは、qemu-img ツールを使用して可視化することができます。

```
#qemu-img info bd57ec9b-c4ac-4a37-a4fd-5c9aa002c778
image: bd57ec9b-c4ac-4a37-a4fd-5c9aa002c778
file format: qcow2
virtual size: 1.0G (1073741824 bytes)
disk size: 516K
cluster_size: 65536

backing file:
/var/NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW0=
/policy_ac9cae9b-5e1b-4899-930c-6aa0600a2105/snapshot_1415095d-
c047-400b-8b05-c88e57011263/vm_id_38b620f1-24ae-41d7-b0ab-85ffc2
d7958b/vm_res_id_d4ab3431-5ce3-4a8f-a90b-07606e2ffa33_vda/7c39
eb6a-6e42-418e-8690-b6368ecaa7bb
Format specific information:
    compat: 1.1
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
```

バッキングファイルパスの `MTAuMTAuMi4yMDovdXBzdHJlYW0=` の部分は base64 ハッシュ値で、提供された各 NFS 共有の NetBackup for OpenStack インストールの構成によって計算されます。

このハッシュ値は、指定された NFS 共有パス (<NFS_IP>/<path>) に基づいて計算されます。指定された NFS 共有パス間で NFS 共有パスの 1 文字が異なる場合は、まったく異なるハッシュ値が生成されます。

NFS 共有間で移動したポリシーでは、増分バックアップが元のソースクラウドと同じパスをたどれる必要があります。そのためには、ターゲットクラウドのすべての計算ノードにマウントパスを作成する必要があります。

その後、マウントバインドを使用して、古いマウントパスと新しいマウントパスを介してポリシーデータにアクセスできます。次の例は、必要なマウントポイントを正常に識別し、マウントバインドを作成する方法のプロセスを示しています。

base64 ハッシュ値の特定

使用されるハッシュ値は、任意の Linux ディストリビューションの base64 ツールを使用して計算できます。

```
# echo -n 10.10.2.20:/NFS_A1 | base64
MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
```

```
# echo -n 10.20.3.22:/NFS_B2 | base64
MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0
```

パスの作成とバインド

特定された base64 ハッシュ値に基づいて、各計算ノードで次のパスが必要です。

```
/var/NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
```

および

```
/var/NetBackupOpenStack-mounts/MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0
```

シナリオでは、NFS Share_A1 のマウントパスを作成して、ターゲットクラウドにバインドする必要があります。

```
#mkdir /var/NetBackupOpenStack-mounts/
 MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
#mount --bind
/var/NetBackupOpenStack-mounts/MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0/

/var/NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
```

再起動後も目的のマウントを維持するには、それに応じてすべての計算ノードの fstab を編集することをお勧めします。

```
#vi /etc/fstab
/var/NetBackupOpenStack-mounts/MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0/

 /var/NetBackup for OpenStack-mounts/
MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
  none        bind        0 0
```

ポリシーの再割り当て

NetBackup for OpenStack ポリシーには明確な所有権が設定されています。ポリシーを別のクラウドに移動するときは、所有権を変更する必要があります。所有権は、OpenStack 管理者のみが変更できます。

必要なドメインとプロジェクトへの管理者ユーザーの追加

必要なタスクを完了するために、管理者の役割のユーザーが使用されます。このユーザーは、ポリシーがリストアされるまで使用されます。したがって、このユーザーにターゲットクラウド上の目的のターゲットプロジェクトへのアクセス権を付与する必要があります。

```
# source {customer admin rc file}
# OpenStack role add Admin --user <my_admin_user> --user-domain
<admin_domain> --domain <target_domain>
# OpenStack role add Admin --user <my_admin_user> --user-domain
<admin_domain> --project <target_project> --project-domain
<target_domain>
# OpenStack role add <Backup Trustee Role> --user <my_admin_user>
--user-domain <admin_domain> --project <destination_project>
--project-domain <target_domain>
```

ターゲットクラウドの NFS ストレージの孤立したポリシーの検出

各 NetBackup for OpenStack インストールでは、NetBackup for OpenStack インストールに認識されているポリシーのデータベースが保持されます。特定の NetBackup for OpenStack インストールによって管理されていないポリシーは、そのインストールの観点から、孤立したポリシーになります。孤立したポリシーは NFS 共有でアクセス可能なポリシーで、NetBackup for OpenStack インストールで保護しているクラウド内の既存のプロジェクトには割り当てられません。

```
# nbosjm policy-get-orphaned-policies-list --migrate_cloud True
```

ターゲットドメインのターゲットクラウドの利用可能なプロジェクトの一覧表示

特定された孤立したポリシーを新しいプロジェクトに割り当てる必要があります。次のコマンドは、target_domain で使用されている管理者ユーザーが表示できる利用可能なすべてのプロジェクトのリストを提供します。

```
# OpenStack project list --domain <target_domain>
```

ターゲットプロジェクトのターゲットクラウドで、適切なバックアップトラスティの役割を持つ利用可能なユーザーの一覧表示

プロジェクト所有者にポリシーの操作を許可し、ポリシーがバックアップトラスティの役割を持つユーザーに割り当てられていることを確認します。

```
# OpenStack role assignment list --project <target_project>
--project-domain <target_domain> --role <backup_trustee_role>
```

ターゲットプロジェクトへのポリシーの再割り当て

すべての情報が収集されたので、ポリシーをターゲットプロジェクトに再割り当てできます。

```
# nbosjm policy-reassign-policies --new_tenant_id
```

```
{target_project_id} --user_id {target_user_id} --policy_ids
{policy-id} --migrate_cloud True
```

目的の target_project でポリシーが利用可能であることの確認

ポリシーが新しいプロジェクトに割り当てられた後、ポリシーがターゲット NetBackup for OpenStack によって管理され、適切なプロジェクトとユーザーに割り当てられていることを確認することをお勧めします。

```
# nbosjm policy-show ac9cae9b-5e1b-4899-930c-6aa0600a2105
```

ポリシーのリストア

再割り当てされたポリシーは、選択的リストアの手順に従って Horizon を使用してリストアできます。p.127 の「選択的リストア」を参照してください。

このランブックは CLI のみのパスで続行されます。

スナップショット情報取得による選択的リストアの準備

必要な選択的リストアを実行できるようにするには、リストアするスナップショットに関するいくつかの情報が必要です。次のプロセスによって、必要なすべての情報が提供されます。

リストアするポリシーのすべてのスナップショットを一覧表示して、リストアするスナップショットを識別します

```
# nbosjm snapshot-list --policy-id ac9cae9b-5e1b-4899-930c-
6aa0600a2105 --all True
```

目的のスナップショットのネットワークの詳細を使用してスナップショットの詳細を取得します

```
# nbosjm snapshot-show --output networks 7e39e544-537d-4417-853d-
11463e7396f9
```

目的のスナップショットのディスクの詳細を使用してスナップショットの詳細を取得します。

```
[root@upstreamcontroller ~(keystone_admin)]# nbosjm snapshot-show
--output disks 7e39e544-537d-4417-853d-11463e7396f9
```

restore.json ファイル作成による選択的リストアの準備

選択的リストアでは、CLI コマンドに restore.json ファイルを使用します。この restore.json ファイルは、目的のリストアに従って調整する必要があります。

```
{
   u'description':u'<description of the restore>',
   u'oneclickrestore':False,
   u'restore_type':u'selective',
   u'type':u'OpenStack',
   u'name':u'<name of the restore>'
   u'OpenStack':{
      u'instances':[
         {
            u'name':u'<name instance 1>',
            u'availability_zone':u'<AZ instance 1>',
            u'nics':[ #####Leave empty for network topology restore
            ],
            u'vdisks':[
               {
                  u'id':u'<old disk id>',
                  u'new_volume_type':u'<new volume type name>',
                  u'availability_zone':u'<new cinder volume AZ>'
               }
            ],
            u'flavor':{
               u'ram':<RAM in MB>,
               u'ephemeral':<GB of ephemeral disk>,
               u'vcpus':<# vCPUs>,
               u'swap':u'<GB of Swap disk>',
               u'disk':<GB of boot disk>,
               u'id':u'<id of the flavor to use>'
            },
            u'include':<True/False>,
            u'id':u'<old id of the instance>'
         } #####Repeat for each instance in the snapshot
      ],
      u'restore_topology':<True/False>,
      u'networks_mapping':{
         u'networks':[ #####Leave empty for network topology restore


         ]
      }
   }
}
```

選択的リストアの実行

実際のリストアを行うには、次のコマンドを使用します。

```
# nbosjm snapshot-selective-restore --filename restore.json
{snapshot id}
```

リストアの検証

NetBackup for OpenStack の観点からリストアが成功したことを検証するには、リストアの状態を確認します。

```
[root@upstreamcontroller ~(keystone_admin)]# nbosjm restore-list
--snapshot_id 5928554d-a882-4881-9a5c-90e834c071af
```

クリーンアップ

ディザスタリカバリプロセスが正常に完了したら、nbosvm インストールを元の状態に戻して、次の DR プロセスの準備を整えておくことをお勧めします。

ポリシーの削除

リストアされたポリシーを削除します。

```
# nbosjm policy-delete <policy-id>
```

データベースエントリの削除

NetBackup for OpenStack データベースは、クラウドオブジェクトの削除時にデータベースエントリを削除しないという OpenStack 標準に従っています。削除されたポリシー (スナップショットまたはリストア) は、削除済みとしてマークされるのみです。

NetBackup for OpenStack インストールで別のディザスタリカバリを準備できるようにするには、リストアされたポリシーのエントリを完全に削除する必要があります。

NetBackup for OpenStack は、ポリシーエントリとすべての接続済みエンティティを NetBackup for OpenStack データベースから安全に削除するためのスクリプトを提供および保守します。

プロジェクトからの管理者ユーザーの削除

ターゲットプロジェクトのすべてのリストアが完了したら、使用した管理者ユーザーをプロジェクトから再度削除することをお勧めします。

```
# source {customer admin rc file}
# OpenStack role remove Admin --user <my_admin_user> --user-domain
<admin_domain> --domain <target_domain>
```

```
# OpenStack role remove Admin --user <my_admin_user> --user-domain
<admin_domain> --project <target_project> --project-domain
<target_domain>
# OpenStack role remove <Backup Trustee Role> --user <my_admin_user>

--user-domain <admin_domain> --project <destination_project>
--project-domain <target_domain>
```

クラウド全体のディザスタリカバリ

このシナリオでは、クラウド全体のディザスタリカバリについて説明します。ここでは、ソースクラウドが停止しているか、完全に失われていると想定されます。ディザスタリカバリを行うには、次に示すおおまかなプロセスに従う必要があります。

1. ターゲット NetBackup for OpenStack インストールを再構成します。
2. 正しいマウントパスを利用可能にします。
3. ポリシーを再割り当てします。
4. ポリシーをリストアします。
5. ターゲット NetBackup for OpenStack インストールを元のインストールに再構成します。
6. クリーンアップします。

ターゲット NetBackup for OpenStack インストールの再構成

ディザスタリカバリプロセスを開始する前に、リストアするバックアップを NetBackup for OpenStack インストールで利用できるようにする必要があります。NetBackup for OpenStack インストールを完全に再構成するには、次の手順を実行する必要があります。

再構成プロセス中、ターゲット領域のすべてのバックアップは保留状態になり、ディザスタリカバリプロセスが完了して元の NetBackup for OpenStack 構成がリストアされるまで、新しいバックアップジョブを作成することはお勧めしません。

NetBackup for OpenStack Appliance クラスタへの NFS B2 の追加

NetBackup for OpenStack Appliance クラスタに NFS-B2 を追加するには、NetBackup for OpenStack を両方の NFS ボリュームを使用するように完全に再構成するか、構成ファイルを編集してすべてのサービスを再起動できます。この手順では、conf ファイルを編集してサービスを再起動する方法について説明します。これはすべての NetBackup for OpenStack Appliance で繰り返す必要があります。

p.62 の「NetBackup for OpenStack の構成」を参照してください。

nbosjm.conf を編集します

```
# vi /etc/nbosjm/nbosjm.conf
```

NFS マウントを定義する行を検索します

```
vault_storage_nfs_export = <NFS_B1/NFS_B1-FQDN>:/<VOL-B1-Path>
```

NFS B2 をカンマ区切りリストとして追加します。スペースは必要ありませんが、設定できます。

```
vault_storage_nfs_export = <NFS-IP/NFS-FQDN>:/<VOL-1-Path>,
<NFS-IP/NFS-FQDN>:/<VOL–2-Path>
```

nbosjm.conf に書き込んで閉じます

nbosjm-policies サービスを再起動します

```
# systemctl restart nbosjm-policies
```

NetBackup for OpenStack Datamover への NFS B2 の追加

NetBackup for OpenStack は、OpenStack 配備ツールにネイティブに統合します。Red Hat Director を使用する場合は、これらのオーケストレータの環境ファイルを適用し、それらを介して Datamover を更新することをお勧めします。

NFS B2 を NetBackup for OpenStack Datamover に手動で追加するには、nbosdm.conf ファイルを編集してサービスを再起動する必要があります。

nbosdm.conf を編集します。

```
# vi /etc/nbosdm/nbosdm.conf
```

NFS マウントを定義する行を検索します。

```
vault_storage_nfs_export = <NFS_B1-IP/NFS_B1-FQDN>:/<VOL-B1-Path>
```

NFS B2 をカンマ区切りリストとして追加します。スペースは必要ありませんが、設定できます。

```
vault_storage_nfs_export = <NFS_B1-IP/NFS-FQDN>:/<VOL-B1-Path>,
<NFS_B2-IP/NFS-FQDN>:/<VOL–B2-Path>
```

nbosdm.conf に書き込んで閉じます

nbosdm サービスを再起動します。

```
# systemctl restart nbosdm
```

マウントパスを利用可能にする

NetBackup for OpenStack バックアップは qcow2 バッキングファイルを使用しており、増分バックアップはすべて完全合成バックアップになります。これらのバッキングファイルは、qemu-img ツールを使用して可視化することができます。

```
#qemu-img info bd57ec9b-c4ac-4a37-a4fd-5c9aa002c778
image: bd57ec9b-c4ac-4a37-a4fd-5c9aa002c778
file format: qcow2
virtual size: 1.0G (1073741824 bytes)
disk size: 516K
cluster_size: 65536

backing file:
/var/NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW0=
/policy_ac9cae9b-5e1b-4899-930c-6aa0600a2105/snapshot_1415095d
-c047-400b-8b05-c88e57011263/vm_id_38b620f1-24ae-41d7-b0ab-85ffc
2d7958b/vm_res_id_d4ab3431-5ce3-4a8f-a90b-07606e2ffa33_vda/7c39eb
6a-6e42-418e-8690-b6368ecaa7bb
Format specific information:
    compat: 1.1
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
```

バッキングファイルパスの `MTAuMTAuMi4yMDovdXBzdHJlYW0=` の部分は base64 ハッシュ値で、提供された各 NFS 共有の NetBackup for OpenStack インストールの構成によって計算されます。

このハッシュ値は、指定された NFS 共有パス (<NFS_IP>/<path>) に基づいて計算されます。指定された NFS 共有パス間で NFS 共有パスの 1 文字が異なる場合は、まったく異なるハッシュ値が生成されます。

NFS 共有間で移動したポリシーでは、増分バックアップが元のソースクラウドと同じパスをたどれる必要があります。そのためには、ターゲットクラウドのすべての計算ノードにマウントパスを作成する必要があります。

その後、マウントバインドを使用して、古いマウントパスと新しいマウントパスを介してポリシーデータにアクセスできます。次の例は、必要なマウントポイントを正常に識別し、マウントバインドを作成する方法のプロセスを示しています。

base64 ハッシュ値の特定

使用されるハッシュ値は、任意の Linux ディストリビューションの base64 ツールを使用して計算できます。

```
# echo -n 10.10.2.20:/NFS_A1 | base64
MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl

# echo -n 10.20.3.22:/NFS_B2 | base64
MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0
```

パスの作成とバインド

特定された base64 ハッシュ値に基づいて、各計算ノードで次のパスが必要です。

```
/var/NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
```

および

```
/var/NetBackupOpenStack-mounts/MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0
```

シナリオでは、NFS Share_A1 のマウントパスを作成して、ターゲットクラウドにバインドする必要があります。

```
#mkdir
/var/NetBackupOpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
#mount --bind
/var/NetBackupOpenStack-mounts/MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0/

/var/NetBackup for
OpenStack-mounts/MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
```

再起動後も目的のマウントを維持するには、それに応じてすべての計算ノードの fstab を編集することをお勧めします。

```
#vi /etc/fstab
/var/NetBackupOpenStack-mounts/MTAuMjAuMy4yMjovdXBzdHJlYW1fdGFyZ2V0/

/ var/NetBackup for OpenStack-mounts/
MTAuMTAuMi4yMDovdXBzdHJlYW1fc291cmNl
none        bind        0 0
```

ポリシーの再割り当て

NetBackup for OpenStack ポリシーには明確な所有権が設定されています。ポリシーを別のクラウドに移動するときは、所有権を変更する必要があります。所有権は、OpenStack 管理者のみが変更できます。

必要なドメインとプロジェクトへの管理者ユーザーの追加

必要なタスクを完了するために、管理者の役割のユーザーが使用されます。このユーザーは、ポリシーがリストアされるまで使用されます。したがって、このユーザーにターゲットクラウド上の目的のターゲットプロジェクトへのアクセス権を付与する必要があります。

```
# source {customer admin rc file}
# OpenStack role add Admin --user <my_admin_user> --user-domain
<admin_domain> --domain <target_domain>
# OpenStack role add Admin --user <my_admin_user> --user-domain
<admin_domain> --project <target_project> --project-domain
<target_domain>
# OpenStack role add <Backup Trustee Role> --user <my_admin_user>
--user-domain <admin_domain> --project <destination_project>
--project-domain <target_domain>
```

ターゲットクラウドの NFS ストレージの孤立したポリシーの検出

各 NetBackup for OpenStack インストールでは、NetBackup for OpenStack インストールに認識されているポリシーのデータベースが保持されます。特定の NetBackup for OpenStack インストールによって管理されていないポリシーは、そのインストールの観点から、孤立したポリシーになります。孤立したポリシーは NFS 共有でアクセス可能なポリシーで、NetBackup for OpenStack インストールで保護しているクラウド内の既存のプロジェクトには割り当てられません。

```
# nbosjm policy-get-orphaned-policies-list --migrate_cloud True
```

ターゲットドメインのターゲットクラウドの利用可能なプロジェクトの一覧表示

特定された孤立したポリシーを新しいプロジェクトに割り当てる必要があります。次のコマンドは、target_domain で使用されている管理者ユーザーが表示できる利用可能なすべてのプロジェクトのリストを提供します。

```
# OpenStack project list --domain <target_domain>
```

ターゲットプロジェクトのターゲットクラウドで、適切なバックアップトラスティの役割を持つ利用可能なユーザーの一覧表示

プロジェクト所有者にポリシーの操作を許可し、ポリシーがバックアップトラスティの役割を持つユーザーに割り当てられていることを確認します。

```
# OpenStack role assignment list --project <target_project>
--project-domain <target_domain> --role <backup_trustee_role>
```

ターゲットプロジェクトへのポリシーの再割り当て

すべての情報が収集されたので、ポリシーをターゲットプロジェクトに再割り当てできます。

```
# nbosjm policy-reassign-policies --new_tenant_id
{target_project_id} --user_id {target_user_id} --policy_ids
{policy-id} --migrate_cloud True
```

目的の target_project でポリシーが利用可能であることの確認

ポリシーが新しいプロジェクトに割り当てられた後、ポリシーがターゲット NetBackup for OpenStack によって管理され、適切なプロジェクトとユーザーに割り当てられていることを確認することをお勧めします。

```
# nbosjm policy-show ac9cae9b-5e1b-4899-930c-6aa0600a2105
```

ポリシーのリストア

再割り当てされたポリシーは、選択的リストアの手順に従って Horizon を使用してリストアできます。

p.127 の「選択的リストア」を参照してください。

このランブックは CLI のみのパスで続行されます。

スナップショット情報取得による選択的リストアの準備

必要な選択的リストアを実行できるようにするには、リストアするスナップショットに関するいくつかの情報が必要です。次のプロセスによって、必要なすべての情報が提供されます。

リストアするポリシーのすべてのスナップショットを一覧表示して、リストアするスナップショットを識別します。

```
# nbosjm snapshot-list --policy-id ac9cae9b-5e1b-4899-930c-
6aa0600a2105 --all True
```

目的のスナップショットのネットワークの詳細を使用してスナップショットの詳細を取得します。

```
# nbosjm snapshot-show --output networks 7e39e544-537d-4417-
853d-11463e7396f9
```

目的のスナップショットのディスクの詳細を使用してスナップショットの詳細を取得します。

```
[root@upstreamcontroller ~(keystone_admin)]# nbosjm snapshot-show
--output disks 7e39e544-537d-4417-853d-11463e7396f9
```

restore.json ファイル作成による選択的リストアの準備

選択的リストアでは、CLI コマンドに restore.json ファイルを使用します。この restore.json ファイルは、目的のリストアに従って調整する必要があります。

```
{
   u'description':u'<description of the restore>',
   u'oneclickrestore':False,
   u'restore_type':u'selective',
   u'type':u'OpenStack',
   u'name':u'<name of the restore>'
   u'OpenStack':{
      u'instances':[
         {
            u'name':u'<name instance 1>',
            u'availability_zone':u'<AZ instance 1>',
            u'nics':[ #####Leave empty for network topology restore
            ],
            u'vdisks':[
               {
                  u'id':u'<old disk id>',
                  u'new_volume_type':u'<new volume type name>',
                  u'availability_zone':u'<new cinder volume AZ>'
               }
            ],
            u'flavor':{
               u'ram':<RAM in MB>,
               u'ephemeral':<GB of ephemeral disk>,
               u'vcpus':<# vCPUs>,
               u'swap':u'<GB of Swap disk>',
               u'disk':<GB of boot disk>,
               u'id':u'<id of the flavor to use>'
            },
            u'include':<True/False>,
            u'id':u'<old id of the instance>'
         } #####Repeat for each instance in the snapshot
      ],
      u'restore_topology':<True/False>,
      u'networks_mapping':{
```

```
        u'networks':[ #####Leave empty for network topology restore


         ]
      }
   }
}
```

選択的リストアの実行

実際のリストアを行うには、次のコマンドを使用します。

```
# nbosjm snapshot-selective-restore --filename restore.json
{snapshot id}
```

リストアの検証

NetBackup for OpenStack の観点からリストアが成功したことを検証するには、リストアの状態を確認します。

```
[root@upstreamcontroller ~(keystone_admin)]# nbosjm restore-list
--snapshot_id 5928554d-a882-4881-9a5c-90e834c071af

[root@upstreamcontroller ~(keystone_admin)]# nbosjm restore-show
5b4216d0-4bed-460f-8501-1589e7b45e01
```

ターゲット NetBackup for OpenStack インストールの元の状態への再構成

ディザスタリカバリプロセスが完了したら、NetBackup for OpenStack インストールを元の構成に戻す必要があります。NetBackup for OpenStack インストールを完全に再構成するには、次の手順を実行する必要があります。

再構成プロセス中、ターゲット領域のすべてのバックアップは保留状態になり、ディザスタリカバリプロセスが完了して元の NetBackup for OpenStack 構成がリストアされるまで、新しいバックアップジョブを作成することはお勧めしません。

NetBackup for OpenStack Appliance クラスタからの NFS B2 の削除

NetBackup for OpenStack Appliance クラスタで NFS-B2 を削除するには、NetBackup for OpenStack を両方の NFS ボリュームを使用するように完全に再構成するか、構成ファイルを編集してすべてのサービスを再起動できます。この手順では、conf ファイルを編集してサービスを再起動する方法について説明します。これはすべての NetBackup for OpenStack Appliance で繰り返す必要があります。

p.62 の「NetBackup for OpenStack の構成」を参照してください。

nbosjm.conf を編集します。

```
# vi /etc/nbosjm/nbosjm.conf
```

NFS マウントを定義する行を検索します。

```
vault_storage_nfs_export = <NFS_B1-IP/NFS-FQDN>:/<VOL-B1-Path>,
<NFS_B2-IP/NFS-FQDN>:/<VOL-B2-Path>
```

カンマ区切りのリストから NFS B2 を削除します。

```
vault_storage_nfs_export = <NFS_B1-IP/NFS_B1-FQDN>:/<VOL-B1-Path>
```

nbosjm.conf に書き込んで閉じます。

nbosjm-policies サービスを再起動します。

```
# systemctl restart nbosjm-policies
```

NetBackup for OpenStack Datamover からの NFS B2 の削除

警告: NetBackup for OpenStack は、OpenStack 配備ツールにネイティブに統合しています。Red Hat Director を使用する場合は、これらのオーケストレータの環境ファイルを適用し、それらを介して Datamover を更新することをお勧めします。

NFS B2 を NetBackup for OpenStack Datamover から手動で削除するには、nbosdm.conf ファイルを編集してサービスを再起動する必要があります。

nbosdm.conf を編集します。

```
# vi /etc/nbosdm/nbosdm.conf
```

NFS マウントを定義する行を検索します。

```
vault_storage_nfs_export = <NFS_B1-IP/NFS-FQDN>:/<VOL-B1-Path>,
<NFS_B2-IP/NFS-FQDN>:/<VOL-B2-Path>
```

カンマ区切りのリストから NFS B2 を削除します。

```
vault_storage_nfs_export = <NFS-IP/NFS-FQDN>:/<VOL-1-Path>
```

nbosdm.conf に書き込んで閉じます。

nbosdm サービスを再起動します。

```
# systemctl restart nbosdm
```

クリーンアップ

ディザスタリカバリプロセスが正常に完了し、再構成した NetBackup for OpenStack インストールを元の状態に戻したら、次のディザスタリカバリプロセスに備えて次の追加手順を実行することをお勧めします。

データベースエントリの削除

NetBackup for OpenStack データベースは、クラウドオブジェクトの削除時にデータベースエントリを削除しないという OpenStack 標準に従っています。削除されたポリシー (スナップショットまたはリストア) は、削除済みとしてマークされるのみです。

NetBackup for OpenStack インストールで別のディザスタリカバリを準備できるようにするには、リストアされたポリシーのエントリを完全に削除する必要があります。

NetBackup for OpenStack は、ポリシーエントリとすべての接続済みエンティティを NetBackup for OpenStack データベースから安全に削除するためのスクリプトを提供および保守します。

プロジェクトからの管理者ユーザーの削除

ターゲットプロジェクトのすべてのリストアが完了したら、使用した管理者ユーザーをプロジェクトから再度削除することをお勧めします。

```
# source {customer admin rc file}
# OpenStack role remove Admin --user <my_admin_user> --user-domain
<admin_domain> --domain <target_domain>
# OpenStack role remove Admin --user <my_admin_user> --user-domain
<admin_domain> --project <target_project> --project-domain
<target_domain>
# OpenStack role remove <Backup Trustee Role> --user <my_admin_user>

--user-domain <admin_domain> --project <destination_project>
--project-domain <target_domain>
```

8

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。

一般的なトラブルシューティングのヒント

OpenStack のような複雑な環境でのトラブルシューティングは非常に時間がかかる場合があります。次のヒントは、根本原因を特定するためのトラブルシューティングプロセスを迅速化するのに役立ちます。

問題の場所と詳細

OpenStack と NetBackup for OpenStack は複数のサービスに分割されます。各サービスは、バックアップまたはリカバリ手順中に呼び出され、それぞれに固有の目的があります。サービスの機能を知ることで、エラーがどこにあるかを理解し、より焦点を絞ったトラブルシューティングを行えます。

NetBackup for OpenStack クラスタ

NetBackup for OpenStack クラスタは、NetBackup for OpenStack のコントローラです。ユーザーからポリシー関連のすべての要求を受信します。

バックアップまたはリストアプロセスの各タスクがトリガされ、ここから管理されます。これには、バックアップターゲットでのディレクトリ構造と初期メタデータファイルの作成が含まれます。

バックアップ処理中

バックアップ処理中に、NetBackup for OpenStack クラスタは OpenStack 環境からバックアップされた VM とネットワークに関するメタデータを収集する役割も担います。構成されたエンドポイントタイプの OpenStack エンドポイントに向けて API コールを送信して、この情報をフェッチします。メタデータを受信すると、NetBackup for OpenStack クラスタはバックアップターゲットに JSON ファイルとして書き込みます。

NetBackup for OpenStack クラスタは Cinder Snapshot コマンドも送信します。

リストア処理中

リストア処理中に、NetBackup for OpenStack クラスタはデータベースから VM メタデータを読み込み、そのメタデータを使用してリストアのシェルを作成します。必要なリソースを作成するために、OpenStack 環境に API 呼び出しを送信します。

nbosdmapi

nbosdmapi サービスは、計算ノードで実行されている NetBackup for OpenStack クラスタとデータムーバー間のコネクタです。

nbosdmapi サービスの目的は、現在のバックアップまたはリストアタスクを担当する計算ノードを識別することです。これを行うために、nbosdmapi サービスは、提供された VM の計算ホストを要求する nova api データベースに接続します。

計算ホストが識別されると、nbosdmapi は NetBackup for OpenStack クラスタから識別された計算ホストで実行されているデータムーバーにコマンドを転送します。

nbosdm

nbosdm は、計算ノードで実行される NetBackup for OpenStack サービスです。

各データムーバーは、計算ノード上で実行されている VM を担当します。データムーバーは、異なる計算ノードで実行されている VM と連携して動作できません。

データムーバーは、VM の凍結と解凍、およびデータの実際の移動を制御します。

バックアップターゲットではすべてがユーザー nova として実行される

NetBackup for OpenStack は、バックアップターゲットで nova:nova として読み取りと書き込みを実行します。

nova:nova の POSIX ユーザー ID とグループ ID は、NetBackup for OpenStack クラスタとすべての計算ノード間で揃える必要があります。これを行わないと、バックアップまたはリストアが、権限の問題やファイルが見つからない問題で失敗する可能性があります。

バックアップターゲット上の必要なすべてのノードに nova:nova として書き込みと読み取りを完全に実行できるかぎり、別の方法でこの目標を達成することが可能です。

データ転送フェーズでエラーが発生した場合、またはファイル権限エラーが発生した場合は、バックアップターゲットで必要な権限を確認することをお勧めします。

NetBackup for OpenStack トラスティの役割

NetBackup for OpenStack は RBAC を使用して、ユーザーに NetBackup for OpenStack 機能の使用を許可します。

このトラスティの役割は必須で、管理者ロールを使用して上書きすることはできません。

ポリシー、バックアップ、またはリストアの作成時に NetBackup for OpenStack でアクセス権のエラーが発生した場合は、NetBackup for OpenStack トラスティの役割の割り当てを確認することをお勧めします。

OpenStack クォータ

Cinder ボリュームを保護するために、NetBackup for OpenStack は、Cinder スナップショットと追加の一時 Cinder ボリュームを作成します。テナント管理者は、適切なスナップショットと完全バックアップと増分バックアップに必要なボリュームをプロビジョニングするために、OpenStack クォータを構成する必要があります。一時ボリュームは、ディスクごとにディスクマップ情報を生成し、増分的に変更されたデータを計算するために使用されます。

ボリュームクォータ要件は、1 つ以上のポリシーを使用して同時にバックアップされるディスクの合計数に基づいています。同時バックアップの数が増加すると、より多くのボリュームクォータが必要になります。テナント管理者は、インスタンスの合計数とそれらのインスタンスに接続されたディスクの合計数を計算して、ボリュームクォータを判断できます。たとえば、10 個のインスタンスを保護し、各インスタンスに 2 つのディスクを接続するとします。1 つ以上のポリシーを使用してこれらのインスタンスを同時に保護する場合、必要なボリュームクォータは 30 です。

エフェメラルディスクバックアップ

エフェメラルストレージは、特定の計算インスタンスにのみ関連付けられた非永続的なストレージ形式です。インスタンスに割り当てられているエフェメラルディスクは、インスタンスが終了すると削除されます。エフェメラルディスクは、一時データの保存に使用するのが理想的です。

NetBackup for OpenStack は、VM インスタンスに割り当てられているエフェメラルディスクを保護しません。

NetBackup for OpenStack Appliance での nbosjm CLI ツールの使用

NetBackup for OpenStack Appliance で nbosjm CLI ツールを使用するには、nbosjm の仮想環境のアクティブ化のみが必要です。

```
source /home/stack/myansible/bin/activate
```

OpenStack に対して認証するための rc ファイルが必要です。

NetBackup for OpenStack の健全性チェック

NetBackup for OpenStack は複数のサービスで構成され、エラーが発生した場合にこれらを確認できます。

NetBackup for OpenStack クラスタ上

nbosjm-policies

このサービスは、すべての NetBackup for OpenStack ノードで実行され、アクティブになります。

```
[root@Upstream ~]# systemctl status nbosjm-policies
● nbosjm-policies.service - nbosjm policies service
   Loaded: loaded (/etc/systemd/system/nbosjm-policies.service;
enabled;
   vendor preset: disabled)
   Active: active (running) since Wed 2020-06-10 13:42:42 UTC; 1
weeks
   4 days ago
```

```
 Main PID: 12779 (nbosjm-wor)
    Tasks: 17
   CGroup: /system.slice/nbosjm-policies.service
           ├─12779 /home/stack/myansible/bin/python
/home/stack/myansible/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           ├─12982 /home/stack/myansible/bin/python
/home/stack/myansible/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           ├─12983 /home/stack/myansible/bin/python
/home/stack/myansible/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           ├─12984 /home/stack/myansible/bin/python
/home/stack/myansible/bin/nbosjm-policies
--config-file=/etc/nbosjm/nbosjm.conf
           [...]
```

nbosjm-api

このサービスは、すべての NetBackup for OpenStack ノードで実行され、アクティブになります。

```
[root@Upstream ~]# systemctl status nbosjm-api
● nbosjm-api.service - nbosjm api service
   Loaded: loaded (/etc/systemd/system/nbosjm-api.service; disabled;

   vendor preset: disabled)
  Drop-In: /run/systemd/system/nbosjm-api.service.d
           └─50-pacemaker.conf
   Active: active (running) since Thu 2020-04-16 22:30:11 UTC;
   2 months 5 days ago
 Main PID: 11815 (nbosjm-api)
    Tasks: 1
   CGroup: /system.slice/nbosjm-api.service
           └─11815 /home/stack/myansible/bin/python /home/stack/
           myansible/bin/nbosjm-api --config-file=/etc/
           nbosjm/nbosjm.conf
```

nbosjm-scheduler

このサービスは、すべての NetBackup for OpenStack ノードで実行され、アクティブになります。

```
[root@Upstream ~]# systemctl status nbosjm-scheduler
● nbosjm-scheduler.service - nbosjm scheduler service
   Loaded: loaded (/etc/systemd/system/nbosjm-scheduler.service;
disabled;
   vendor preset: disabled)
  Drop-In: /run/systemd/system/nbosjm-scheduler.service.d
           └─50-pacemaker.conf
   Active: active (running) since Thu 2020-04-02 13:49:22 UTC; 2
months
   20 days ago
 Main PID: 29439 (nbosjm-sch)
    Tasks: 1
   CGroup: /system.slice/nbosjm-scheduler.service
           └─29439 /home/stack/myansible/bin/python
/home/stack/myansible
           /bin/nbosjm-scheduler --config-file=/etc/nbosjm/
           nbosjm.conf
```

nbosjm-cron

このサービスはペースメーカーによって制御され、マスターノードでのみ実行されます

```
[root@Upstream ~]# systemctl status nbosjm-cron
● nbosjm-cron.service - Cluster Controlled nbosjm-cron
   Loaded: loaded (/etc/systemd/system/nbosjm-cron.service; disabled;

   vendor preset: disabled)
  Drop-In: /run/systemd/system/nbosjm-cron.service.d
           └─50-pacemaker.conf
   Active: active (running) since Wed 2021-01-27 19:59:26 UTC; 6 days
 ago
 Main PID: 23071 (nbosjm-cro)
   CGroup: /system.slice/nbosjm-cron.service
           ├─23071 /home/stack/myansible/bin/python3 /home/stack/
myansible/bin/nbosjm-cron --config-file=/etc/nbosjm
/nbosjm.conf
           └─23248 /home/stack/myansible/bin/python3 /home/stack/
myansible/bin/nbosjm-cron --config-file=/etc/nbosjm/
nbosjm.conf

Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: ● nbosjm-cron.service - Cluster Controlled nbosjm-cron
```

```
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: Loaded: loaded (/etc/systemd/system/nbosjm-cron.service;
disabled;
vendor preset: disabled)
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: Drop-In: /run/systemd/system/nbosjm-cron.service.d
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: └─50-pacemaker.conf
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: Active: active (running) since Wed 2021-01-27 19:59:26 UTC;

6 days ago
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: Main PID: 23071 (nbosjm-cro)
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: CGroup: /system.slice/nbosjm-cron.service
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: ├─23071 /home/stack/myansible/bin/python3
/home/stack/myansible/
bin/nbosjm-cron --config-file=/etc/nbosjm/nbosjm.conf
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: ├─23248 /home/stack/myansible/bin/python3
/home/stack/myansible/
bin/nbosjm-cron --config-file=/etc/nbosjm/nbosjm.conf
Feb 03 19:28:43 nbosvm1-ansible-ussuri-ubuntu18-vagrant nbosjm-cron
[23071]: └─27145 /usr/bin/systemctl status nbosjm-cron
```

ペースメーカークラスタの状態

ペースメーカークラスタは、NetBackup for OpenStack クラスタ上の VIP を制御し、監視します。また、nbosjm-api と nbosjm-scheduler サービスを実行するノードも制御します。

```
[root@Upstream ~]# pcs status
Cluster name: NetBackup for OpenStack

WARNINGS:
Corosync and pacemaker node names do not match (IPs used in setup?)

Stack: corosync
Current DC: nbosvm1-ansible-ussuri-ubuntu18-vagrant (version
1.1.23-1.el7_9.1-9acf116022) - chapterition with quorum
Last updated: Wed Feb  3 19:20:02 2021
Last change: Wed Jan 27 20:00:12 2021 by root via crm_resource on
```

```
nbosvm1-ansible-ussuri-ubuntu18-vagrant

1 node configured
6 resource instances configured

Online: [ nbosvm1-ansible-ussuri-ubuntu18-vagrant ]

Full list of resources:

 virtual_ip     (ocf::heartbeat:IPaddr2):       Started
nbosvm1-ansible-
ussuri-ubuntu18-vagrant
 virtual_ip_public      (ocf::heartbeat:IPaddr2):       Started
nbosvm1-
ansible-ussuri-ubuntu18-vagrant
 virtual_ip_admin       (ocf::heartbeat:IPaddr2):       Started
nbosvm1-
ansible-ussuri-ubuntu18-vagrant
 virtual_ip_internal    (ocf::heartbeat:IPaddr2):       Started
nbosvm1-
ansible-ussuri-ubuntu18-vagrant
 nbosjm-cron      (systemd:nbosjm-cron):    Started nbosvm1-ansible-
ussuri-ubuntu18-vagrant
 Clone Set: lb_nginx-clone [lb_nginx]
     Started: [ nbosvm1-ansible-ussuri-ubuntu18-vagrant ]

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

マウントの可用性

NetBackup for OpenStack クラスタはバックアップターゲットにアクセスする必要があり、常に正しいマウントを行う必要があります。

```
[root@Upstream ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
devtmpfs                3.8G     0  3.8G   0% /dev
tmpfs                   3.8G   38M  3.8G   1% /dev/shm
tmpfs                   3.8G  427M  3.4G  12% /run
tmpfs                   3.8G     0  3.8G   0% /sys/fs/cgroup
/dev/vda1                40G  8.8G   32G  22% /
```

```
tmpfs                    773M     0  773M   0% /run/user/996
tmpfs                    773M     0  773M   0% /run/user/0
10.10.2.20:/upstream  1008G  704G  254G  74%
/var/NetBackupOpenStack-mounts/

MTAuMTAuMi4yMDovdXBzdHJlYW0=
10.10.2.20:/upstream2  483G   22G  462G   5%
/var/NetBackupOpenStack-mounts/

MTAuMTAuMi4yMDovdXBzdHJlYW0y
```

nbosdmapi サービス

nbosdmapi サービスには独自の Keystone エンドポイントがあり、実際のサービス状態に加えてこれを確認する必要があります。

```
[root@upstreamcontroller ~(keystone_admin)]# openstack endpoint list
 |
grep nbosdmapi
| 47918c8df8854ed49c082e398a9572be | RegionOne | nbosdmapi

| datamover    | True    | public    | http://10.10.2.10:8784/v2
                 |
| cca52aff6b2a4f47bcc84b34647fba71 | RegionOne | nbosdmapi

| datamover    | True    | internal  | http://10.10.2.10:8784/v2
                 |
| e9aa6630bfb74a9bb7562d4161f4e07d | RegionOne | nbosdmapi

| datamover    | True    | admin     | http://10.10.2.10:8784/v2
                 |

[root@upstreamcontroller ~(keystone_admin)]# curl
http://10.10.2.10:8784/v2
{"error": {"message": "The request you have made requires
authentication.",
"code": 401, "title": "Unauthorized"}}


[root@upstreamcontroller ~(keystone_admin)]# systemctl status
nbosdmapi.service
● nbosdmapi.service - NetBackup for OpenStack DataMover API service
   Loaded: loaded (/etc/systemd/system/nbosdmapi.service; enabled;
```

```
   vendor preset: disabled)
   Active: active (running) since Sun 2020-04-12 12:31:11 EDT; 2
months
   9 days ago
 Main PID: 11252 (python)
    Tasks: 2
   CGroup: /system.slice/nbosdmapi.service
           ├─11252 /usr/bin/python /usr/bin/nbosdmapi-api
           └─11280 /usr/bin/python /usr/bin/nbosdmapi-api
```

nbosdm サービス

nbosdm サービスは各計算ノードで実行され、nova 計算サービスとして統合されます。

```
[root@upstreamcontroller ~(keystone_admin)]# openstack compute service
 list


[root@upstreamcompute1 ~]# systemctl status nbosdm
● nbosdm.service - NetBackup for OpenStack datamover service
   Loaded: loaded (/etc/systemd/system/nbosdm.service; enabled; vendor

preset: disabled)
   Active: active (running) since Wed 2020-06-10 10:07:28 EDT; 1
weeks
4 days ago
 Main PID: 10384 (python)
    Tasks: 21
   CGroup: /system.slice/nbosdm.service
           └─10384 /usr/bin/python /usr/bin/nbosdm
--config-file=/etc/nova/
nova.conf --config-file=/etc/nbosdm/nbosdm.conf
```

重要なログファイル

NetBackup for OpenStack ノード上

NetBackup for OpenStack クラスタには複数のログファイルが含まれています。

メインのログは nbosjm-policies.log で、進行中および過去の NetBackup for OpenStack のバックアップおよびリストアタスクに関するすべてのログが含まれます。これは、次の場所にあります。

```
/var/log/nbosjm/nbosjm-policies.log
```

次に重要なログは、NetBackup for OpenStack クラスタが受信した API 呼び出しに関するすべてのログを含む nbosjm-api.log です。これは、次の場所にあります。

```
/var/log/nbosjm/nbosjm-api.log
```

3 番目のサービスのログは nbosjm-scheduler.log です。これには、NetBackup for OpenStack クラスタ内の NetBackup for OpenStack ノード間の内部ジョブスケジュールに関するすべてのログが含まれています。

```
/var/log/nbosjm/nbosjm-scheduler.log
```

NetBackup for OpenStack ノードで実行されている最後のサービスは、スケジュールされた自動バックアップを制御する nbosjm-cron サービスです。

```
/var/log/nbosjm/nbosjm-cron.log
```

S3 をバックアップターゲットとして使用する場合は、S3 ストレージへの接続に使用される S3-Fuse プラグインを追跡するログファイルもあります。

```
/var/log/nbosjm/s3vaultfuse.py.log
```

RHOSP の NetBackup for OpenStack Datamover サービスログ

RHOSP の NetBackup for OpenStack Datamover サービスログには次のものがあります。

- nbosdmapi ログ
  NetBackup for OpenStack Datamover API サービスのログは、NetBackup for OpenStack Datamover API コンテナが実行されているノード (通常はコントローラ) にあります。
  ```
  /var/log/containers/nbosdmapi/nbosdmapi.log
  ```
- nbosdm ログ
  NetBackup for OpenStack Datamover サービスのログは、NetBackup for OpenStack Datamover コンテナが実行されているノード (通常は計算) にあります。
  ```
  /var/log/containers/nbosdm/nbosdm.log
  ```
  S3 が使用されている場合、S3 Fuse プラグインのログは次に示す同じノードにあります。
  ```
  /var/log/containers/nbosdm/nbos-object-store.log
  ```

VxMS でサポートされている Linux ファイルシステムの場合、増分バックアップの VxMS ログは次の場所に格納されます: `/usr/openv/netbackup/logs/vxms/`

VxMS ログレベルは /usr/openv/netbackup/bp.conf ファイルで定義され、デフォルトでは 3 に構成されます。

```
VXMS_VERBOSE = 3
```

ログレベルは 0 から 5 までを構成できます。数値が大きいほど、ログは詳細になります。

メモ: ログの詳細度を高く設定すると、VxMS ログにかなりのディスク容量が必要になる場合があります。ディスク容量に関連する問題を避けるために、VxMS ログファイルを定期的にクリーンアップしてください。

表 8-1 VxMS のログレベル

ログレベル	説明
0	ログなし
1	エラーログ
2	レベル 1 + 警告メッセージ
3	レベル 2 + 情報メッセージ
4	レベル 3 と同じ。
5	非常に詳細 (レベル 1 を含む) + 補助的な証拠ファイル (.MMF、.DUMP、.XML、.RVPMEM)

Ansible OpenStack の NetBackup for OpenStack Datamover サービスログ

Ansible OpenStack の NetBackup for OpenStack Datamover サービスログには次のものがあります。

- nbosdmapi ログ
  NetBackup for OpenStack Datamover API サービスのログは、NetBackup for OpenStack Datamover API コンテナが実行されているノード (通常はコントローラ) にあります。`lxc-attach` コマンドを使用して nbosdmapi コンテナにログインします。
  ```
  lxc-attach -n controller_nbosdmapi_container-a11984bf
  ```
  ログファイルは次の場所にあります。
  ```
  /var/log/nbosdmapi/nbosdmapi.log
  ```
- nbosdm ログ
  通常、NetBackup for OpenStack Datamover サービスのログは計算ノードにあり、ログは次の場所にあります。
  ```
  /var/log/nbosdm/nbosdm.log
  ```
  同じノードにある S3 Fuse プラグインのログで S3 が使用されている場合:
  ```
  /var/log/nbos-object-store/nbos-object-store.log
  ```

VxMS でサポートされている Linux ファイルシステムの場合、増分バックアップの VxMS ログは次の場所に格納されます: `/usr/openv/netbackup/logs/vxms/`

VxMS ログレベルは /usr/openv/netbackup/bp.conf ファイルで定義され、デフォルトでは 3 に構成されます。

```
VXMS_VERBOSE = 3
```

ログレベルは 0 から 5 までを構成できます。数値が大きいほど、ログは詳細になります。

メモ: ログの詳細度を高く設定すると、VxMS ログにかなりのディスク容量が必要になる場合があります。ディスク容量に関連する問題を避けるために、VxMS ログファイルを定期的にクリーンアップしてください。

表 8-2 VxMS のログレベル

ログレベル	説明
0	ログなし
1	エラーログ
2	レベル 1 + 警告メッセージ
3	レベル 2 + 情報メッセージ
4	レベル 3 と同じ。
5	非常に詳細 (レベル 1 を含む) + 補助的な証拠ファイル (.MMF、.DUMP、.XML、.RVPMEM)

Kolla Ussuri の NetBackup for OpenStack Datamover サービスログ

- nbosdmapi ログ:
  NetBackup for OpenStack Datamover API サービスのログは、NetBackup for OpenStack Datamover API コンテナが実行されているノード (通常はコントローラ) にあります。
  Docker コマンドを使用して nbosdmapi コンテナにログインします。
  ```
  docker container exec -it < nbosdmapi_container_id > /bin/bash
  ```
  ログファイルは次の場所にあります。/var/log/kolla/nbosdmapi/nbosdmapi.log
- nbosdm ログ:
  通常、NetBackup for OpenStack Datamover サービスのログは計算ノードにあります。
  Docker コマンドを使用して nbosdm コンテナにログインします。
  ```
  docker container exec -it < nbosdm_container_id > /bin/bash
  ```
  ログファイルは次の場所にあります。var/log/kolla/nbosdm/nbosdm.log

利用できないマウントポイントが原因でオフライン状態になる NBOSDM コンテナのトラブルシューティング

NetBackup for OpenStack Datamover コンテナが応答を停止した場合は、利用できないマウントポイントまたは誤ったマウントパスが原因である可能性があります。

ログでエラーを確認します。NetBackup for OpenStack Datamover コンテナログは次の場所に保存されます。

- RHOSP: `/var/log/nbosdm/nbosdm.log`
- OpenStack Ansible: `/var/log/nbosdm/nbosdm.log`

ログファイルの例:

```
2021-08-31 12:42:37.630 17 ERROR
oslo_messaging.rpc.server nbosdm.exception.InvalidNFSMountPoint:
Error: '/var/lib/nova/NetBackupOpenStack-mounts/MTAuMjIxLjk5LjUx
Oi9tbnQvbmZzX3NoYXJlL2RvY3M=' is not
'10.2xx.xx.50:/mnt/nfs_share/docs'
mounted
2021-08-31 12:42:37.630 17 ERROR oslo_messaging.rpc.server
```

この問題を RHOSP で解決するには

1. `nbos_env.yaml` ファイルに正しいマウントパスを指定します。
2. 次の配備コマンドを実行します。

   ```
   openstack overcloud deploy
   ```

OpenStack Ansible でこの問題を解決するには

1. NBOSDM と NBOSDMAPI サービスをアンインストールします。

   ```
   openstack-ansible os-nbos-install.yml --tags "nbos-all-uninstall"
   ```

2. `/etc/openstack_deploy/user_nbos_vars.yml`ファイルに正しいマウントパスを指定します。
3. 次のインストールコマンドを実行します。

   ```
   openstack-ansible os-nbos-install.yml
   ```

複数の OpenStack 配布間で同じ NFS 共有パスを使用する場合のアクセス権拒否エラーについて

環境内に保護対象の OpenStack 配布が複数ある場合は、各 OpenStack 配布に異なる NFS 共有パスを使用する必要があります。すべての OpenStack 配布に同じ NFS 共

有パスを使用すると、バックアップ操作の実行中にアクセス権の拒否エラーが表示されます。

各 OpenStack セットアップで nova ユーザー ID が異なるため、アクセス権拒否エラーが発生します。たとえば、RHOSP の nova ユーザー ID は 42436 で、OpenStack Ansible の場合は 999 です。NetBackup for OpenStack VM がスナップショットを実行するとき、nova ユーザーを使用して `nbosdm_tasks` ディレクトリを作成します。このディレクトリを作成する最初の nova ユーザーには必要な権限がありますが、2 番目の nova ユーザーには必要な権限が付与されません。したがって、同じ NFS 共有パスを異なる OpenStack セットアップ間で使用することはできません。

同じ NFS 共有パスを複数の OpenStack セットアップで使用できるのは、nova ユーザー ID がすべてのセットアップで同じ場合のみです。

Windows インスタンスのリストア後にディスクがオフライン状態になる

Windows インスタンスをリストアすると、インスタンスに接続されているディスクがオフライン状態になります。リストア後に Windows インスタンスのディスクは自動的にオンラインとして表示されません。

リストア後にディスクが自動的にオンラインとして表示されるようにするには、インスタンスのバックアップの前に SAN ポリシーを OnlineAll に更新します。

SAN ポリシーを更新するには

1. 管理者として Windows コマンドプロンプトを実行します。
2. `diskpart` と入力して、Enter キーを押します。
3. `san` と入力して Enter キーを押して、現在の SAN ポリシーを表示します。
4. `san POLICY=OnlineAll` と入力し、Enter キーを押して SAN ポリシーを OnlineAll に更新します。

メモ: この問題は、Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012 にのみ該当します。
