NetBackup™ for OpenStack 管理者ガイド

リリース 11.1

VERITAS
now part of Cohesity

NetBackup™ for OpenStack 管理者ガイド

最終更新日: 2026-01-22

法的通知と登録商標

Cohesity、Veritas、Cohesity ロゴ、Veritas ロゴ、Veritas Alta、Cohesity Alta、NetBackup for OpenStack は、Cohesity, Inc. またはその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、Cohesity 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア(「サードパーティ製プログラム」)が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このCohesity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。Cohesity, Inc. 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。Cohesity, Inc. およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

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

Cohesity, Inc.
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サ

ポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Cohesity Account の情報を管理できます。

https://my.veritas.com

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

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

マニュアル

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

Cohesity Services and Operations Readiness Tools (SORT)

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

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

目次

1

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

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バックアップとしてキャプチャします。これらのバックアップは MSDP を使用した NetBackup ユニバーサル共有に保持され、NetBackup をサポートするターゲットストレージに複製できます。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。増分バックアップは、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

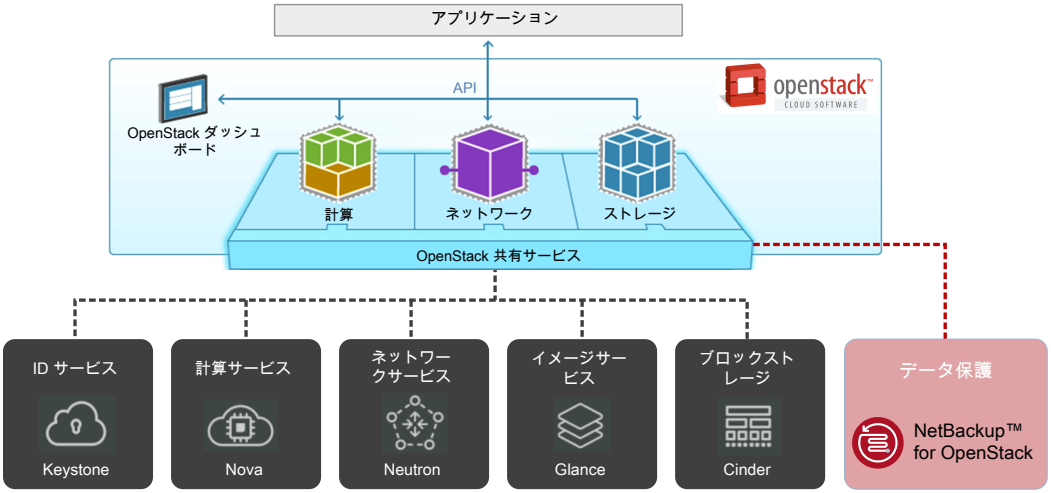
降に変更されたデータブロックのみが含まれるため、バックアップ処理が効率的で、バックアップイメージをバックアップメディアに効率的に格納します。

- 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、複数の仮想マシン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。
- 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)

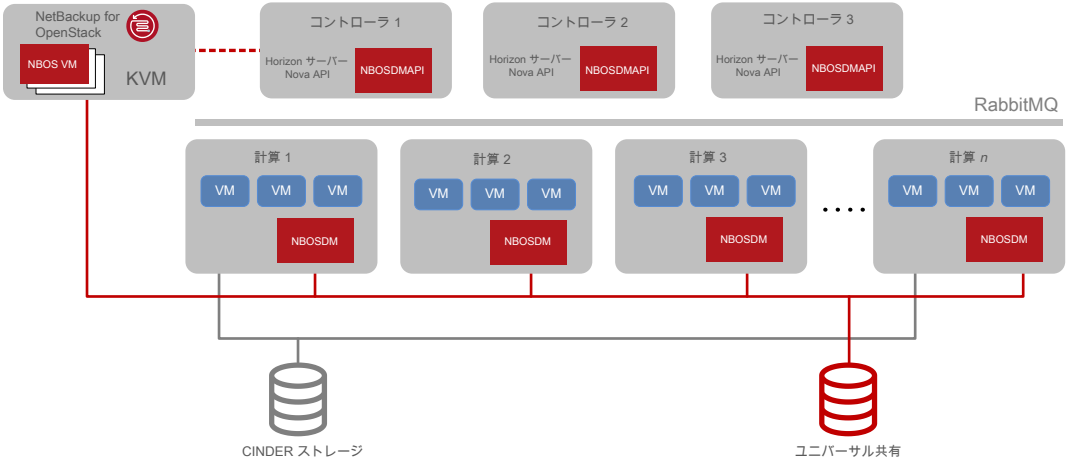
図 1-1 BaaS (Backup as a Service) を提供するデータ保護プロジェクト



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

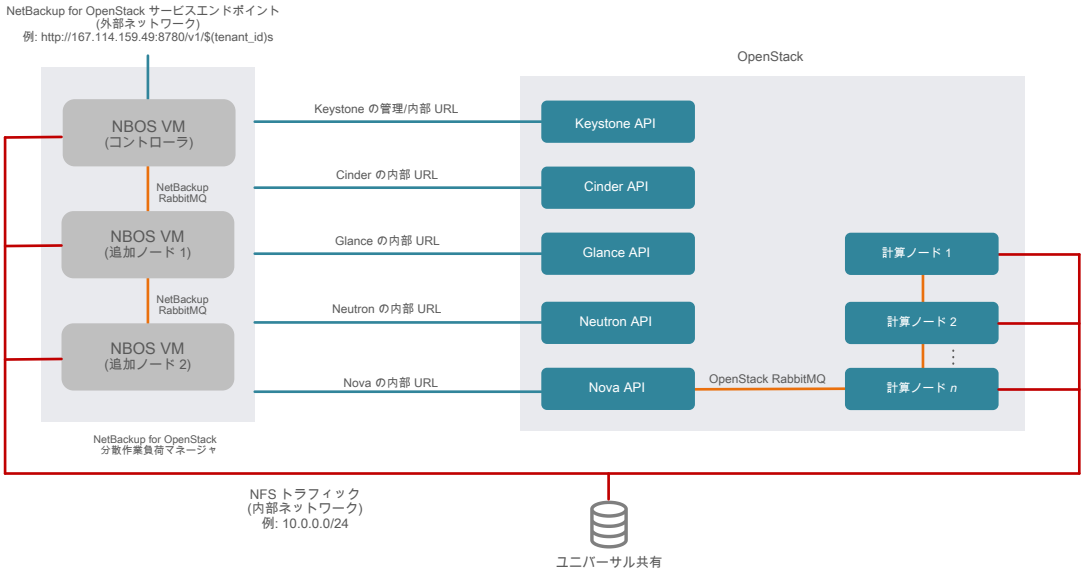


NetBackup for OpenStack には、4 つの主要なソフトウェアコンポーネントがあります。

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

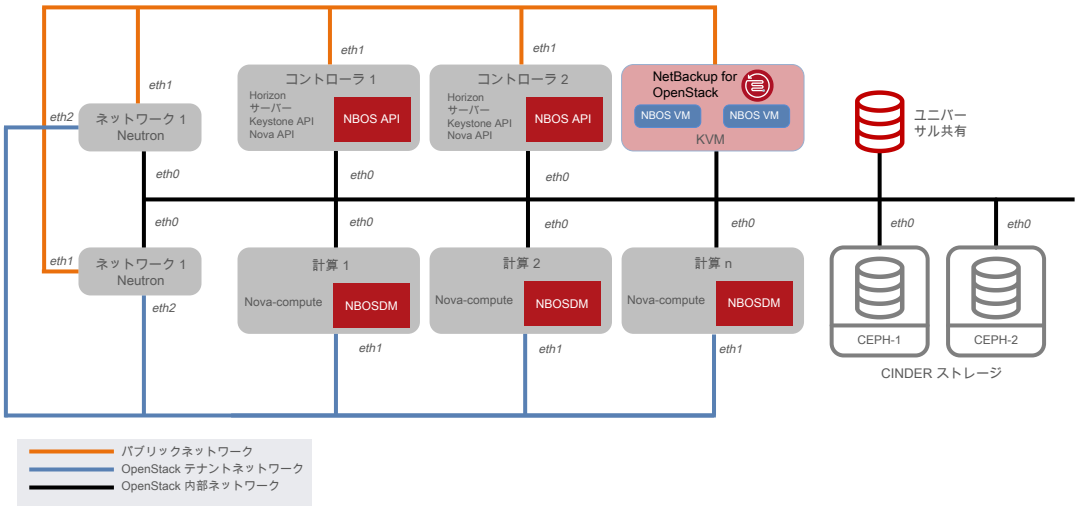
図 1-3　　サービスのエンドポイントの概要



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

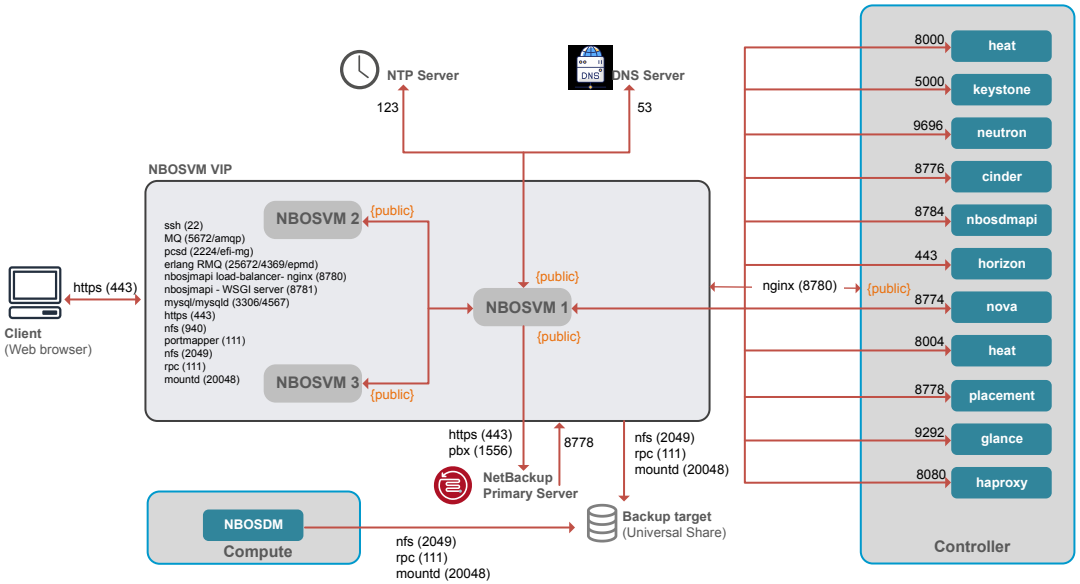
図 1-4　　ネットワークトポロジーの例



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でパブリック URL エンドポイントを公開します。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。

NetBackup for OpenStack ポート

図 1-5 NetBackup for OpenStack ポート



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 Datamover 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.17 の「NetBackup for OpenStack 仮想マシンのシステム要件」を参照してください。

p.17 の「ソフトウェア要件 」を参照してください。

NetBackup for OpenStack 仮想マシンのシステム要件

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。

Cohesity 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 仮想マシンデータベースまたはログファイルが 40 GB ディスクを超える場合は、Cohesity カスタマー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 仮想マシン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
Red Hat Enterprise Linux	8.9
Virsh	libvirt 2.0.0 以降
QEMU	2.0.0 以降
QEMU ディスクイメージユーティリティ(qemu-img)	2.6.0 以降

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されます。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されます。管理エンドポイントは、OpenStack 管理者が使用されます。

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。NetBackup for OpenStack はパブリックエンドポイントと内部エンドポイントをサポートします。

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

Cohesity 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 仮想マシン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 datamover 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。

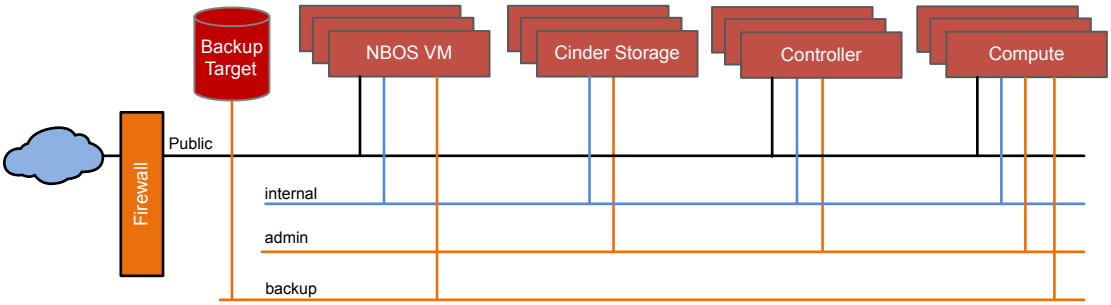
- NetBackup for OpenStack Appliance はバックアップターゲットにアクセスする必要があります。
- すべての計算ノードがバックアップターゲットにアクセスする必要があります。

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。

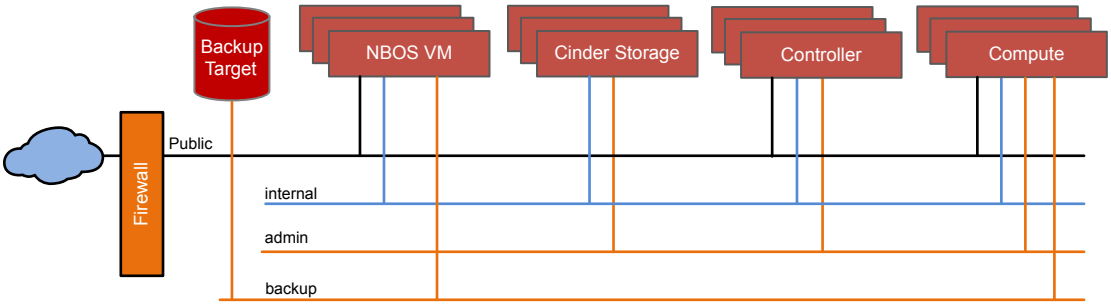
図 2-1 NetBackup for OpenStack のインストール前の標準的な OpenStack ネットワーク構成



OpenStack の標準とCohesity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



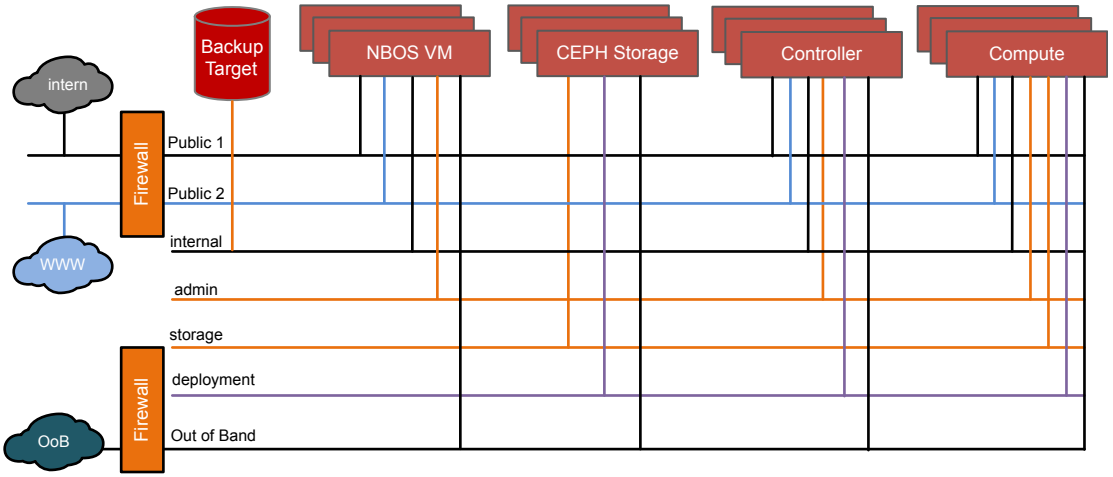
必要に応じてネットワークを組み合わせられます。必要なネットワークアクセスが利用可能であるかぎり、NetBackup for OpenStack は機能します。

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。

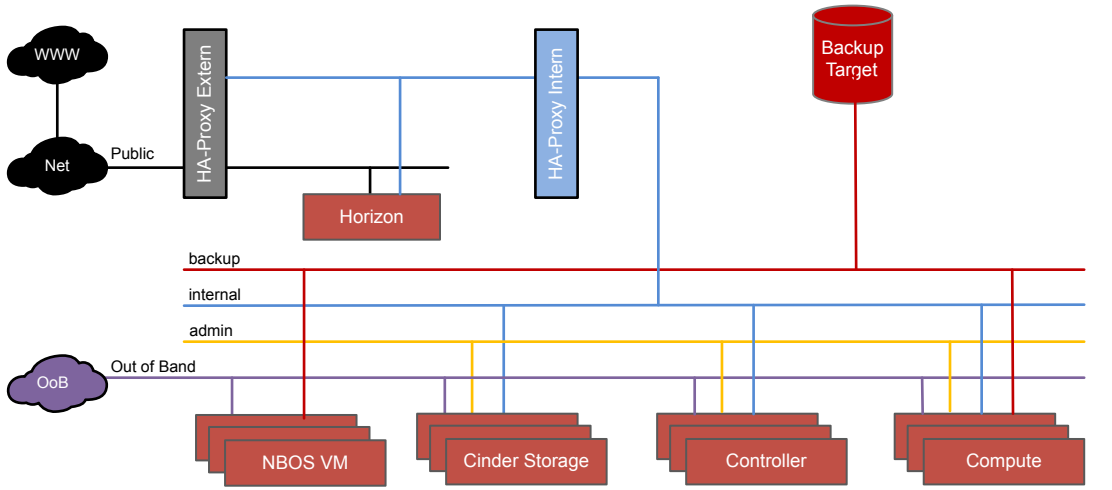
最初の例は、機能別にネットワークを分割する必要がある製造会社で、NetBackup for OpenStack バックアップターゲットを内部ネットワークに配置することにしました。バックアップとリカバリ機能が OpenStack 内部ソリューションとして識別されています。この例は複雑に見えますが、NetBackup for OpenStack が推奨どおりに統合されています。

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。

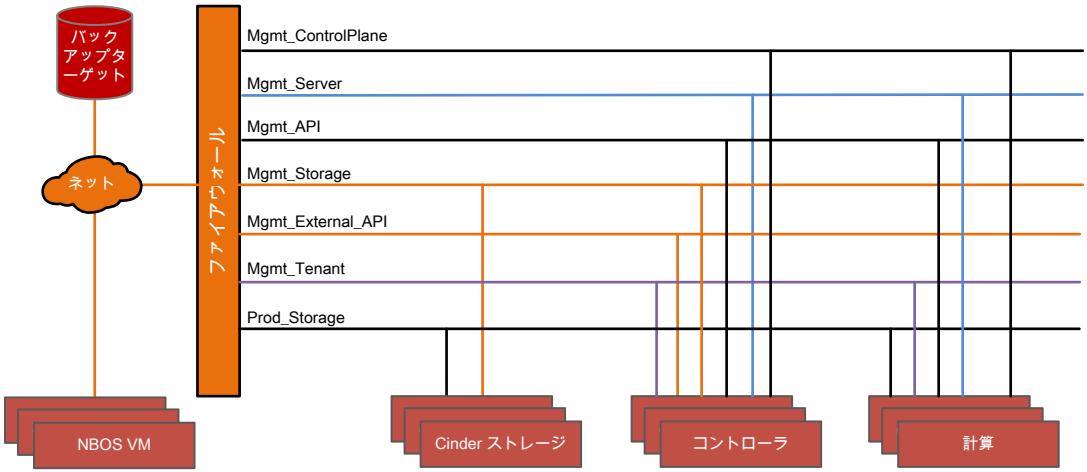
図 2-4 トラストネットワークがない例



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。

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 仮想マシンのスピンアップ

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
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、いくつかのスクリプトと設定情報が含まれています。たとえば、ユーザーパスワードです。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 コマンドラインと作成された 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
```

KVM サーバー - RHEL バージョン 9 以降の場合:

```
virt-install -n nbosvm --memory 24576  --vcpus 8 ¥
--osinfo rhel8-unknown ¥
--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

NetBackup for OpenStack はユニバーサル共有を使用してバックアップイメージを格納します。

ユニバーサル共有の構成について詳しくは、『NetBackup 重複排除ガイド』の「ユニバーサル共有の構成と管理」の章を参照してください。

ユニバーサル共有を作成するときに、[ホスト (Host)]フィールドに、すべての計算ノードと NetBackup for OpenStack 仮想マシンの IP アドレスまたはサブネットを追加します。

例:

IP アドレス: `10.210.xxx.xx1, 10.210.xxx.xx2, 10.210.xxx.xx3, 10.210.xxx.xx4, 10.210.xxx.xx5, 10.210.xxx.xx6, ... 10.210.xxx.x20`

サブネット: `10.210.128.0/20`

メモ: 計算ノードと NetBackup for OpenStack 仮想マシンにメディアサーバーからアクセスして、計算ノードと NetBackup for OpenStack 仮想マシンにユニバーサル共有をマウントできることを確認します。

パフォーマンス向上のために、専用のバックアップネットワークを計算ノードに割り当て、このネットワークを使用してユニバーサル共有をマウントできます。

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

NetBackup for OpenStack 仮想マシンまたは NetBackup for OpenStack 仮想マシン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.29 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.29 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.30 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.30 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.32 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.33 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.34 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.35 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.36 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.27 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.29 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。

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。

- `rhosp17.1`

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-rhel9/openstack-keystone:17.1
```

RHOSP17.1 の CONTAINER_TAG 形式: <NBOS_VERSION>-rhosp17.1

例:

```
sudo ./prepare_nbos_images.sh nbos-undercloud 10.4.1.1035-rhosp17.1
/home/stack/nbos/nbos-rhosp17.1-10.4.1.1035
```

次のコマンドを使用して、変更内容を確認できます。

```
sudo podman images | grep nbos
localhost/nbos-horizon-plugin
                    10.4.1.1035-rhosp17.1  c4ba2c4ff0f8  3 days ago
    1.01 GB
localhost/nbosdmapi
                    10.4.1.1035-rhosp17.1  8baac9920a8e  3 days ago
    1.13 GB
localhost/nbosdm
                    10.4.1.1035-rhosp17.1  86542c17acc2  3 days ago
    2.76 GB
```

```
(undercloud) [stack@host scripts]$ grep -i image
../environments/nbos_env.yaml
   docker_nbosdm_image:
nbos-undercloud:8787/nbosdm:10.4.1.1035-rhosp17.1
   docker_nbosdmapi_image:
nbos-undercloud:8787/nbosdmapi:10.4.1.1035-rhosp17.1
   ContainerHorizonImage:
nbos-undercloud:8787/nbos-horizon-plugin:10.4.1.1035-rhosp17.1
```

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、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

```
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:10.4.1.1035-rhosp17.1
   docker_nbosdmapi_image:
nbos-undercloud:8787/nbosdmapi:10.4.1.1035-rhosp17.1

   ## 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:
```

```
10.4.1.1035-rhosp17.1


## 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 --stack overcloud --templates ¥
  -n /home/stack/templates/network_data.yaml ¥
  -r /home/stack/templates/roles_data.yaml ¥
  -e /home/stack/templates/enable-tls.yaml ¥
  -e /home/stack/templates/inject-trust-anchor-hiera.yaml ¥
  -e /home/stack/nbos-cfg-scripts/redhat-director-scripts/
<RHOSP_RELEASE_DIRECTORY>/environments/nbos_env_tls_endpoints_public_ip.yaml
 ¥
  -e /home/stack/templates/overcloud-baremetal-deployed.yaml ¥
  -e /home/stack/templates/overcloud-networks-deployed.yaml ¥
  -e /home/stack/templates/overcloud-vip-deployed.yaml ¥
  -e /home/stack/containers-prepare-parameter.yaml ¥
  -e /home/stack/templates/environment-file.yaml ¥
  -e /home/stack/nbos-cfg-scripts/redhat-director-scripts/
<RHOSP_release_directory>/environments/nbos_env.yaml ¥
```

```
  --ntp-server 172.16.8.24 >
/home/stack/templates/overcloud_deploy.log
```

配備の検証

nbosdmapi コンテナがコントローラノードに配備されておらず、nbosdm コンテナが計算ノードに配備されていない場合は、次の手順を実行します。

1. 次のコマンドを実行して、変更した roles_data.yaml ファイルでテンプレートをレンダリングし、オーバークラウド配備を実行します。

   ```
   /usr/share/openstack-tripleo-heat-templates/tools/process-templates.py
   -p /usr/share/openstack-tripleo-heat-templates -r
   /home/stack/templates/roles_data.yaml -n
   /home/stack/templates/default-network-isolation.yaml -o
   /home/stack/templates/generated-openstack-tripleo-heat-templates
   --safe
   ```

2. overcloud deploy コマンドを使用して、生成されたテンプレートパスを指定します。

   例:

   ```
   openstack overcloud deploy --stack overcloud --templates
   /home/stack/templates/generated-openstack-tripleo-heat-templates
   ```

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。

- コントローラノード上:
  NetBackup for 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 for 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  ~]# podman ps | grep nbos
  26fcb9194566
  rhospqa.ctlplane.localdomain:8787/nbosdmapi:10.4.1.1035-rhosp17.1

  kolla_start           5 days ago  Up 5 days ago         nbosdmapi
  094971d0f5a9  rhospqa.ctlplane.localdomain:
  8787/nbos-horizon-plugin:10.4.1.1035-rhosp17.1       kolla_start

  5 days ago  Up 5 days ago         horizon
  ```

- 計算ノード上:

NetBackup for 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 for 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  ~]# podman ps | grep nbos
26fcb9194566
rhospqa.ctlplane.localdomain:8787/nbosdmapi:10.4.1.1035-rhosp17.1

kolla_start           5 days ago  Up 5 days ago         nbosdmapi
094971d0f5a9  rhospqa.ctlplane.localdomain:
8787/nbos-horizon-plugin:10.4.1.1035-rhosp17.1       kolla_start

5 days ago  Up 5 days ago         horizon
```

- 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。

メモ: 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 Horizon プラグインがあります。

```
[root@overcloud-controller-0  ~]# podman ps | grep horizon
094971d0f5a9  rhospqa.ctlplane.localdomain:
8787/nbos-horizon-plugin:10.4.1.1035-rhosp17.1       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配備されます。

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取得します。

- `(undercloud)$ openstack stack failures list <overcloud>--long`
  `<overcloud>` オーバークラウドの名前。
- `(undercloud)$ openstack stack list --nested --property status=FAILED`

詳しくは、OpenStack のマニュアルを参照してください。

nbosdmapi コンテナが起動しないか、再起動状態にある場合は、次のコマンドを実行してトラブルシューティングを行うためにログを取得します。

- `podman logs nbosdmapi`
- `tail -f /var/log/containers/nbosdmapi/nbosdmapi.log`

nbosdm コンテナが起動しないか、再起動状態にある場合は、次のコマンドを実行してトラブルシューティングを行うためにログを取得します。

- `podman 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.37 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。

手順	作業	説明
2	NetBackup for OpenStack ノードの nova ユーザー ID の変更	p.38 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.39 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.42 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.43 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 仮想マシン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 仮想マシン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 仮想マシンの `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.27 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



###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
```

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 RHEL 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 へのインストール

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

表 2-3 Kolla 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.45 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.27 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.46 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.46 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。
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.48 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.54 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 バックアップマウント機能の有効化	p.54 の「NetBackup for OpenStack バックアップマウント機能の有効化」を参照してください。
7	NetBackup for OpenStack コンテナイメージのプル	p.56 の「NetBackup for OpenStack コンテナイメージのプル」を参照してください。
8	NetBackup for OpenStack コンポーネントの配備	p.57 の「NetBackup for OpenStack コンポーネントの配備」を参照してください。
9	NetBackup for OpenStack 配備の検証	p.57 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 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 仮想マシン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 仮想マシン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 仮想マシンの 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. インストールディレクトリに移動します。

   Yoga リリース: `cd kolla_yoga`

   Caracal リリース: `cd kolla`
2. `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 NetBackupOpenStack_globals.yml >> /etc/kolla/globals.yml
   ```

3 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 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>
```

4 NetBackup for OpenStack's YAML ファイルのコンテンツを kolla ansible の site.yml ファイルに追加します。

メモ: YAML ファイルのコンテンツを追加する前に、site.ymlファイルのバックアップを作成します。

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

Caracal リリース: `cat NetBackupOpenStack_site.yml >> /path/to/venv/share/kolla-ansible/ansible/site.yml`

Yoga リリース: `cat NetBackupOpenStack_yoga_site.yml >> /path/to/venv/share/kolla-ansible/ansible/site.yml`

5 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 NetBackupOpenStack_inventory.txt >> <your inventory file name path>
```

次に例を示します。

```
cat 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.48 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.48 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

RHEL 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	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 }}-{{ openstack_release }}.tar
  ```

  次に例を示します。

  ```
  docker load --input nbosdmapi-ubuntu-9.1.2.20211021104525-{{
  openstack_release }}.tar
  ```

- nbosdm

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

  例:

  ```
  docker load --input nbosdm-ubuntu-9.1.2.20211021104525-{{
  openstack_release }}.tar
  ```

- nbos-horizon-plugin (Yoga リリース)

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

  例:

  ```
  docker load --input
  nbos-horizon-plugin-source-ubuntu-9.1.2.20211021104525-{{
  openstack_release }}.tar
  ```

- nbos-horizon-plugin (Caracal リリース)

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

  例:

  ```
  docker load --input
  nbos-horizon-plugin-ubuntu-9.1.2.20211021104525-{{
  openstack_release }}.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 localhost/nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }} nbos/nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}`
  - `docker tag localhost/nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}`

FQDN:5001/nbos/nbosdmapi-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}

例:

- docker tag localhost/nbosdmapi-ubuntu:9.1.2.20211021104525-{{ openstack_release }} nbos/nbosdmapi-ubuntu:9.1.2.20211021104525-{{ openstack_release }}
- docker tag localhost/nbosdmapi-ubuntu:9.1.2.20211021104525-{{ openstack_release }} deployment-vm.vxindia.veritas.com:5001/nbos/nbosdmapi-ubuntu:9.1.2.20211021104525-{{ openstack_release }}

- nbosdm
  - docker tag localhost/nbosdm-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }} nbos/nbosdm-<kolla-base-distro>:<NBOS_version>-{{ openstack_release }}
  - docker tag localhost/nbosdm-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }} FQDN:5001/nbos/nbosdm-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}

  例:

  - docker tag localhost/nbosdm-ubuntu:9.1.2.20211021104525-{{ openstack_release }} nbos/nbosdm-ubuntu:9.1.2.20211021104525-{{ openstack_release }}
  - docker tag localhost/nbosdm-ubuntu:9.1.2.20211021104525-{{ openstack_release }} deployment-vm.vxindia.veritas.com:5001/nbos/nbosdm-ubuntu:9.1.2.20211021104525-{{ openstack_release }}

- nbos-horizon-plugin (Yoga リリース)
  - docker tag localhost/nbos-horizon-plugin-{{ kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }} nbos/nbos-horion-plugin-{{ kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}

- docker tag localhost/nbos-horizon-plugin-{{ kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }} FQDN:5001/nbos/nbos-horizon-plugin-{{ kolla-install-type }}-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}

例:

- docker tag localhost/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-{{ openstack_release }} nbos/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-{{ openstack_release }}
- docker tag localhost/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-{{ openstack_release }} deployment-vm.vxindia.veritas.com:5001/nbos/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-{{ openstack_release }}

- nbos-horizon-plugin (Caracal リリース)
  - docker tag localhost/nbos-horizon-plugin-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }} nbos/nbos-horion-plugin-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}
  - docker tag localhost/nbos-horizon-plugin-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }} FQDN:5001/nbos/nbos-horizon-plugin-{{ kolla-base-distro }}:{{ NBOS_version }}-{{ openstack_release }}

例:

- docker tag localhost/nbos-horizon-plugin-ubuntu:9.1.2.20211021104525-{{ openstack_release }} nbos/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-{{ openstack_release }}
- docker tag localhost/nbos-horizon-plugin-ubuntu:9.1.2.20211021104525-{{ openstack_release }} deployment-vm.vxindia.veritas.com:5001/nbos/nbos-horizon-plugin-source-ubuntu:9.1.2.20211021104525-{{ openstack_release }}

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 }}-{{ openstack_release }}
  ```

  次に例を示します。

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

- nbosdm

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

  例:

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

- nbos-horizon-plugin (Yoga リリース)

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

  例:

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

- nbos-horizon-plugin (Caracal リリース)

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

  例:

  ```
  docker push
  deployment-vm.vxindia.veritas.com:5001/nbos/nbos-horizon-plugin
  -ubuntu:9.1.2.20211021104525-{{ openstack_release }}
  ```

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-ubuntu",
"nbos/nbosdm-ubuntu","nbos/nbosdmapi-ubuntu"]}
```

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。

NetBackup for OpenStack バックアップマウント機能の有効化

NetBackup for OpenStack のバックアップ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   r0000-000-vm00.sample.name.com:
5001/nbos/nbosdmapi-ubuntu:10.0.0.1.1007-{{ openstack_release }}

"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   r0000-000-vm00.sample.name.com:
5001/nbos/nbosdm-ubuntu:10.0.0.1.1007-{{ openstack_release }}
"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   r0000-000-vm00.sample.name.com:
5001/nbos/nbos-horizon-plugin-binary-ubuntu:10.0.0.1.1007-{{
openstack_release }}
"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。

メモ: NetBackup Flex Appliance の場合、NetBackup for OpenStackを構成する前に、有効な NetBackup CA が署名した証明書を `/etc/nbos/ssl/nbu_cacert.pem` に手動でコピーする必要があります。

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 と OpenStack 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。NetBackup for OpenStack はパブリックエンドポイントと内部エンドポイントをサポートします。
  - 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のドメイン
  - 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_

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。

p.62 の「NBOSVM 用の安全な通信の構成」を参照してください。

NBOSVM 用の安全な通信の構成

NBOSVM 用に安全な通信を使用できます。安全な通信を使用する場合は、証明書とその秘密鍵をアップロードする必要があります。

安全な通信を設定するには

1. OpenStack コンフィギュレータ UI のNetBackupにログオンします。
2. [構成の詳細 (Configuration Details)]タブで、ページの最後にある[再構成 (Reconfigure)]をクリックします。
3. [詳細設定 (Advanced Settings)]を選択します。
4. [NetBackup for OpenStack URL]フィールドで、URL の HTTP を HTTPS に変更します。
5. [証明書 (Certificate)]と[秘密鍵 (Private Key)]をクリックして、ファイルをアップロードします。

   証明書とキーを生成するには、いずれかの NBOSVM ノードの `/etc/nbos/ssl` の場所に移動し、次のコマンドを実行します。

   ```
   ./gen-cer <NBOSVM VIP>
   ```

   このコマンドは、ファイル名として NBOSVM 仮想 IP を持つ証明書ファイルとキーファイルを生成します。

   たとえば、NBOSVM 仮想 IP が 10.10.20.111 の場合、コマンド `./gen-cert 10.10.20.111` を実行します。

   このコマンドは `10.10.20.111.crt` や `10.10.20.111.key` などのファイルを生成します。

   `10.10.20.111.crt` ファイルと`10.10.20.111.key`ファイルをアップロードします。
6. [NetBackup for OpenStack URL]フィールドの横にあるドロップダウンをクリックします。

   [NetBackup for OpenStack 管理 URL (NetBackup for OpenStack Admin URL)]と[NetBackup for OpenStack 内部 URL (NetBackup for OpenStack Internal URL)]フィールドで、HTTP を HTTPS に変更します。
7. NBOSVM の構成が正常に完了したら、NBOSVM から次の場所にある各コントローラノードに `/opt/stack/data/cert/nbosjm.cert` ファイルをコピーします。

- Kolla-openstack: `/etc/kolla/horizon`
- RHOSP: `/var/lib/config-data/puppet-generated/horizon`

8 これらのファイルに次の権限を与えます。

- Kolla-openstack:

```
chmod o+x /etc/kolla/horizon
chmod o+rx /etc/kolla/horizon/nbosjm.cert
```

- RHOSP:

```
chmod o+rx
/var/lib/config-data/puppet-generated/horizon/nbosjm.cert
```

9 nbosjm CLI を使う前に、NBOSVM で次のコマンドを実行します。

```
export OS_CACERT=/etc/nbosjm/ca-chain.pem
```

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、Cohesity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。

NetBackup for OpenStack でのリソーススロットル

リソーススロットルは、パフォーマンスを管理し、システムの過負荷を防ぎ、プロジェクト間で NetBackup for OpenStack のリソース割り当てが均等に行われるようにします。スロットルはリソースの過剰な消費を防ぎ、安定の維持に役立ちます。また、スロットルは、システム障害と、パフォーマンス低下によって発生する問題を防ぎます。

表 2-6 NetBackup for OpenStack でのリソーススロットルのオプション

オプション	説明
MAX_BFS_JOBS_PER_NBOS	スナップショットジョブからバックアップ数を同時に実行するための NetBackup 側のリソーススロットル。 NetBackup プライマリサーバーの /usr/openv/netbackup/bp.conf ファイルにある値を構成します。 デフォルト値: MAX_BFS_JOBS_PER_NBOS = 3
max_snapshot_jobs_per_project	プロジェクトごとにスナップショットジョブ数を同時に実行するための NetBackup for OpenStack 仮想マシンでのリソーススロットル。 各 nbosvm ノードの /etc/nbosjm/nbosjm.conf ファイルで値を設定します。 このサービスを実行している nbosvm ノードのいずれかで、nbosjm-scheduler サービスを再起動します。3 ノードクラスタで、次のコマンドを実行して、nbosjm-scheduler サービスが実行されている nbosvm ノードを確認します: pcs status デフォルト値: max_snapshot_jobs_per_project = 2

オプション	説明
max_snapshot_expiry_jobs_per_project	プロジェクトごとにスナップショットジョブ数を同時に期限切れにするための NetBackup for OpenStack 仮想マシンでのリソーススロットル。 各 nbosvm ノードの /etc/nbosjm/nbosjm.conf ファイルで値を設定します。 このサービスを実行している nbosvm ノードのいずれかで、nbosjm-scheduler サービスを再起動します。3 ノードクラスタで、次のコマンドを実行して、nbosjm-scheduler サービスが実行されている nbosvm ノードを確認します: pcs status デフォルト値: max_snapshot_expiry_jobs_per_project = 2
max_uploads_pending	計算ノードごとにデータ移動操作を同時に実行するための NetBackup for OpenStack datamover のリソーススロットル。 計算ノードの nbosdm.conf ファイルで値を設定します。 その計算ノードで実行されている nbosdm コンテナを再起動します。 デフォルト値: max_uploads_pending = 5

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してください。

```
[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.
```

NetBackup for OpenStack のアンインストール

NetBackup for OpenStack のアンインストール手順は、インストールされている OpenStack 配布によって異なります。ただし、次の大まかな手順はすべてのディストリビューションで同じです。

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 サービスをクリーニングします。	p.72 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 サービスをクリーニングします。	p.73 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 リソースをクリーニングします。	p.74 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 リソースをクリーニングします。	p.75 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をクリーニングします。	p.75 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します。	p.76 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 コンテナに復元します。	p.76 の「元の RHOSP Horizon コンテナの復元」を参照してください。
NetBackup for OpenStack 仮想マシンクラスタを破棄します。	p.77 の「NetBackup for OpenStack 仮想マシンクラスタの破棄」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 RHOSP17.1 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 RHOSP17.1 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 RHOSP17.1 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 RHOSP17.1 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 RHOSP17.1 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 仮想マシンクラスタの破棄

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 仮想マシンを破棄します

```
virsh destroy <NetBackup for OpenStack virtual machine Name or ID>
```

NetBackup for OpenStack 仮想マシンの定義を解除します

```
virsh undefine <NetBackup for OpenStack virtual machine name>
```

KVM ホストストレージから NetBackup for OpenStack 仮想マシン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.78 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.78 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.78 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.79 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.79 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.79 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.80 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.80 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.80 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.81 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 仮想マシンクラスタの破棄	p.81 の「NetBackup for OpenStack 仮想マシンクラスタの破棄」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 仮想マシンクラスタの破棄

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 仮想マシンを破棄します

```
virsh destroy <NetBackup for OpenStack virtual machine Name or ID>
```

NetBackup for OpenStack 仮想マシンの定義を解除します

```
virsh undefine <NetBackup for OpenStack virtual machine name>
```

KVM ホストストレージから NetBackup for OpenStack 仮想マシン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 仮想マシンクラスタの破棄

NetBackup for OpenStack 仮想マシン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 仮想マシンを破棄します

   ```
   virsh destroy <NetBackup for OpenStack virtual machine Name or
   ID>
   ```

3 NetBackup for OpenStack 仮想マシンの定義を解除します

```
virsh undefine <NetBackup for OpenStack virtual machine name>
```

4 KVM ホストストレージから NetBackup for OpenStack 仮想マシンディスクを削除します。

5 NetBackup for OpenStack を登録解除します。

- 次の API を使用してトークンを生成します。

```
POST https://<primary-server>:1556/netbackup/login

Provide username and password in body as :
{
  "userName": "username",
  "password": "password"
}
```

- 次の登録解除 API でトークンを Bearer トークンとして使用します。

```
DELETE
https://<primary-servver>/netbackup/config/servers/nbosvm-servers/<NBOSVM
 VIP
```

nbosjm CLI クライアントのインストール

nbosjm CLI クライアントは RPM および Debian パッケージとして提供されます。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 クライアントが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 クライアントは Python 3 でのみサポートされます。

nbosjm CLI クライアントをインストールするには

◆
- RPM ベースのオペレーティングシステムで次のコマンドを実行します。

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

- Debian ベースのオペレーティングシステムで次のコマンドを実行します。

```
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スタックを更新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 2-7 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 **2-7** 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 2-8 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 2-8 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
	}

NetBackup for OpenStack のアップグレード

NetBackup for OpenStack は以前のリリースからアップグレードできます。

前提条件:

- 既存の NetBackup for OpenStack 仮想マシンを削除する前に、構成ファイル /etc/nbosjm/nbosjm.conf のバックアップを作成します。このファイルを使用して、以前の構成変更を新しい NetBackup for OpenStack 仮想マシンに適用できます。
- すべてのスナップショットジョブが既存の NetBackup for OpenStack 仮想マシンで完了している必要があります。
- すべてのバックアップジョブが既存の NetBackup for OpenStack 仮想マシンで完了している必要があります。NetBackupプライマリサーバーで、不完全な SLP ジョブを完了としてマークします。
  - 不完全な SLP を一覧表示します。
    ```
    nbstlutil stlilist -image_incomplete
    ```
  - 不完全な SLP をキャンセルします。
    ```
    nbstlutil cancel -backupid
    ```
- 孤立スナップショットを削除します。
  p.92 の「孤立スナップショットの削除」を参照してください。

アップグレードでは、次の情報は保持されません。

- スナップショットのみの保護
- 電子メールの設定
- 監査ログ
- リストアされた VM データ

アップグレードでは、次の NetBackup for OpenStack データベーステーブルの情報は保持されません。

- `atomdetails`
- `auditlogs`
- `flowdetails`
- `logbooks`
- `restore_metadata`
- `restored_vm_meta`
- `restored_vm_res`
- `restored_vms restores`

NetBackup for OpenStack をアップグレードするには

1. ダウンロードセンターから最新の NetBackup for OpenStack パッケージをダウンロードします。
2. 新しい NetBackup for OpenStack 仮想マシンをスピンアップします。

   p.24 の「NetBackup for OpenStack 仮想マシンのスピンアップ」を参照してください。
3. 次のコマンドを実行して、いずれかの NetBackup for OpenStack 仮想マシンで保護をインポートします。

   ```
   nbosjm protection-import
   ```

   保護インポートジョブのタイムアウトは、デフォルトで 10 分です。タイムアウトを設定するには、`/etc/nbosjm/nbosjm.conf` ファイルで `protection_import_job_timeout_in_mins=<minutes>` を指定します。
4. 次のコマンドを実行して、インポートジョブの状態を表示します。

   ```
   nbosjm get-protection-import-status
   ```
5. グローバルジョブスケジューラを起動します。

   ```
   nbosjm enable-global-job-scheduler
   ```

孤立スナップショットの削除

スナップショットのコピーのみで構成されたリカバリポイントはアップグレードプロセス中にインポートされず、これらの孤立したスナップショットはコンピューティングストレージに残ります。

これらのスナップショットは delete_snapshots.py スクリプトを使用して削除できます。

孤立スナップショットを削除する方法

1. nbos-cfg-scripts パッケージを古い NBOSVM にコピーし、ファイルを抽出します。

   ```
   cp <imagelocation>/nbos-cfg-scripts.tar.gz /home/stack
   ```

   ```
   tar -xvf /home/stack/nbos-cfg-scripts.tar
   ```

2. 次のディレクトリに移動します。

   ```
   cd /home/stack/nbos-cfg-scripts/
   ```

3. nbosjm の仮想環境をアクティブ化します。

   ```
   source /home/stack/myansible/bin/activate
   ```

4. delete_snapshots.pyスクリプトを実行して、スナップショットコピーのみで構成されたリカバリポイントを削除します。

   ```
   python3 delete_snapshots.py delete
   ```

5. 次のコマンドを実行して、スナップショットの削除状態を取得します。

   ```
   python3 delete_snapshots.py get_delete_status
   ```

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 プライマリサーバーの詳細の構成

NetBackup for OpenStack 仮想マシンでプライマリ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。

プライマリ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. プライマリサーバーのホスト名を入力します。
3. サービスプリンシパル ID を入力します。
4. API キーを入力します。
5. ［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。
6. ［送信 (Submit)］をクリックします。
7. ［Ansible 出力 (Ansible Output)］タブでは、NetBackup プライマリ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 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 ログのダウンロード

NetBackup for OpenStack コンフィギュレータ UI から NetBackup for OpenStack ログを直接ダウンロードできます。

NetBackup for OpenStack コンフィギュレータ UI を使用してログをダウンロードするには

1. NetBackup for OpenStack コンフィギュレータ UI にログオンします。
2. ［ログ (Logs)］に移動します。
3. ダウンロードするログを選択します。
   - NetBackup for OpenStack Appliance のログは個別にダウンロードできます。
   - 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/`

API キーの更新

全体の再構成を実行しなくても、NetBackup サービスプリンシパルを更新できます。これは、サービスプリンシパルの有効期限が切れている場合、または最初に構成されたサービスプリンシパルが失効している場合に特に便利です。

API キーを更新する方法

1. NetBackup for OpenStack コンフィギュレータ UI にログオンします。
2. 左側で［API キー (API Key)］をクリックします。
3. ［API キーの検証 (API Key Validation)］で、サービスプリンシパル ID と API キーを更新します。
4. ［送信 (Submit)］をクリックします。

API 証明書のアップロード

HTTPS を使用して OpenStack クラウドが構成されている場合、OpenStack クラウド CA 証明書をアップロードできます。

API キーを更新する方法

1. NetBackup for OpenStack コンフィギュレータ UI にログオンします。
2. 左側で［API 証明書 (API Certificate)］をクリックします。
3. ［認証局 (Certificate Authorities)］をクリックして、証明書ファイルをアップロードします。

4

NetBackup プライマリサーバーの構成

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 Web UI からの OpenStack Horizon UI の起動について
- NBOSVM サービスプリンシパルの構成
- NetBackup for OpenStack 保護計画について
- NetBackup for OpenStack での自動イメージレプリケーションについて

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 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.98 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。
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.98 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.99 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 にサインインします。

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。

NBOSVM サービスプリンシパルの構成

NBOSVM と NetBackupの間で安全な通信を行うために、サービスプリンシパルを構成する必要があります。

NBOSVM サービスプリンシパルの構成

1 NetBackup プライマリサーバーに root 以外のユーザーを作成します。

```
adduser <username>
```

2 NetBackup プライマリサーバーの Web UI にログインします。

3 左側のメニューから、［セキュリティ (Security)］、［RBAC］、［デフォルトのセキュリティ管理者 (Default Security Administrator)］の順に移動します。

4 ［ユーザー (Users)］タブで、作成した root 以外のユーザーを追加します。

5 ［セキュリティ (Security)］、［アクセスキー (Access keys)］の順に移動します。

6 ［追加 (Add)］をクリックし、root 以外のユーザーを入力してアクセストークンを作成します。

7 生成されたアクセストークンと NetBackupHostName を cURL コマンドに追加し、NetBackup プライマリサーバーで実行します。

```
curl --insecure --location --request POST  ¥

'https://<NetBackupHostName>:1556/netbackup/security/service-principal-configs'
 ¥
  -H 'accept: application/vnd.netbackup+json;version=11.0' ¥
  -H 'Content-Type: application/vnd.netbackup+json;version=11.0'
 ¥
  -H 'Authorization: <Access Token>' ¥
  -d '{
  "data": {
    "type": "servicePrincipalConfiguration",
    "attributes": {
      "servicePrincipalId": "Service_Principal_NBOSVM",
      "servicePrincipalType": "OPENSTACK",
      "servicePrincipalApiKeyExpireAfterDays": "P365D",
      "isSecurityAdmin": true,
      "accessDefinitions": [

        {
          "namespace": "|SECURITY|USERS|API-KEYS|",
          "operations": [

            "|OPERATIONS|VIEW|"
          ]
        },
        {
          "namespace": "|SECURITY|SERVICE-PRINCIPAL|",
          "operations": [

            "|OPERATIONS|VIEW|"
          ]
        },
        {
          "namespace": "|ASSETS|OPENSTACK|",
          "operations": [
            "|OPERATIONS|ADD|",
            "|OPERATIONS|VIEW|",
             "|OPERATIONS|UPDATE|",
            "|OPERATIONS|ASSETS|OPENSTACK|RESTORE_ORIGINAL|",
            "|OPERATIONS|ASSETS|OPENSTACK|RESTORE_ALTERNATE|",
```

```
    "|OPERATIONS|ASSETS|OPENSTACK|PROTECT|"
  ]
},
{
  "namespace": "|PROTECTION|PROTECTION_PLAN|",
  "operations": [
    "|OPERATIONS|VIEW|",
    "|OPERATIONS|PROTECTION|PROTECTION_PLAN|SUBSCRIBE|"
  ]
},
{
  "namespace": "|PROTECTION|POLICIES|",
  "operations": [
    "|OPERATIONS|PROTECTION|POLICIES|MANUAL-BACKUP|",
    "|OPERATIONS|VIEW|"
  ]
},
{
  "namespace": "|CREDENTIALS|",
  "operations": [

    "|OPERATIONS|ADD|",
    "|OPERATIONS|UPDATE|",
    "|OPERATIONS|DELETE|"
  ]
},
{
  "namespace": "|MANAGE|NBOSVM-SERVER|",
  "operations": [
    "|OPERATIONS|ADD|",
    "|OPERATIONS|UPDATE|",
     "|OPERATIONS|DELETE|"
  ]
},
{
  "namespace": "|MANAGE|JOBS|",
  "operations": [
    "|OPERATIONS|ADD|",
    "|OPERATIONS|VIEW|"
  ]
},
{
  "namespace": "|STORAGE|STORAGE-SERVERS|",
```

```
            "operations": [
              "|OPERATIONS|VIEW|"
            ]
          },
          {
            "namespace":
"|STORAGE|STORAGE-SERVERS|UNIVERSAL-SHARES|",
            "operations": [
              "|OPERATIONS|VIEW|"
            ]
          },
          {
             "namespace": "|MANAGE|IMAGES|",
             "operations": [
               "|OPERATIONS|VIEW|"
            ]
          }
        ]
      }
    }
}'
```

メモ: cURL の応答から、`servicePrincipalId` と `apiKey` に関するメモを保存します。これらは NetBackup for OpenStack 構成に必要です。

`service-principal-configs` API について詳しくは、NetBackup API マニュアルを参照してください。

NetBackup for OpenStack 保護計画について

NetBackup の Web UI で、保護計画を作成する必要があります。

保護計画の作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。

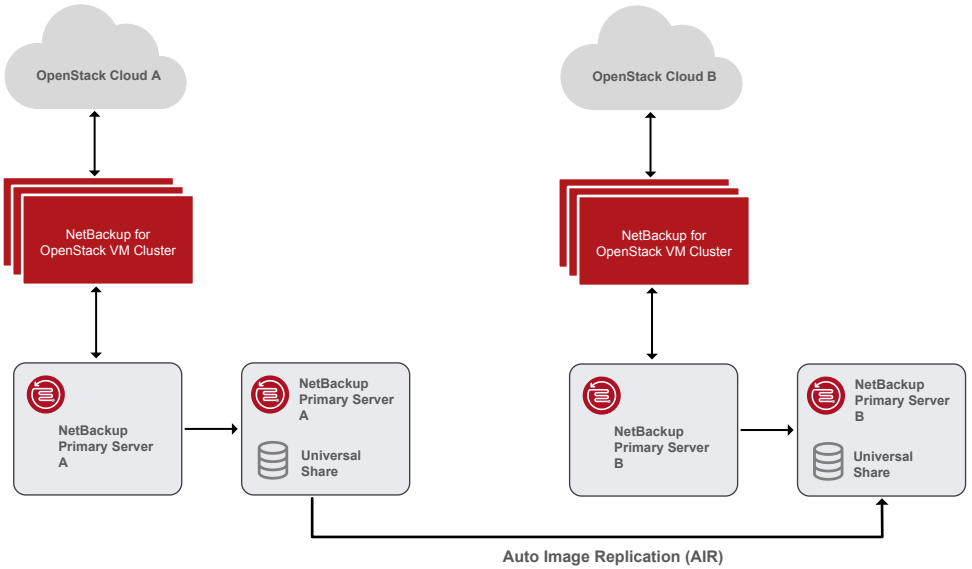
NetBackup for OpenStack での自動イメージレプリケーションについて

1 つの NetBackup ドメインで生成されたバックアップは、1 つ以上のターゲット NetBackup ドメインのストレージにレプリケートできます。この処理は自動イメージレプリケーション (AIR) と呼ばれます。

NetBackup for OpenStack 10.5 以降のバージョンでは、1 つの NetBackup ドメインのメディアサーバー重複排除プール (MSDP) から、別のドメインの MSDP への AIR がサポートされます。NetBackup は、AIR 操作を管理するソースドメインとターゲットドメインでストレージライフサイクルポリシー (SLP) を使用します。

次の図は、OpenStack Cloud A と OpenStack Cloud B 間で AIR を使用するアーキテクチャを示しています。NetBackup メディアサーバー A に格納されているバックアップイメージは、NetBackup メディアサーバー B にレプリケートされます。

図 4-1 自動イメージレプリケーション



p.104 の「NetBackup for OpenStack での AIR の構成 」を参照してください。

NetBackup for OpenStack での AIR の構成

2 台の NetBackup プライマリサーバー間で AIR を構成すると、ソース NetBackup プライマリサーバーからのバックアップコピーが、ターゲット NetBackup プライマリサーバーにレプリケートされます。すべての保護、リカバリポイント、必要なメタデータをインポートできます。保護をインポートした後、古いバックアップコピーからインスタンスをリカバリできます。

NetBackup for OpenStack で AIR を構成するには

1. NBOSVM コンフィギュレータ UI を使用して、ソースプライマリサーバーで NBOSVM を構成します。
2. ソースとターゲットの NetBackup プライマリサーバー間で信頼関係を作成します。

   『NetBackup 重複排除ガイド』の「自動イメージレプリケーション (A.I.R.) の構成」トピックを参照してください。
3. ソース NetBackup プライマリサーバーで、レプリケーションターゲットを追加します。

   『NetBackup 重複排除ガイド』の「MSDP レプリケーションターゲットの設定」トピックを参照してください。
4. ターゲット NetBackup プライマリサーバーでインポート SLP を作成します。

   『NetBackup 重複排除ガイド』の「A.I.R. のストレージライフサイクルポリシー (SLP) の構成」トピックを参照してください。
5. ソース NetBackup プライマリサーバーでレプリケーション SLP を作成します。

   『NetBackup 重複排除ガイド』の「A.I.R. のストレージライフサイクルポリシー (SLP) の構成」トピックを参照してください。
6. ソース NetBackup プライマリサーバーで保護計画を作成します。
7. 保護計画を使用して、Horizon UI で保護を作成します。
8. バックアップジョブを実行します。

ターゲット NBOSVM でイメージを取得するには

1. ターゲット NBOSVM で、ユニバーサル共有に格納されているバックアップイメージを使用して、NetBackup から保護をインポートします。

   ```
   nbosjm protection-import-to-new-cloud
   ```

   保護は孤立した保護として一覧表示されます。OpenStack クラウド A のプロジェクトとユーザーが、OpenStack クラウド B に存在しません。

   メモ: 別のクラウドに保護をインポートした後、グローバルジョブスケジューラを有効にすると、保護にインスタンスが接続されていないため、スケジューラの信頼が有効になっているすべての保護が破損していると表示されます。保護を更新してインスタンスを割り当て、スケジューラの信頼を有効にします。
2. 孤立した保護を一覧表示します。

   孤立した保護は、クラウド内のアクティブなテナントまたはユーザーにリンクされなくなった保護です。現在のクラウド環境に関連付けられた `tenant_id` または `user_id` がないすべての孤立した保護を識別して一覧表示するには、次のコマンドを実行します。

```
nbosjm protection-get-orphaned-protections-list [--migrate_cloud
{True,False}]
```

- `--migrate_cloud` 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。デフォルト値は `False` です。

3 新しいテナントまたはユーザーに保護を割り当てます。

```
nbosjm protection-reassign-protections [--old_tenant_ids
<old_tenant_id>]
                                       [--new_tenant_id
<new_tenant_id>]
                                       --protection_plan_id
<protection_plan_id>
                                       [--user_id <user_id>]
                                       [--migrate_cloud
{True,False}]
                                       [--map_file <map_file>]
```

- `--old_tenant_ids` 保護の割り当て元である古いテナントの ID。
- `--new_tenant_id` 保護の割り当て先である新しいテナントの ID。
- `--protection_plan_id` 保護の割り当て先である保護計画の ID。
- `--user_id` 保護の割り当て先であるユーザーの ID。
- `--migrate_cloud` 他のクラウドからも保護を割り当てる場合は、`True` に設定します。デフォルトの値は `False` です。
- `--map_file` マップファイルのファイル名を持つファイルパス。ファイル形式は YAML です。

4 次のコマンドを実行して、インポートジョブの状態を表示します。

```
nbosjm get-protection-import-status
```

5

NetBackup for OpenStack の保護

この章では以下の項目について説明しています。

保護について

保護とは、構成に従って OpenStack 仮想マシンを保護するバックアップジョブです。必要な数の保護を作成できますが、1 つの保護に関連付けられるのは 1 台の仮想マシンのみです。

保護のリスト

Horizon の使用

Horizon でプロジェクトのすべての利用可能な保護を表示する方法

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

Horizon の概要には、すべての保護が次の追加情報と一緒に一覧表示されます。

- 作成時刻
- 保護名
- 保護の説明
- この保護内の合計リカバリポイント
  - 成功したリカバリポイントの合計数
  - 失敗したリカバリポイントの合計数
- 保護の説明
- 保護タイプ
- 保護状態
- スケジューラの信頼
  - 「確立済み」は、スケジューラが保護を有効にするかどうかを示します。

CLI の使用

```
nbosjm protection-list [--all {True,False}]
```

- `--all {True,False}` すべてのプロジェクトのすべての保護を一覧表示します。admin ユーザーのみに有効です。

保護の作成

Horizon の使用

Horizon 内に保護を作成するには、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)]、[保護 (Protection)]の順に移動します。
2. [保護の追加 (Add protection)]をクリックします。
3. [詳細 (Details)]タブで、保護の名前、説明、および形式 (シリアルまたはパラレル) を指定します。
4. [インスタンス (Instances)]タブで、保護する仮想マシンを選択します。
5. [保護計画 (Protection Plan)]タブで、ドロップダウンリストから保護計画を選択します。

6 [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、スナップショット/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。

7 [オプション (Options)]タブでは、スナップショットの作成中に仮想マシンを一時停止できます。[VM を一時停止(Pause VM)]を選択します。

8 [作成 (Create)]をクリックします。

作成された保護は数秒後に利用可能になり、指定されたスケジュールと保護計画に従ってバックアップの作成を開始します。

CLI の使用

```
nbosjm protection-create [--protection-plan-id <protection plan_id>]

      [--instance <instance-id=instance-uuid>]
      [--display-name <display-name>]
      [--display-description <display-description>]
      [--protection-type-id <protection-type-id>]
      [--source-platform <source-platform>]
      [--jobschedule <key=key-name>]
      [--metadata <key=key-name>]
```

- --protection-plan-id 保護と関連付ける保護計画 ID。
- --display-name 保護名。
- --display-description 保護の説明。
- --protection-type-id 保護タイプ ID。
- --source-platform 保護ソースプラットフォームが必要です。openstack はサポート対象のプラットフォームです。
- --instance 保護に含めるインスタンスを指定します。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"
```

- --metadata 保護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。

保護の概要

保護に関する情報を保護の概要に表示します。

Horizon の使用

Horizon 内に保護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)]、[保護 (Protection)]の順に移動します。
2. 表示する保護を特定します。
3. 保護名をクリックすると、保護の概要が表示されます。

詳細

[保護の詳細 (Protection Details)]タブには、保護に関する次の情報が表示されます。

- 名前
- 説明 (Description)
- 可用性ゾーン (Availability Zone)
- 作成日
- 最終更新日
- 保護 ID
- 保護タイプ
- 保護計画名
- 保護計画 ID
- プロジェクト ID
- ユーザー ID
- 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 ゲストエージェントの状態は、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。

保護対象の仮想マシンのリストから、保護対象の仮想マシンに直接移動できます。

リカバリポイント

[リカバリポイント (Recovery Point)]タブには、選択した保護で利用可能なすべてのリカバリポイントのリストが表示されます。

コピーはリカバリポイントに対して表示されます。これらのコピーには、スナップショット、バックアップ、複製のコピーを指定できます。

p.115 の「リカバリポイントについて」を参照してください。

保護計画	[保護計画 (Protection Plan)]タブには、現在構成されているスケジューラと保持保護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 ■ 繰り返す間隔 ■ 次回のスナップショット実行までの時間 ■ バックアップ保持期間 ■ バックアップ保持期間 ■ 複製

CLI の使用

```
nbosjm protection-show <protection-id>
[--verbose <verbose>]
[--scheduler_trust <scheduler_trust {true}>]
```

- `<protection-id>` 表示する保護の ID または名前。
- `--verbose` 保護についての追加情報を表示するオプション。
- `--scheduler_trust` スケジュールが有効またはそうでない保護を表示します。

保護の編集

変更するニーズに合わせて、すべてのコンポーネントで保護を変更できます。

メモ: 保護を編集すると、ユーザーが新しい所有者として設定されます。

Horizon の使用

保護を編集するには

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. 変更する保護を特定し、ドロップダウンリストから[保護の編集 (Edit Protection)]を選択します。
3. 必要に応じて保護を修正します。保護形式を除くすべてのパラメータを変更できます。
4. [更新 (Update)]をクリックします。

CLI の使用

```
nbosjm protection-modify [--display-name <display-name>]
                         [--display-description <display-description>]

                           [--instance <instance-id=instance-uuid>]
                           [--jobschedule <key=key-name>]
                           [--metadata <key=key-name>]
                          [--protection-plan-id <protection_plan_id>]

                           <protection-id>
```

- `--display-name` 保護名。
- `--display-description` 保護の説明。
- `--instance <instance-id=instance-uuid>` 保護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。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適用されます。

  ```
  "start_date" : "06/05/2014"
  "end_date" : "07/15/2014"
  "start_time" : "2:30 PM"
  ```

- `--metadata` 保護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。
- `--protection-plan-id` 保護の ID。
- `<protection-id>` 編集する保護の ID。

保護の削除

保護が不要になった場合は、その保護を削除できます。保護を削除する前に、すべてのリカバリポイントを期限切れにする必要があります。

p.115 の「リカバリポイントについて」を参照してください。

Horizon の使用

保護を削除するには

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. 変更する保護を特定し、ドロップダウンリストから[保護の削除 (Delete Protection)]を選択します。
3. もう一度[保護の削除 (Delete Protection)]をクリックして確定します。

CLI の使用

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

- `<protection-id>` 削除する保護の ID。
- `--database_only` 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。デフォルト値は False です。

保護のロックを解除する

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保護は、以降のタスクのためにロックされます。必要に応じて強制的に保護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します。

Horizon の使用

保護のロックを解除するには

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. 変更する保護を特定し、ドロップダウンリストから[保護のロック解除 (Unlock Protection)]を選択します。
3. もう一度[保護のロック解除 (Unlock Protection)]をクリックして確定します。

CLI の使用

```
nbosjm protection-unlock <protection-id>
```

- `<protection-id>` ロック解除する保護の ID。

6

OpenStack のスナップショット、バックアップ、およびリストアの実行

この章では以下の項目について説明しています。

リカバリポイントについて

リカバリポイントは、すべてのデータとメタデータを含む保護の単一の NetBackup for OpenStack バックアップです。保護が保護するすべての仮想マシンの情報が含まれます。

リカバリポイントのリスト

Horizon の使用

リカバリポイントのリストを表示する方法

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. 詳細を表示する保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。

   選択した保護のリカバリポイントのリストには、次の追加情報が含まれています。

   - 作成時刻
   - リカバリポイントの名前
   - リカバリポイントの説明
   - このリカバリポイントからのリストアの数
     - 成功したリストアの数
     - 失敗したリストアの数

- 状態 (Status)
- コピー
- 処理

CLI の使用

```
nbosjm recovery-point-list [--protection-id <protection-id>]
                           [--nbos_node <host>]
                           [--date_from <date_from>]
                           [--date_to <date_to>]
                           [--all {True,False}]
```

- `--protection-id` 結果を protection-id (保護 ID) でフィルタ処理します。
- `--nbos_node` NetBackup for OpenStack ノードでスケジュール設定されているすべてのリカバリポイント操作を一覧表示します。デフォルト値は None です。
- `--date_from YYYY-MM-DDTHH:MM:SS` という形式の開始日。たとえば、2016-10-10T00:00:00。時間を指定しない場合、デフォルトでは 00:00 となります。
- `--date_to YYYY-MM-DDTHH:MM:SS` という形式の終了日。デフォルトは今日の日付です。同じ日にリカバリポイントを取得する時間を `HH:MM:SS` 形式で指定します。
- `--all` すべてのプロジェクトのすべてのリカバリポイントを一覧表示します。admin ユーザーのみに有効です。

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

保護の概要と保護スナップショットのリストページからスナップショットを作成できます。

保護の概要からスナップショットを作成するには

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. スナップショットを作成する保護を特定します。

3 ［今すぐバックアップ (Backup Now)］をクリックしてスナップショットを作成します。

4 スナップショットの名前と説明を入力します。

5 ［作成 (Create)］をクリックします。

保護スナップショットからスナップショットを作成するには

1 Horizon コンソールで、［NBOS バックアップ (NBOS Backups)］、［保護 (Protection)］の順に移動します。

2 スナップショットを作成する保護を特定します。

3 保護名をクリックして、保護の概要を入力します。

4 ［リカバリポイント (Recovery Points)］タブで、［今すぐバックアップ (Backup Now)］をクリックします。

5 スナップショットの名前と説明を入力します。

6 ［作成 (Create)］をクリックします。

CLI の使用

```
nbosjm protection-snapshot [--display-name <display-name>]
                           [--display-description
<display-description>]
                           <protection-id>
```

- `<protection-id>` スナップショットを作成する保護の ID。
- `--display-name` スナップショットの名前。
- `--display-description` スナップショットの説明。

スナップショットとバックアップの概要

各リカバリポイントには、スナップショットとバックアップコピーに関する情報が含まれます。この情報はリカバリポイントの概要に表示されます。

スナップショット操作の完了後に、nova-booted インスタンスを計算ノードから別の計算ノードに移行した場合、スナップショットコピーからのバックアップまたはリストアはサポートされません。

バックアップコピーがファイルリカバリマネージャインスタンスにマウントされている場合、ファイルリカバリマネージャインスタンスのバックアップを作成するには、バックアップコピーのマウントを解除する必要があります。

Horizon の使用

リカバリポイン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)]、[保護 (Protection)]の順に移動します。
2. 表示するリカバリポイントを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。
5. リカバリポイントリストで検索されたリカバリポイントを特定します。
6. リカバリポイント名をクリックします。

詳細

[リカバリポイントの詳細 (Recovery Points Details)]タブには、リカバリポイントに関する次の情報が表示されます。

- ID、名前、説明
- スケジュールされている日付
- 合計ボリュームサイズ
- 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所要時間
- スナップショットの状態
- バックアップサイズ (Backup Size)
- バックアップにかかる時間
- バックアップの状態
- バックアップ形式
- リカバリポイントの一部である仮想マシン
- リカバリポイントの仮想マシンごとに、次の情報が表示されます。
  - 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)、デバイスパス
  - その他 - VM の元の ID

リストア

[リストア (Restores)]タブには、選択したリカバリポイントから開始されたリストアのリストが表示されます。リストアはここから開始できます。

p.120 の「リストアについて」を参照してください。

その他

[その他 (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
- ID
- スナップショットを含む保護の保護 ID

CLI の使用

```
nbosjm recovery-point-show [--output <output>] <recovery_point_id>
```

- <recovery_point_id> 表示するリカバリポイントの ID。
- --output <output> 追加のスナップショットの詳細を取得するオプション。
  リカバリポイントのメタデータの場合は --output metadata を指定します。
  スナップショット仮想マシンネットワークの場合は --output networks を指定します。
  スナップショット仮想マシンディスクの場合は --output disks を指定します。
  すべてのコピー (スナップショット、バックアップおよび複製コピー) を一覧表示するには、--output copies 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。

リカバリポイントの有効期限

リカバリポイントが期限切れになると、イメージクリーンアップ操作がプライマリサーバーからトリガされます。この操作は、リカバリポイントの一部であるボリュームスナップショットもクリーンアップします。

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 または保護 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 --recovery_point_id <recovery_point_id>
nbosjm volume-snapshot-cleanup --protection_id <protection_id>
```

- <recovery_point_id> ボリュームスナップショットのクリーンアップを実行するリカバリポイントの ID。
- <protection_id> ボリュームスナップショットのクリーンアップを実行する保護の ID。

メモ: recovery_point_id オプションと protection_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 が保護に関連付けられている必要があります。

リストアについて

リストアは、NetBackup for OpenStack のスナップショット、バックアップ、複製のコピーからバックアップ済みの仮想マシンを戻すワークフローです。

メモ: スナップショット操作の完了後に、nova-booted インスタンスを計算ノードから別の計算ノードに移行した場合、スナップショットからのバックアップまたはリストアはサポートされません。

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、4 つの異なる保護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。これらの保護を使用して、4 台の仮想マシンのバックアップを作成します。スナップショットまたはバックアップコピーからインスタンスをリストアすると、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

リカバリポイン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)]、[保護 (Protection)]の順に移動します。
2. 表示するリカバリポイントを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。
5. リカバリポイントリストのリカバリポイントを特定します。

6. リカバリポイン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 [--recovery_point_id <recovery_point_id>]
```

- `--recovery_point_id` リカバリポイントの ID によって結果をフィルタ処理します。

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)］、［保護 (Protection)］の順に移動します。
2. 表示するスナップショットを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. ［リカバリポイント (Recovery Points)］タブに移動します。
5. リカバリポイントリストのリカバリポイントを特定します。
6. リカバリポイン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、リストアに関する次の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。

- リストアされた仮想マシンのリスト
  - リストアされた仮想マシン名
  - リストアされた仮想マシンの状態
  - リストアされた仮想マシン ID
- NetBackupコピー番号 (Copy Number)
- NetBackup コピー形式 (Copy Type)

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
- リストアを含むリカバリポイント ID
- 保護 (Protection)

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>` 追加のリストアの詳細を取得するオプション。
  リストアメタデータの場合は `-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、保護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

サブメニューを使用した単一のリストアの削除

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. 削除するリカバリポイントを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。
5. リカバリポイントリストで検索されたリカバリポイントを特定します。
6. リカバリポイン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。

リカバリポイン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

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. 表示するリカバリポイントを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。
5. リカバリポイントリストで検索されたリカバリポイントを特定します。
6. リカバリポイント名をクリックしてリカバリポイントを入力します。
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

継続的なリストアは、コマンドラインを使用して取り消すことができます。

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またはバックアップからすべての VM を戻します。これらは同じデータセンターの同じクラスタに配置され、同じストレージドメインを使用し、同じネットワークに接続し、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 を保護するために保護を自動的に更新します。

メモ: スナップショットまたはバックアップ時に存在したインスタンスのプロパティがリストア時に存在しない場合、ワンクリックリストアは失敗します。

Horizon の使用

ワンクリックリストアを実行する方法

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. リストアするリカバリポイントを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery points)]タブに移動します。
5. リストアするリカバリポイントを特定します。
6. 特定されたリカバリポイントと同じ行の[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。

CLI の使用

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

                          <recovery_point_id>
                          <copy_number>
                          <copy_type>
```

- <recovery_point_id> リストアするリカバリポイントの ID。
- <copy_number> リストア用のスナップショットまたはバックアップのコピー番号。
- <copy_type> リストアするスナップショットまたはバックアップのコピー形式を指定します。
- --display-name リストアの省略可能な名前。
- --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。

- リストアされる仮想マシン。
- リストアされた仮想マシンの名前
- 接続先のネットワーク。
- 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

選択的リストアを実行するには

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. リストアするリカバリポイントを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery points)]タブに移動します。
5. リストアするリカバリポイントを特定します。
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。

CLI の使用

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

                           [--filename <filename>]
                           <recovery_point_id>
```

- `<recovery_point_id>` リストアするリカバリポイントの ID。
- `--display-name` リストアの省略可能な名前。
- `--display-description` リストアの省略可能な説明。
- `--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、`/home/stack/myansible/lib/python3.8/site-packages/nbosjmclient/input-files/restore_from_backup_copy.json` ファイルを読み取ります。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 で状態を確認します。

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仮想マシンが必要な場合は、他のいずれかのリストアオプションを使用します。

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。

メモ: インプレースリストアはスナップショットからのリストアをサポートしません。

メモ: バックアップ時に存在したインスタンスのプロパティがリストア時に存在しない場合、インプレースリストアは失敗します。

Horizon の使用

インプレースリストアを実行する方法

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. リストアするリカバリポイントを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。
5. リストアするリカバリポイントを特定します。
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。

CLI の使用

```
nbosjm inplace-restore [--display-name <display-name>]
                       [--display-description <display-description>]

                        [--filename <filename>]
                        <recovery_point_id>
```

- `<recovery_point_id>` バックアップコピーからリストアするリカバリポイントの ID。
- `--display-name` リストアの省略可能な名前。
- `--display-description` リストアの省略可能な説明。

- --filename 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。デフォルトでは、/home/stack/myansible/lib/python3.8/site-packages/nbosjmclient/input-files/restore_from_backup_copy.json ファイルを読み取ります。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。

CLI に必要な restore.json ファイル

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リカバリポイントの概要に収集できます。

```
{
  'name': 'sel-rest-5',
  'description': 'sel-rest-desc-5',
  'oneclickrestore': False,
  'restore_type': 'selective',
  'copy_number': '2',
  'copy_type': 'BACKUP',
  'type': 'openstack',
 'openstack':
   {
    'restore_topology':False,
    'instances':
      [
        {
          'id': '91a26084-7134-4ae4-970c-8203fb18669f',
          'name': 'sample-instance-restore',
          'restore_boot_disk': True,
          'availability_zone': 'nova',
          'include': True,
          'vdisks':
          [
             {
               'id': 'c6fe8309-a95b-4bbb-9d72-57beafe4a3ae',
               'new_volume_type': '__DEFAULT__',
               'availability_zone': 'nova'
             }
```

```
            ],
            'nics':
            [
               { 'id': 'd8680981-2113-45a8-aa7c-6edd68c97819',
                 'mac_address': 'fa:16:3e:d1:ce:ae',
                 'network': {
                    'id': 'd8680981-2113-45a8-aa7c-6edd68c97819',
                    'subnet': {
                      'id': '28206b2e-0a0e-46a3-9034-9d621b4bfb4f'
                    }
                 },
                 'ip_address': '172.20.2.230'
               }
            ]
          }
       ],
      'networks_mapping': {
        'networks': [
            {'snapshot_network': {
                 'name': 'private',
                 'id': 'd8680981-2113-45a8-aa7c-6edd68c97819',
                 'subnet': {
                     'id': '28206b2e-0a0e-46a3-9034-9d621b4bfb4f'
                 }
                },
             'target_network': {
                 'id': 'd8680981-2113-45a8-aa7c-6edd68c97819',
                 'name': 'private',
                 'subnet': {
                     'id': '28206b2e-0a0e-46a3-9034-9d621b4bfb4f'
                 }
             }
            }
        ]
      }
    }
}
```

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。このオプションを 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。
- copy number バックアップコピーの番号。
- copy_type データの形式。

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、リストアするリカバリポイン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 インスタンスが起動する 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':[
         ]
      }
   }
}
```

バックアップマウントについて

NetBackup for OpenStack では、バックアップコピーからファイルを表示またはダウンロードできます。バックアップコピー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、バックアップコピー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。バックアップコピー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 や RHEL 8.2 以降などの 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。大きいバックアップコピーはより多くの RAM を必要とすることがあります。

RHEL 8.2 以降の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-ga.conf` ファイルを生成します。

   ```
   qemu-ga -D > /etc/qemu/qemu-ga.conf
   ```

4. ファイルに次の行を追加します。

   ```
   fsfreeze-hook=/etc/qemu/fsfreeze-hook
   ```

5. qemu-guest-agent サービスを再起動します。
6. Python 3 をインストールします。

   ```
   apt-get install python3
   ```

7. インスタンスを再起動します。

バックアップコピーのマウント

File Recovery Manager にバックアップコピーをマウントすると、マウントされたバックアップコピー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。

マウントされたバックアップ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。保持ポリシーはマウントされたバックアップをパージしません。

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。

このマウント処理中、OpenStack インスタンスは再起動されます。

バックアップは常に File Recovery Manager インスタンスにのみマウントします。

メモ: ミラーボリュームは、ファイルリカバリマネージャインスタンスに自動的にマウントされません。ミラーボリュームは手動でマウントする必要があります。

バックアップコピーをマウントする方法

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. マウントするバックアップを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。

5 リカバリポイントの行の右側にある[コピー (Copies)]をクリックします。

6 バックアップコピーを特定し、ドロップダウンリストから[ワンクリックリストア (One Click Restore)]を選択します。

7 [ファイルリストアのためのマウント (Mount for file restore)]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場合、File Recovery Manager イメージに次のプロパティセットがあることを確認します。

```
nbos_recovery_manager=yes
```

CLI の使用

```
nbosjm backup-mount <mount_vm_id> <copy_number> <recovery_point_id>
```

- `<mount_vm_id>` バックアップボリュームがマウントされる VM ID。
- `<copy_number>` バックアップマウントのコピー番号を指定します。
- `<recovery_point_id>` マウントするリカバリポイントの 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。

マウントされたバックアップコピーは次のパスにあります。

```
/home/ubuntu/nbos-mounts/mounts/
```

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。

マウントされたバックアップの識別

バックアップコピー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バックアップの識別には、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バックアップの ID が含まれます。

メモ: この値は、新しいバックアップがマウントされたときにのみ更新されます。

リカバリポイントリストから

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. マウントするバックアップを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。
5. リカバリポイントの行の右側にある[コピー (Copies)]をクリックします。
6. [バックアップのマウント解除 (Unmount Backup)]オプションを指定したバックアップコピーを検索します。

CLI の使用

```
nbosjm backup-mounted-list
```

- マウントされているすべてのバックアップのリスト。

バックアップのマウント解除

マウントされたバックアップが不要になったら、バックアップをマウント解除することをお勧めします。

バックアップをマウント解除すると、次のバックアップ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バックアップがパージされます。

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。バックアップは、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)]、[保護 (Protection)]の順に移動します。
2. マウント解除するバックアップを含む保護を特定します。
3. 保護名をクリックして、保護の概要を入力します。
4. [リカバリポイント (Recovery Points)]タブに移動します。
5. リカバリポイントの行の右側にある[コピー (Copies)]をクリックします。
6. バックアップコピーを特定し、[バックアップのマウント解除 (Unmount Backup)]をクリックします。

CLI の使用

```
nbosjm backup-dismount <recovery_point_id>
```

- `<recovery_point_id>` マウント解除するリカバリポイントの ID。

スケジュールについて

すべての保護には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

スケジュールの有効化または無効化

Horizon とコマンドラインインターフェースを使って、単一の保護のスケジューラを有効または無効にできます。

Horizon を使って単一の保護のスケジューラを有効または無効にするには

1. Horizon コンソールで、[NBOS バックアップ (NBOS Backups)]、[保護 (Protection)]の順に移動します。
2. 変更する保護を識別します。
3. [処理 (Actions)]列のドロップダウンから、[保護の編集 (Edit Protection)]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)]または[無効 (Disabled)]を選択します。
6. [更新 (Update)]をクリックします。

コマンドラインを使って単一の保護のスケジューラを有効または無効にするには

1. 次のコマンドを実行して、スケジューラを有効にします。

```
nbosjm enable-scheduler --protectionids <protectionid>
```

2. 次のコマンドを実行して、スケジューラを無効にします。

```
nbosjm disable-scheduler --protectionids <protectionid>
```

- `--protectionids` 少なくとも 1 つの保護 ID が必要です。スケジュールを有効または無効にするには、保護の 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。

スケジュールの変更

スケジュールを変更するには、保護を変更する必要があります。

p.111 の「保護の編集」を参照してください。

電子メール通知のアクティブ化について

NetBackup for OpenStack はバックアップとリストアのたびに電子メール通知を送信します。保護の所有者に電子メールが送信されます。

電子メール通知をアクティブ化するには、OpenStack 管理者が次の要件を満たしていることを確認する必要があります。

- ユーザー電子メールが割り当てられている
  電子メールが保護の所有者に送信されるため、保護を作成した 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。
- NetBackup for OpenStack メールサーバーが構成されている

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 でメールサーバーを設定できます。

電子メール通知をアクティブ化するには

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)]チェックボックスのチェックマークを付けるか、またははずします。

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。

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 とコマンドラインインターフェースに加えて 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へのアクセス

1. 管理者ユーザーで Horizon コンソールにログインします。
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。

   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。次の情報を提供します。

- 既存の仮想マシンの数と比較した保護対象の仮想マシンの数
- 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。

[サブスクリプション (Subscriptions)]タブ

このタブには、その時点に存在するすべての保護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。

- 保護を所有するユーザー ID。
- 保護を含むプロジェクト。
- サブスクリプション
- 保護タイプ
- 可用性ゾーン (Availability Zone)
- 保護対象の仮想マシンの数
- 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)
- 完全バックアップと増分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
- その保護によって使用されるストレージ。
- 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。
- 保護の一般的な間隔
- 保護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 ■ テナントで保護された仮想マシン ドリルダウンして、保護ごとに同じ情報を表示したり、最後に保護対象の仮想マシンごとに表示できます。 ［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保護と仮想マシンが表示されます。
［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、現在アクティブなコントローラノードの下に表示されます。
［NBOSDM］タブ (NetBackup for OpenStack データムーバーサービス)	このタブには、NetBackup for OpenStack データムーバー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。 ■ 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

[監査 (Audit)]タブ	監査ログは、保護の作成、スナップショットの作成など、ユーザーが実行する保護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。 監査ログで文字列を検索できます。たとえば、特定のユーザーによって実行されたエントリだけを対象にできます。 また、必要に応じて、表示される時間枠を変更できます。
[保護計画 (Protection Plan)]タブ	保護計画を操作するには、[保護計画 (Protection Plan)]タブを使用します。
[設定 (Settings)]タブ	このタブは、クラウド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。 ■ 電子メールの設定 p.147 の「電子メールの設定」を参照してください。 ■ ジョブスケジューラの設定 p.150 の「ジョブスケジューラの有効化または無効化」を参照してください。

電子メールの設定

これらの設定は、ユーザーにリカバリポイン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構成する必要があります。

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。

コマンドラインを使用した電子メール設定の構成

1 電子メール設定を初めてまたは削除後に設定します。

```
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。

2 既存の電子メール設定を更新します。

```
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。

3 既存の電子メール設定を表示します。

```
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。

4 電子メール設定を削除します。

```
nbosjm setting-delete <setting_name>
```

- <setting_name> 削除する設定の名前。

表 7-1 電子メールの設定

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	管理
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有効化または無効化

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。

Horizon を使ってジョブスケジューラを有効または無効にするには

1. 管理者ユーザーで Horizon コンソールにログインします。
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。

コマンドラインを使ってジョブスケジューラを有効または無効にするには

1. グローバルジョブスケジューラの状態を取得します。

```
nbosjm get-global-job-scheduler
```

2. ジョブスケジューラを有効にします。

```
nbosjm enable-global-job-scheduler
```

3. ジョブスケジューラを無効にします。

```
nbosjm disable-global-job-scheduler
```

保護計画

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保護を制御できます。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保護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保護に従った場合、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、NetBackup 管理者が事前定義済みの保護計画を定義でき、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、NetBackup 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。

利用可能な保護計画の一覧表示

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. 管理者ユーザーで Horizon コンソールにログインします。
2. ［管理 (Admin)］、［NBOS バックアップ管理 (NBOS Backup Admin)］、［NetBackupOpenStack］、［保護計画 (Protection Plan)］の順に移動します。

利用可能な各保護計画について、次の情報が表示されます。

- 作成時刻
- 名前
- 説明
- 状態 (Status)
- 間隔 (interval)
- スナップショットとバックアップのオプション
- スナップショットの保持期間
- バックアップの保持期間
- 処理

CLI の使用

```
nbosjm protection-plan-list
```

保護計画へのプロジェクトのサブスクライブ

Horizon の使用

保護計画にプロジェクトをサブスクライブするには、次の手順を実行します。

1. 管理者ユーザーで Horizon コンソールにログインします。
2. ［管理 (Admin)］、［NBOS バックアップ管理 (NBOS Backup Admin)］、［NetBackupOpenStack］、［保護計画 (Protection Plan)］の順に移動します。
3. プロジェクトをサブスクライブまたはサブスクライブ解除する保護計画を特定します。
4. ［プロジェクトのサブスクライブ/サブスクライブ解除 (Subscribe/Unsubscribe Projects)］をクリックします。
5. 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。
6. ［適用 (Apply)］をクリックします。

CLI の使用

```
nbosjm protection-plan-assign [--add_project <project_id>]
                              [--remove_project <project_id>]
                              <protection_id>
```

- `--add_project` 保護計画を割り当てるプロジェクトの ID。
- `--remove_project` 保護計画を削除するプロジェクトの ID。
- `<protection_id>` サブスクライブまたはサブスクライブ解除される保護計画。

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、保護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、コマンドラインを使用してのみ管理できます。

信頼を管理するには

1. すべての信頼を一覧表示します。

   ```
   nbosjm trust-list
   ```

2. 信頼を表示します。

   ```
   nbosjm trust-show <trust_id>
   ```

3. 信頼を作成します。

   ```
   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` 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。

4. 信頼を削除します。

   ```
   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。

メモ: policy-reassign コマンドは NetBackup for OpenStack 10.4 ではサポートされません。

ポリシーのインポート

バックアップターゲットから NetBackup for OpenStack データベースにポリシーをインポートできます。

ポリシーのインポート機能は、クラウド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。

ポリシーをインポートするには

1 インポートできるポリシーのリストを取得します。

```
nbosjm policy-get-importpolicies-list [--project_id <project_id>]
[--storage_type <storage_type>] [--backup_path <backup_path>]
```

- --project_id 指定したプロジェクトのみに属するポリシーを一覧表示します。
- --storage_type ポリシーが格納されるストレージ形式 (S3 または NFS)。
- --backup_path バックアップが格納されるバックアップストレージパス。

S3 の場合、storage_type と backup_path はオプションのパラメータです。

2 ポリシーを NetBackup for OpenStack データベースにインポートします。

```
nbosjm policy-importpolicy [--policies <policyid>] [--storage_type
<storage_type>] [--backup_path <backup_path>]
```

- --policyids 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。
- --storage_type ポリシーが格納されるストレージ形式 (S3 または NFS)。
- --backup_path バックアップが格納されるバックアップストレージパス。

S3 の場合、storage_type と backup_path はオプションのパラメータです。

3 ポリシーが正しくインポートされていることを確認します。

```
./nbosjm ./nbosjm policy-verify-importedpolicies
```

- --policyids ポリシー ID を指定して、ポリシーが正しくインポートされていることを確認します。
- --storage_type ポリシーが格納されるストレージ形式 (S3 または NFS)。
- --backup_path バックアップが格納されるバックアップストレージパス。

S3 ストレージ形式のインポートポリシーコマンドを実行する前に、次の手順を実行します。

1. /etc/nbos/nbosjm.conf ファイルに次の詳細を追加します。

```
vault_s3_auth_version = DEFAULT
 vault_s3_access_key_id = << s3_access_key >>
 vault_s3_secret_access_key = <<s3_secret_access_key>>
 vault_s3_region_name = << s3_region_name >>
 vault_s3_bucket = << vault_s3_bucket >>
 vault_s3_endpoint_url = << vault_s3_endpoint_url >>
 vault_s3_signature_version = default
 vault_s3_ssl = False
 vault_s3_ssl_cert =
 vault_enable_threadpool = True
 vault_s3_support_empty_dir = False
 [s3fuse_sys_admin]
 helper_command = sudo /home/stack/myansible/bin/nbosjm-rootwrap
 /etc/nbosjm/rootwrap.conf privsep-helper
```

2. nbos-object-store サービスを起動します。

```
systemctl start nbos-object-store
```

3. nbos-object-store サービスの状態を確認します。実行中の状態である必要があります。

```
systemctl status nbos-object-store
```

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` 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` ポリシー再割り当て API の入力として使用する YAML ファイル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。

メモ: `policy-get-orphaned-policies-list` コマンドは NetBackup for OpenStack 10.4 ではサポートされません。

8

ディザスタリカバリ

この章では以下の項目について説明しています。

NetBackup for OpenStack のディザスタリカバリについて

障害が発生した場合は、リカバリのために次の手順を実行します。

異なる OpenStack クラウドに対してディザスタリカバリを実行するには

1. NetBackup でディザスタリカバリを実行します。

   『NetBackup トラブルシューティングガイド』の「ディザスタリカバリ」の章を参照してください。

2. NetBackup for OpenStack クラスタを再構成します。

   p.93 の「NetBackup for OpenStack クラスタの再構成」を参照してください。

3. NetBackup for OpenStack VM から保護をインポートします。

   ```
   nbosjm protection-import-to-new-cloud
   ```

   保護は孤立した保護として一覧表示されます。OpenStack クラウド A のプロジェクトとユーザーが、OpenStack クラウド B に存在しません。

4. 孤立した保護を一覧表示します。

   孤立した保護は、クラウド内のアクティブなテナントまたはユーザーにリンクされなくなった保護です。現在のクラウド環境に関連付けられた `tenant_id` または `user_id` がないすべての孤立した保護を識別して一覧表示するには、次のコマンドを実行します。

   ```
   nbosjm protection-get-orphaned-protections-list [--migrate_cloud
   {True,False}]
   ```

- --migrate_cloud 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。デフォルト値は False です。

5 新しいテナントまたはユーザーに保護を割り当てます。

```
nbosjm protection-reassign-protections [--old_tenant_ids
<old_tenant_id>]
                                       [--new_tenant_id
<new_tenant_id>]
                                       --protection_plan_id
<protection_plan_id>
                                       [--user_id <user_id>]
                                       [--migrate_cloud
{True,False}]
                                       [--map_file <map_file>]
```

- --old_tenant_ids 保護の割り当て元である古いテナントの ID。
- --new_tenant_id 保護の割り当て先である新しいテナントの ID。
- --protection_plan_id 保護の割り当て先である保護計画の ID。
- --user_id 保護の割り当て先であるユーザーの ID。
- --migrate_cloud 他のクラウドからも保護を割り当てる場合は、True に設定します。デフォルトの値は False です。
- --map_file マップファイルのファイル名を持つファイルパス。ファイル形式は YAML です。

同じ OpenStack クラウドに対してディザスタリカバリを実行するには

1 NetBackup でディザスタリカバリを実行します。

『NetBackup トラブルシューティングガイド』の「ディザスタリカバリ」の章を参照してください。

2 NetBackup for OpenStack クラスタを再構成します。

p.93 の「NetBackup for OpenStack クラスタの再構成」を参照してください。

3 NetBackup for OpenStack VM から保護をインポートします。

```
nbosjm protection-import
```

4 次のコマンドを実行して、インポートジョブの状態を表示します。

```
nbosjm get-protection-import-status
```

5 保護インポート操作が完了したら、グローバルジョブスケジューラを有効にします。

```
nbosjm enable-global-job-scheduler
```

9

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。ユーザーから保護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。

保護、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 つ以上の保護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 つ以上の保護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、仮想マシン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
```

RHOSP の NetBackup for OpenStack データムーバーサービスログ

RHOSP の NetBackup for OpenStack データムーバーサービスログには次のものがあります。

- nbosdmapi ログ
  NetBackup for OpenStack データムーバー API サービスのログは、NetBackup for OpenStack データムーバー 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 データムーバーサービスのログは、NetBackup for OpenStack データムーバー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
  ```

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 2 に構成されます。

```
VXMS_VERBOSE = 2
```

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 9-1 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 データムーバーサービスログ

Ansible OpenStack の NetBackup for OpenStack データムーバーサービスログには次のものがあります。

- nbosdmapi ログ
  NetBackup for OpenStack データムーバー API サービスのログは、NetBackup for OpenStack データムーバー 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 データムーバー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
  ```

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 2 に構成されます。

```
VXMS_VERBOSE = 2
```

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 9-2 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 の NetBackup for OpenStack データムーバーサービスログ

- nbosdmapi ログ:

NetBackup for OpenStack データムーバー API サービスのログは、NetBackup for OpenStack データムーバー 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 データムーバー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 データムーバー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 データムーバー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
   ```

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。

スナップショットコピーからの選択的リストアが失敗する

スナップショットコピーからの選択的リストアは、nova-booted インスタンスで次のエラーで失敗することがあります。`copy_backup_image_to_volume operation failed.`

OpenStack が新しいインスタンスを作成するために選択した計算ノードまたは Hypervisor が、元のインスタンスが存在する計算ノードと異なる場合、スナップショットコピーからの選択的リストアは失敗します。この場合、バックアップコピーから選択的リストアを実行します。

ユニバーサル共有パスの古い nova ID が原因でバックアップが失敗する

ユニバーサル共有パスに古い nova ID がある場合、バックアップジョブは失敗します。

Horizon UI で、バックアップジョブが次のエラーメッセージで失敗します。

```
Failed taking backup of policy snapshot: 'NoneType' object has no
attribute 'strip'
```

この問題を解決するには

1. 次のサービスを停止します。

```
systemctl stop nbosjm-policies
systemctl stop nbosjm-api
systemctl stop nbosjm-scheduler
systemctl stop nbosjm-cron
```

2. スクリプト /home/stack/nova_userid.shを実行して nova ID を変更します。

```
./nova_userid.sh
```

3. 3. 次のコマンドを実行して、ディレクトリ /etc/nbosjm とマウントディレクトリ (/var/nbos など) のディレクトリ所有権を nova に変更します。

```
chown -R nova:nova <directory_name>
```

4. 次のサービスのみを再起動します。

```
systemctl stop nbosjm-policies
systemctl stop nbosjm-api
systemctl stop nbosjm-scheduler
systemctl stop nbosjm-cron
```

NetBackup for OpenStack での NetBackup サポートユーティリティの使用

NetBackup サポートユーティリティ (nbsu) はコマンドラインツールです。ホストに問い合わせて、NetBackup とオペレーティングシステムに関する適切な診断情報を収集します。

このユーティリティを使用して、NBOSVM に関する診断情報を収集できます。NBOSVM の /var/log/ ディレクトリで生成されるすべてのログファイルを収集し、.tgz ファイルを作成します。この情報を使用して問題をトラブルシューティングできます。

メモ: NetBackup サポートユーティリティは、NBOSVM でのみ実行する必要があります。

NetBackup サポートユーティリティを使用するには

1. NetBackup for OpenStack 仮想マシンにログオンします。
2. ディレクトリを `/usr/openv/netbackup/bin/support` に変更します。
3. NBOSVM の役割でユーティリティを実行します。

   ```
   ./nbsu -r nbosvm
   ```

   `.tgz` ファイルが作成されます。このファイルには、`/var/log` ディレクトリで利用可能なすべてのログが含まれています。

   例: `NBSU_<hostname>_nbosvm_10092023_082422.tgz`

物理ボリュームおよびボリュームグループのメタデータサイズが小さい場合、ボリュームを作成できない

物理ボリュームとボリュームグループ用に指定されたメタデータサイズが十分でない場合、ボリュームを作成できません。

この問題を解決するには、物理ボリュームとボリュームグループを作成するときに十分なメタデータサイズを指定します。

ボリュームのメタデータサイズを確認するには、次のコマンドを実行します。

```
pvdisplay -C -o name,mda_size,mda_free
vgdisplay -C -o name,mda_size,mda_free
```

物理ボリュームまたはボリュームグループの作成時に、次のコマンドを実行してメタデータサイズを設定します。

```
pvcreate –metadatasize <metadata size>
```

次に例を示します。`pvcreate --metadatasize 1g`

DNS サーバーが IP アドレスを解決できない、または IP アドレスが間違っている場合、NBOSVM の構成が失敗する

/etc/hosts ファイルに間違った IP アドレスが設定されている場合、NBOSVM の設定は失敗します。DNS サーバーが IP アドレスを解決できない場合にも失敗します。

NBOSVM コンフィギュレータ UI で、コントローラノードフィールドの IP または短縮名が間違っている場合、NBOSVM の構成は失敗します。

コントローラノードフィールドにあるすべての NBOISVM ノードが正しい IP または短縮名であることを確認します。

複数のストレージサーバーでストレージユニットが作成される場合のエラー

複数のストレージサーバーでストレージユニットを作成するときに、NetBackup がユニバーサル共有が構成されていないストレージサーバーを選択すると、ネットワークエラーが発生する場合があります。

複数のストレージサーバーでストレージユニットを作成する場合は、すべてのストレージサーバーにすべてのメディアサーバーが構成されていることを確認します。

この問題を解決するには

1. NetBackup Web UI を開きます。
2. 左側で[ストレージ (Storage)]、[ディスクストレージ (Disk storage)]の順に選択します。
3. [ストレージサーバー (Storage servers)]タブをクリックします。
4. ストレージサーバーをクリックします。
5. [メディアサーバー (Media servers)]で、ストレージユニットにある他のすべてのメディアサーバーを追加します。
6. 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host properties)]の順に選択します。
7. メディアサーバーを選択し、[メディアサーバーの編集 (Edit media server)]をクリックします。
8. [サーバー (Servers)]、[追加サーバー (Additional servers)]の順に選択し、[追加 (Add)]をクリックして、ストレージユニットにある他のすべてのメディアサーバーを追加します。

OpenStack イメージに OpenStack ユーザーがアクセスできない場合、スナップショットジョブが失敗する

スナップショットジョブをトリガする OpenStack ユーザーが OpenStack イメージにアクセスできない場合、スナップショットジョブは失敗し、次のエラーメッセージが表示されます。

```
Couldn't find the image <image_id> of instance <instance_id> for
snapshot_id <snapshot_id>. Check whether image is present or has
required permission for user <user_id> and project <project_id
```

この問題を解決するには、OpenStack ユーザーが OpenStack イメージにアクセスできることを確認します。

インスタンスに接続されたサブネットが OpenStack ユーザーにアクセスできない場合、ワンクリックリストアが失敗する

ワンクリックリストアをトリガする OpenStack ユーザーが OpenStack インスタンスに接続されているサブネットにアクセスできない場合、ワンクリックリストアは失敗し、次のエラーメッセージが表示されます。

```
Tenant <project_id> not allowed to create port on this network
```

この問題を解決するには、OpenStack ユーザーが、OpenStack インスタンスに接続されたサブネットにアクセスできることを確認します。

NBOSVM コンフィギュレータ UI がプライマリサーバーを検出しない

マスターサーバーの FQDN が NetBackup for OpenStack VM の `/etc/hosts` ファイルに追加されていない場合、NBOSVM コンフィギュレータ UI はプライマリサーバーを検出できません。

この問題を解決するには、NetBackup for OpenStack VM の `/etc/hosts` ファイルにプライマリサーバー名を追加します。

リカバリポイント名がデフォルト名に更新される

1 文字で作成されたリカバリポイントは、自動イメージレプリケーション後にデフォルト名「recovery point」になります。

この問題を解決するには、リカバリ名に 2 文字以上使用していることを確認します。

スタックの更新後に、[NBOS Backups]タブと[NBOS Backup Admin]タブが Horizon UI から消える

OpenStack スタックを更新すると、NetBackup for OpenStack Horizon UI で[NBOS バックアップ (NBOS Backups)]タブと[NBOS バックアップ管理 (NBOS Backup Admin)]タブが表示されなくなります。スタックの更新によって、OpenStack からエンドポイントが誤って削除されます。

この問題を解決するには、ディレクタノードでスクリプト `register_nbopenstack_service.sh` を実行します。このスクリプトはインストールパッケージとともに提供され、次のパスから入手できます: `<download location> /nbos-cfg-scripts/redhat-director scripts/rhosp17.1/register_nbopenstack_service.sh`。

```
sh register_nbopenstack_service.sh {overcloudrc file} {NBOS Protocol} {NBOSVM VIP}
```

例:

```
sh register_nbopenstack_service.sh /home/stack/overcloudrc http 10.xxx.xxx.xx
```

このスクリプトは、Horizon UI に [NBOS バックアップ (NBOS Backups)]タブと[NBOS バックアップ管理 (NBOS Backup Admin)]タブが表示されるように、NetBackup for OpenStack サービスを登録します。

Horizon UI で保護の作成が失敗する場合

保護の作成時に、次のエラーで失敗します。

```
Error: subscription request failed with status 404.
```

NetBackup Web UI で保護計画が削除されているかどうかを確認します。保護計画が削除されている場合は、別の保護計画を使用して保護を作成します。

NBOSVM の再起動後に NetBackup for OpenStack サービスが起動しない

NBOSVM の再起動後に次の NetBackup for OpenStack サービスが起動しない:

- `Nginx`
- `rabbitmq-server`

この問題を解決するには

1 次のコマンドを実行し、3 つの NBOSVM ノードすべてでサービスを有効にして起動します。

```
systemctl enable nginx
systemctl enable rabbitmq-server

systemctl start nginx
systemctl start rabbitmq-server
```

2 NBOSVM ノードのいずれかで次のコマンドを実行し、NBOSVM クラスタサービスを起動します。

```
pcs resource cleanup
pcs resource refresh
```

NBOSVM がコントローラノードの nbosdmapi と通信できない場合

NBOS VM ポートがコントローラノードでブロックされている場合、NBOS VM はコントローラノードの nbosdmapi と通信できません。

NBOS VM が HTTPS で構成されている場合、ポートは 13784 です。NBOSVM が HTTP で構成されている場合、ポートは 8784 です。

すべてのコントローラノードでポートを有効にする方法

1 次のコマンドを実行して DROP iptables ルール行番号を特定します。

```
iptables -L --line-numbers | grep -i DROP
```

2 次のコマンドを実行して、DROP ルールの前に iptables ルールを挿入します。

```
sudo iptables -I INPUT <linenumber> -p tcp -s <nbosvm subnet>
--dport <HTTP/HTTPS port number> -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

たとえば、DROP iptables ルール行番号が 88 の場合、NBOSVM サブネットは 10.xxx.xxx.xx/20 であり、NBOSVM は HTTPS で構成されています。コマンドは次のようになります。

```
sudo iptables -I INPUT 87 -p tcp -s 10.xxx.xxx.xx/20 --dport 13784
-m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
```

OpenStack Keystone 認証エラーのトラブルシューティング

OpenStack Keystone 認証が次のエラーメッセージで失敗します。

```
The request you have made requires authentication. (HTTP 401)
```

この問題を解決するには

1. OpenStack プロジェクトの OpenStack RC ファイルと、問題が表示されるユーザーをソースします。

   ```
   source <OpenStack RC file path>
   ```

   例: `source /home/openrc.sh`

2. OpenStack プロジェクトの信頼 ID と、問題が表示されるユーザーを一覧表示します。

   ```
   nbosjm trust-list
   ```

3. 次のコマンドを実行して、信頼を削除します。

   ```
   nbosjm trust-delete <TrustID>
   ```