NetBackup™ Snapshot Manager for Cloud インストールおよびアップグレードガイド

リリース 11.1

VERITAS
now part of Cohesity

NetBackup™ Snapshot Manager for Cloud インストールおよびアップグレードガイド

最終更新日: 2026-01-22

法的通知と登録商標

Copyright © 2026 Cohesity, Inc. All rights reserved.

Cohesity、Veritas、Cohesity ロゴ、Veritas ロゴ、Veritas Alta、Cohesity Alta、NetBackup 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。

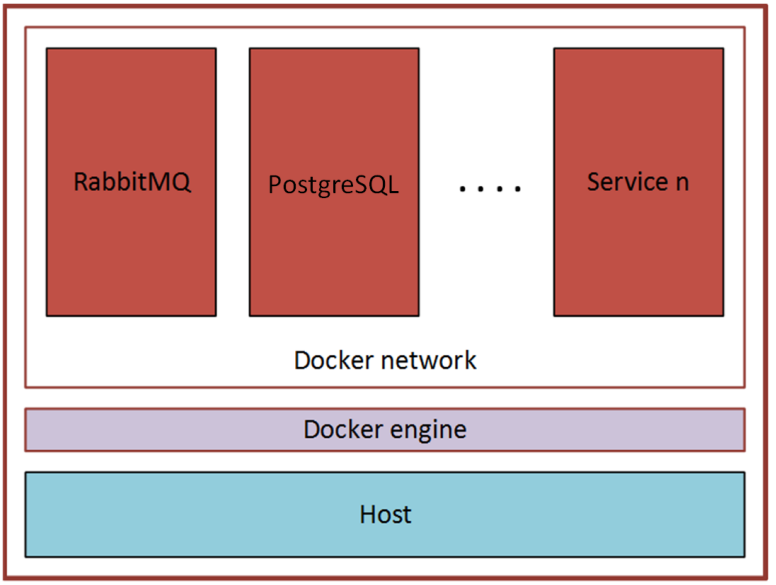
- 配備方法について
- NetBackup Snapshot Manager for Cloud を実行する場所の決定
- クラウドでの NetBackup Snapshot Manager の配備について

配備方法について

NetBackup Snapshot Manager はインストールのマイクロサービスモデルを使用します。Docker イメージをロードして実行すると、NetBackup Snapshot Manager は、各サービスを同じ Docker ネットワーク内の個々のコンテナとしてインストールします。RabbitMQ を使用して、すべてのコンテナが相互に安全に通信します。

2 つの主要なサービスは RabbitMQ と PostgreSQL です。RabbitMQ は NetBackup Snapshot Manager のメッセージブローカーであり、PostgreSQL は NetBackup Snapshot Manager が検出するすべての資産に関する情報を格納します。

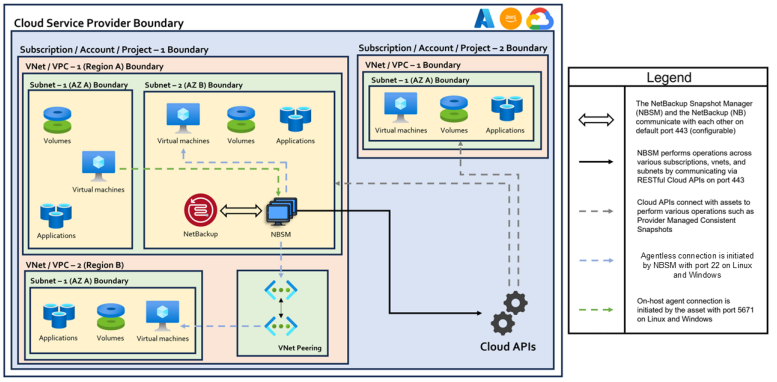
次の図は、NetBackup Snapshot Manager マイクロサービスモデルを示しています。



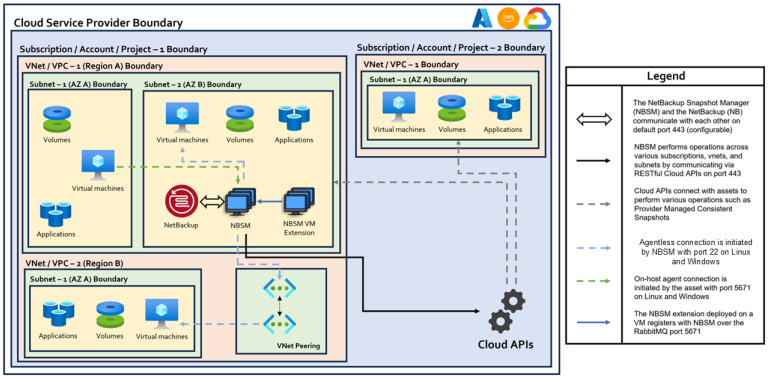
NetBackup Snapshot Manager ソリューションは、仮想マシン、VM ベースの拡張機能、および Kubernetes サービスクラスタ環境に配備できます。

次の図に、さまざまな配置モデル図を示します。

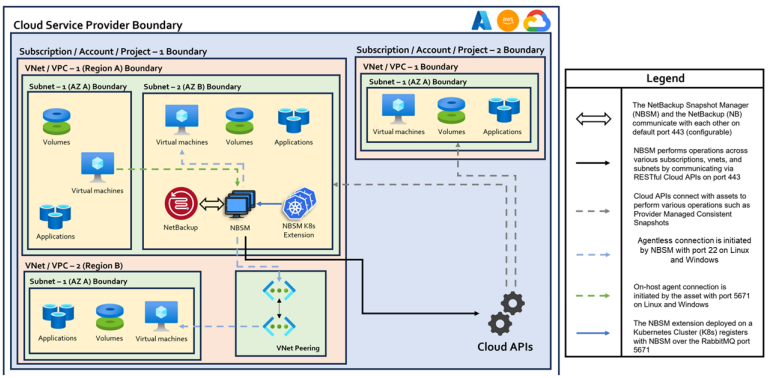
- VM ベースの配備:



- VM ベースの拡張機能の配備:



- Kubernetes ベースの NetBackup Snapshot Manager 拡張機能の配備



詳しくは、『Kubernetes クラスタ向け Cohesity Cloud Scale Technology 手動配備ガイド』を参照してください。

これらの配備方法には、次の利点があります。

- NetBackup Snapshot Manager にインストールの最小限の要件があります。
- 配備はいくつかのコマンドのみを必要とします。

クラウド並列ストリームジョブ階層

NetBackup 11.1 では、クラウド仮想マシン (VM) の並列ストリームバックアップメカニズムの一部として、新しいジョブ階層が導入されました。

クラウド VM バックアップ中に並列読み取りが有効な場合、クラウド VM スナップショット操作の一部として、次のように複数のストリームイメージが作成されます。

- 各 VM ディスクに対して、1 つの子イメージ (ストリーム) が生成されます。
- ストリーム 1 は、他のすべての子ストリームのデータを組み合わせた、合成イメージまたは統合イメージとして機能します。
- すべての子ストリームが正常に完了すると、ストリーム 1 (アンカーイメージ) のバックアップが続行されます。

ストリーム 1 ジョブは、アンカー (親の親) のイメージジョブの役割を果たし、バックアップ階層全体の最上位コントローラとして機能します。

ジョブ階層処理

仮想マシン (VM) のバックアップジョブの開始時:

1. プライマリジョブ (アンカー/親の親のイメージジョブ) が開始され、前処理タスクが実行されます。
2. 前処理の完了後、ストレージライフサイクルポリシー (SLP) が個々のデータ転送ジョブ (VM ディスクごとに 1 つ) をトリガします。
3. SLP によって開始されるジョブはすべて、同じ親の親階層の一部となります。
4. SLP によって開始される今後の再試行ジョブも同じ階層に分類され、構造の一貫性が維持されます。

たとえば、3 つの仮想ディスクを含む VM の場合、ジョブ階層は次のように表示されます。

```
10    —  Backup From Snapshot  ----------Top job in hierarchy (Anchor
 image job/Parent Job)  (Parent stream  Stream No = 1)

         17 — Backup from Snapshot — Data transfer job for Stream 1
 - This is synthesized job, which synthesizes all the child stream
data.

        13  — Backup from Snapshot ---------- Export Snapshot  Job
for Disk  1 ( Child stream backup  stream = 2 )

          .      14  — Backup from Snapshot ---------- Data transfer
 Job for Disk  1

        12  — Backup from Snapshot ---------- Export Snapshot Job
for Disk  2 ( Child stream backup  stream = 3 )

           .     15  — Backup from Snapshot ---------- Data transfer
 Job for Disk  2

        11  — Backup from Snapshot ---------- Export Snapshot Job
for Disk  3 ( Child stream backup  stream = 4 )
```

```
.   16  — Backup from Snapshot ---------- Data transfer
Job for Disk  3
```

NetBackup Snapshot Manager for Cloud を実行する場所の決定

NetBackup Snapshot Manager for Cloud を次の方法で配備できます。

- NetBackup Snapshot Manager をクラウドに配備し、同じクラウドの資産を管理します。
- NetBackup Snapshot Manager を 1 つのクラウドに配備し、複数のクラウド内の資産を管理します。

Cohesityは、NetBackup Snapshot Manager をクラウドの資産を保護するためにクラウドに配備することをお勧めします。クラウド内の資産を保護する場合は、NetBackup Snapshot Manager ホストインスタンスを同じクラウド環境に配備します。

Azure Files、Azure NetApp Files、FSx for AWS などのストレージアレイを使用してクラウド資産を保護するには、*『NetBackup Snapshot Manager for Data Center 管理者ガイド』*を参照してください。

複数のホストに NetBackup Snapshot Manager をインストールする場合は、各 NetBackup Snapshot Manager インスタンスが独立したリソースを管理することをお勧めします。たとえば、2 つの NetBackup Snapshot Manager インスタンスが同じ AWS アカウントまたは同じ Azure サブスクリプションを管理しないようにする必要があります。次のシナリオは、2 つの NetBackup Snapshot Manager インスタンスが同じリソースを管理し、問題が発生する理由を示しています。

- NetBackup Snapshot Manager インスタンス A および NetBackup Snapshot Manager インスタンス B は、両方とも同じ AWS アカウントの資産を管理します。
- NetBackup Snapshot Manager インスタンス A では、管理者は AWS 仮想マシンのスナップショットを取得します。NetBackup Snapshot Manager インスタンス A のデータベースに、仮想マシンのメタデータが格納されます。このメタデータには、仮想マシンのストレージサイズとそのディスク構成が含まれます。
- その後、NetBackup Snapshot Manager インスタンス B で、管理者が仮想マシンのスナップショットをリストアします。NetBackup Snapshot Manager インスタンス B には、仮想マシンのメタデータへのアクセス権がありません。スナップショットをリストアしますが、仮想マシンの特定の構成を識別できません。代わりに、ストレージサイズ構成のデフォルト値を置き換えます。その結果、リストアされた仮想マシンが、元の仮想マシンと一致しなくなります。

クラウドでの NetBackup Snapshot Manager の配備について

NetBackup Snapshot Manager は、手動で配備するか、サポート対象クラウドのマーケットプレイスで利用可能な NetBackup Snapshot Manager テンプレートを使用して配備できます。

マーケットプレイスの配備について詳しくは、次の文書を参照してください。

Microsoft Azure での NetBackup™ マーケットプレイスの配備

AWS での NetBackup™ マーケットプレイスの配備

手動で NetBackup Snapshot Manager を配備する場合は、NetBackup Snapshot Manager のブートディスクの UUID が一意であり、他の資産ノードの FS の UUID と競合していないことを確認します。

クラウドに NetBackup Snapshot Manager インスタンスを配備する方法について詳しくは、NetBackup の詳細に関する説明を参照してください。

1

NetBackup Snapshot Manager for Cloud のインストールと構成

2

NetBackup Snapshot Manager for Cloud のインストールの準備

この章では以下の項目について説明しています。

- システム要件への準拠
- NetBackup Snapshot Manager ホストのサイズの決定に関する推奨事項
- NetBackup Snapshot Manager 拡張機能のサイズの決定に関する推奨事項
- MSDP-C キャッシュサイズの推奨事項
- NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備
- コンテナプラットフォーム (Docker、Podman) のインストール
- NetBackup Snapshot Manager データを格納するボリュームの作成とマウント
- インスタンスまたは物理ホストで特定のポートが開いていることの確認
- NetBackup Snapshot Manager でのスナップショットジョブからのバックアップの準備
- OCI - スナップショットジョブからのバックアップの iptables ルール

システム要件への準拠

NetBackup Snapshot Manager ホストの要件

NetBackup Snapshot Manager をインストールするホストは、次の要件を満たしている必要があります。

p.29 の「NetBackup Snapshot Manager ホストのサイズの決定に関する推奨事項」を参照してください。

表 2-1 NetBackup Snapshot Manager ホストのオペレーティングシステム、プロセッサ、およびパッケージの要件

カテゴリ	要件
オペレーティングシステム	詳しくは、NetBackup Snapshot Manager SCL (ソフトウェアの互換性リスト) を参照してください。
プロセッサアーキテクチャ	詳しくは、NetBackup Snapshot Manager SCL (ソフトウェアの互換性リスト) を参照してください。
NetBackup Snapshot Manager ホストのパッケージ	次に、NetBackup Snapshot Manager ホストにインストールするオペレーティングシステム固有の必須パッケージを示します。 ■ Ubuntu: lvm2、udev ■ SUSE: lvm2、udev ■ RHEL: podman-plugins、lvm2、systemd-udev、udica、policycoreutils-devel ■ OEL: podman-plugins、lvm2、systemd-udev、udica、policycoreutils-devel

メモ: NetBackup Snapshot Manager の単一のホスト名または FQDN には、64 文字の制限があります。これはインストール時に必要です。

マルチエイリアス機能は、Snapshot Manager ではサポートされなくなりました。

Snapshot Manager バージョン 10.4 以降のインストールは、旧バージョンの NetBackup プライマリサーバー (10.2 以前) ではサポートされません。10.2 以前のリリースからのアップグレードサポートの場合:

p.275 の「NetBackup Snapshot Manager のアップグレード」を参照してください。

表 2-2 NetBackup Snapshot Manager ホストのシステム要件

NetBackup Snapshot Manager がインストールされているホスト	要件
アマゾンウェブサービス (AWS) インスタンス	■ Elastic Compute Cloud (EC2) インスタンスタイプ: t3.large ■ vCPU: 2 ■ RAM: 16 GB ■ root ディスク: ソリッドステートドライブ (GP2) 付き 64 GB ■ データボリューム: スナップショット資産データベースに対する暗号化があるタイプ GP2 の 50 GB EBS (Elastic Block Store) ボリューム。このデータボリュームは開始時の値として使用し、必要に応じてストレージを拡張します。 PaaS 作業負荷の場合: ■ Elastic Compute Cloud (EC2) インスタンスタイプ: m4.2xlarge ■ CPU: 8 ■ RAM: 32 GB
Microsoft Azure VM	■ 仮想マシン形式: D2s_V3 標準 ■ CPU コア: 2 ■ RAM: 16 GB ■ ルートディスク: 64 GB SSD ■ データボリューム: スナップショット資産データベース用の 50 GB Premium SSD バージョン 1。ストレージアカウントの種類 Premium_LRS。ホストキャッシュを読み取り/書き込みに設定します。 Azure クラウドで RHEL インスタンスに NetBackup Snapshot Manager を配備する前に、次の操作を行ってください。 ■ Red Hat Subscription Manager を使用して Red Hat に RHEL インスタンスを登録する ■ ディスク容量の最小要件を満たすために RHEL インスタンスのデフォルトの LVM パーティションを拡張する

NetBackup Snapshot Manager がインストールされているホスト	要件
Microsoft Azure Stack Hub VM	■ 仮想マシン形式: ■ DS2_v2 Standard - CPU コア数 2、RAM 7 GB ■ DS3_v2 Standard - CPU コア数 4、RAM 14 GB ■ ルートディスク: 64 GB SSD ■ データボリューム: スナップショット資産データベース用の 50 GB Premium SSD バージョン 1。ストレージアカウントの種類 Premium_LRS。ホストキャッシュを読み取り/書き込みに設定します。 Azure Stack Hub クラウドで RHEL インスタンスに NetBackup Snapshot Manager を配備する前に、次の操作を行ってください。 ■ Red Hat Subscription Manager を使用して Red Hat に RHEL インスタンスを登録する ■ ディスク容量の最小要件を満たすために RHEL インスタンスのデフォルトの LVM パーティションを拡張する
Google Cloud Platform (GCP) VM	■ 仮想マシンタイプ: n2-standard-4 ■ vCPU: 2 ■ RAM: 16 GB ■ ブートディスク: 64 GB の標準永続ディスク ■ データボリューム: 自動暗号化があるスナップショット資産データベース用の 50 GB SSD 永続ディスク **メモ:** LVM のインデックス付けに対応するため、NetBackup Snapshot Manager ホストでマルチパスサービスが無効になっていることを確認します。 **メモ:** カスタムイメージを使用して NetBackup Snapshot Manager を配備する場合は、「ゲスト環境をインストールする」に記載されている GCP のガイドラインに従います。

NetBackup Snapshot Manager がインストールされているホスト	要件
OCI (Oracle Cloud Infrastructure)	■ VM タイプ (シェイプタイプ): VM.Standard.E4.Flex/ VM.Standard.E5.Flex/ VM.Standard3.Flex/ VM.Optimized3.Flex ■ OCPU: 1 ■ RAM: 16 GB ■ ブートボリューム: 50 GB ■ データボリューム: 50 GB **メモ:** スナップショットからのバックアップとシングルファイルリストアを使用するには、Oracle Cloud Agent が実行されており、ブロックボリューム管理プラグインが OCI コンソールから有効になっていることを確認します。詳しくは、Oracle のマニュアルを参照してください。

ディスク容量の要件

NetBackup Snapshot Manager はホスト上の次のファイルシステムを使用して、インストール時にすべてのコンテナイメージとファイルを保存します。

- / *(ルートファイルシステム)*
- `/var`

`/var` ファイルシステムは、コンテナの実行時にさらに使用されます。NetBackup Snapshot Manager のインストールまたはアップグレード先のホストに、次のコンポーネント用の十分な空き容量があることを確認します。

表 2-3 NetBackup Snapshot Manager コンポーネントの空き容量に関する考慮事項

コンポーネント	空き容量の要件
NetBackup Snapshot Manager コンテナ	最小 10 GB (推奨 30 GB) の空き容量。
NetBackup Snapshot Manager エージェントとプラグイン	350 MB の空き容量 (構成する各 NetBackup Snapshot Manager プラグインおよびエージェント用)

さらに、NetBackup Snapshot Manager は NetBackup Snapshot Manager データを格納するために個別のボリュームも必要です。このボリュームを作成して NetBackup Snapshot Manager ホストの `/cloudpoint` に確実にマウントします。`/cloudpoint` ディレクトリの権限が 755 であることを確認します。

表 2-4 NetBackup Snapshot Manager データボリュームの空き容量に関する考慮事項

ボリュームのマウントパス	サイズ
/cloudpoint	50 GB 以上

p.29 の「NetBackup Snapshot Manager ホストのサイズの決定に関する推奨事項」を参照してください。

ファイアウォールポートの要件

インバウンドとアウトバウンドのファイアウォールポートの要件を次に示します。

- 次のインバウンドポートを開く必要があります。
  - 443: プライマリ、メディア、クライアントからの API 要求を処理します。デフォルトポートで構成する場合は、カスタムポートのファイアウォールでインバウンドを許可する必要があります。
  - 5671: Snapshot Manager のエージェント用。
- 次のアウトバウンドポートが必要です。
  - 22: Linux VM (OpenSSH) と Windows VM (WMI) へのエージェントレス接続用。
  - 1556: NetBackup プライマリサーバーへの登録用。

バックアップコピーからの SFR (シングルファイルリストア) に必要な追加ポートを次に示します。

- Windows の場合: ストレージサーバーから SMB 共有にアクセスするには、ポート 139 と 445 をクライアント (オンホストエージェントが実行されているターゲット VM) からアウトバウンドに開く必要があります。
- Linux の場合: ストレージサーバーから NFS 共有にアクセスするには、ポート 2049 と 111、標準の NFS ポート、2049 と 111 をクライアント (オンホストエージェントが実行されているターゲット VM) からアウトバウンドに開く必要があります。

NetBackup Snapshot Manager エージェントとプラグインのサポート対象アプリケーション、オペレーティングシステム、クラウドプラットフォーム

NetBackup Snapshot Manager は次のアプリケーション、オペレーティングシステム、クラウドプラットフォームをサポートしています。

これらの資産は、NetBackup Snapshot Manager の構成方法、NetBackup Snapshot Manager クラウドエージェントとプラグイン (旧名はオフホストプラグイン) を使用するかどうか、NetBackup Snapshot Manager アプリケーション設定プラグイン (旧名はオンホス

トプラグイン) を使用するかどうか、または NetBackup Snapshot Manager エージェントレス機能を使用するかどうかにかかわらずサポートされます。

表 2-5　サポート対象アプリケーション、オペレーティングシステム、クラウドプラットフォーム

カテゴリ	サポート
アプリケーション	■ ファイルシステム ■ Linux ネイティブファイルシステム: ext3、ext4、XFS ■ Microsoft Windows: NTFS ■ Microsoft SQL p.228 の「Microsoft SQL プラグインの構成に関する要件」を参照してください。 ■ Windows Server ■ Windows アプリケーションは OCI ではサポートされません。 ■ Oracle 単一ノード構成がサポート対象です。 p.235 の「Oracle プラグインの構成に関する要件」を参照してください。 **メモ:** サポートされているバージョンの完全なリストについては、NetBackup Snapshot Manager SCL (ソフトウェア互換性リスト) を参照してください。
サポート対象資産のオペレーティングシステム	■ RHEL (Red Hat Enterprise Linux) ■ Windows Server ■ OEL (Oracle Enterprise Linux) **メモ:** サポートされているバージョンの完全なリストについては、NetBackup Snapshot Manager SCL (ソフトウェア互換性リスト) を参照してください。

カテゴリ	サポート
クラウドプラットフォーム	アマゾンウェブサービス (AWS) アプリケーションを保護する場合、アプリケーションは t2.large 以上の仕様の AWS インスタンスタイプでホストされている必要があります。現在、NetBackup Snapshot Manager では t2.medium 以下のインスタンスタイプで実行されているアプリケーションはサポートされません。 t2 シリーズのインスタンスは、AWS によって推奨されるデバイスの命名規則に従っている場合にのみサポートされます。 詳しくは、次のリンクを参照してください。 ■ Windows: Windows インスタンスのデバイス名 ■ Linux: Linux インスタンスのデバイス名 Microsoft Windows ベースのアプリケーションを保護するには、t2.xlarge または t3.xlarge 以上の仕様のインスタンスタイプを使用します。 AWS の構成に必要な権限について詳しくは、次のリンクを参照してください。 p.126 の「NetBackup Snapshot Manager に必要な AWS アクセス権」を参照してください。
	Microsoft Azure アプリケーションを保護する場合、アプリケーションは D2s_V3 標準以上の仕様の Azure 仮想マシン形式でホストされている必要があります。 Microsoft Windows ベースのアプリケーションを保護するには、B4ms または D4s_V3 以上の仕様の仮想マシンを使用します。 **メモ:** NetBackup Snapshot Manager Azure プラグインは Premium SSD v2 (PremiumV2_LRS)、UltraSSD_LRS、Premium_LRS、Standard_LRS、StandardSSD_LRS のディスク形式をサポートします。 その他のすべてのディスク形式は、スナップショットのリストア操作中にデフォルトで Standard_LRS になります。 Azure の構成に必要な権限について詳しくは、次のリンクを参照してください。 p.179 の「Microsoft Azure でのアクセス権の設定」を参照してください。

カテゴリ	サポート
	Microsoft Azure Stack Hub (2008 以降) アプリケーションを保護する場合、アプリケーションは DS2_v2 Standard 以降の仕様の Azure Stack Hub 仮想マシン形式でホストされている必要があります。詳しくは、「Azure Stack Hub でサポートされている VM サイズ」を参照してください。 **メモ:** NetBackup Snapshot Manager Azure Stack Hub プラグインは Premium_LRS、Standard_LRS、StandardSSD_LRS のディスク形式をサポートします。 その他のすべてのディスク形式は、スナップショットのリストア操作中にデフォルトで Standard_LRS になります。 Microsoft Azure Stack の構成に必要な権限について詳しくは、次のリンクを参照してください。 p.192 の「Microsoft Azure Stack Hub でのアクセス権の設定」を参照してください。
	GCP (Google Cloud Platform) アプリケーションを保護する場合、アプリケーションは n2-standard-4 以上の仕様の GCP 仮想マシン形式でホストされている必要があります。 Google Cloud Platform の構成に必要な権限について詳しくは、次のリンクを参照してください。 p.159 の「NetBackup Snapshot Manager で必要な Google Cloud Platform アクセス権」を参照してください。
	OCI (Oracle Cloud Infrastructure) アプリケーションを保護する場合は、x86_64 マシンでアプリケーションをホストします。2 つの OCPU と 16 GB の RAM を使用します。 OCI の構成に必要な権限について詳しくは、次のリンクを参照してください。 p.202 の「NetBackup Snapshot Manager に必要な OCI 権限」を参照してください。 アプリケーションリストア機能を使用するには、OCI コンソールからホストする VM のブロックボリューム管理プラグインを有効にします。詳しくは、以下を参照してください。 ブロックボリューム管理プラグインの有効化

NetBackup Snapshot Manager タイムゾーン

NetBackup Snapshot Managerを配備するホストのタイムゾーン設定が、要件に従っており、パブリック NTP サーバーと同期していることを確認します。

デフォルトでは、NetBackup Snapshot Manager は NetBackup Snapshot Manager のインストール先のホストに設定されているタイムゾーンを使用します。ログのすべてのエントリのタイムスタンプは、ホストマシンのクロック設定に従います。

プロキシサーバーの要件

NetBackup Snapshot Manager を配備しているインスタンスが、プロキシサーバーの背後にある場合、つまり、NetBackup Snapshot Manager インスタンスがプロキシサーバーを使用してインターネットに接続する場合は、NetBackup Snapshot Manager のインストール時にプロキシサーバーの詳細を指定する必要があります。NetBackup Snapshot Manager インストーラは、プロキシサーバーの情報を、NetBackup Snapshot Manager コンテナ固有の一連の環境変数に格納します。

次の表に、NetBackup Snapshot Manager インストーラに提供する必要がある環境変数とプロキシサーバー情報を示します。この情報を手元に用意してください。NetBackup Snapshot Manager のインストール時にこれらの詳細を入力する必要があります。

表 2-6 NetBackupSnapshot Manager に必要なプロキシサーバーの詳細

NetBackup Snapshot Manager インストーラによって作成される環境変数	説明
VX_HTTP_PROXY	すべての接続に使用されるHTTPプロキシ値が格納されます。たとえば、"http://proxy.mycompany.com:8080/" です。
VX_HTTPS_PROXY	すべての接続に使用されるHTTPプロキシ値が格納されます。たとえば、"http://proxy.mycompany.com:8080/" です。

NetBackup Snapshot Manager インストーラによって作成される環境変数	説明
VX_NO_PROXY	プロキシサーバーをバイパスできるホストが格納されます。たとえば、"localhost,mycompany.com,192.168.0.10:80" です。 **メモ:** NetBackup Snapshot Manager をクラウドに配備する場合は、このパラメータで次の値をそれぞれ設定していることを確認します。 AWS インスタンス、Azure VM、OCI インスタンスの場合: 169.254.169.254 GCP 仮想マシンの場合: 169.254.169.254,metadata,metadata.google.internal NetBackup Snapshot Manager はこれらのアドレスを使用して、インスタンスメタデータサービスからインスタンスメタデータを収集します。 Microsoft Azure では、設定がプライベートネットワーク内にあり、バックアップトラフィックにプロキシを経由させない場合に、次のエンドポイントを[プロキシなし (No Proxy)]構成に追加します。 .storage.azure.net

プロキシサーバー経由で外部と通信する必要がある NetBackup Snapshot Manager サービスは、NetBackup Snapshot Manager のインストール時に設定された事前定義済みの環境変数を使用します。

FIPS サポート要件

FIPS サポートは、次の場合にのみ適用されます。

- NetBackup、NetBackup Snapshot Manager およびすべての保護対象の作業負荷の FIPS 準拠の状況は、次の表に示すとおりです。

コンポーネント	FIPS の状態		FIPS の状態	
NetBackup	Y	N	Y	Y
NetBackup Snapshot Manager	N	Y	Y	Y
作業負荷システム	Y/N	Y/N	Y	N
推奨	N	N	Y	N

- RHEL 8 プラットフォームでの新規インストールと、VM ベース (BYOD) の配備のみに限定されます。

メモ: OCI の NetBackup Snapshot Manager 配備は FIPS 準拠ではありません。

NetBackup Snapshot Manager ホストのサイズの決定に関する推奨事項

NetBackup Snapshot Manager ホストの構成は、主に作業負荷の数と、保護する作業負荷の種類によって異なります。また、パフォーマンス容量がピーク時に NetBackup Snapshot Manager 上で同時に稼働する操作の最大数にも依存します。

パフォーマンスに影響するもう 1 つの要因は、資産の保護に NetBackup Snapshot Manager を使用する方法です。NetBackup Snapshot Manager エージェントレスオプションを使用して資産を検出して保護すると、作業負荷の種類によってパフォーマンスが異なります。

エージェントレスでは、NetBackup Snapshot Manager はプラグインデータをアプリケーションホストに転送し、検出および構成タスクを実行し、その後、アプリケーションホストからプラグインパッケージを削除します。

Cohesity は、NetBackup Snapshot Manager ホストに対して次の構成をお勧めします。

表 2-7 並列実行タスクの数に基づく標準的な NetBackup Snapshot Manager ホストの構成

作業負荷メトリック	NetBackup Snapshot Manager ホストの設定
最大 16 個の同時操作タスク	CPU: 2 個の CPU メモリ: 16 GB たとえば、AWS クラウドでは、NetBackup Snapshot Manager ホスト仕様は、t3.xlarge インスタンスと同等である必要があります。
最大 32 個の同時操作タスク	CPU: 4-8 個の CPU メモリ: 32 GB 以上 たとえば、AWS クラウドでは、NetBackup Snapshot Manager ホスト仕様は、t3.2xlarge インスタンス以上の種類と同等である必要があります。

一般的な考慮事項とガイドライン:

NetBackup Snapshot Manager ホストの構成を選択するときは、次の点を考慮してください。

- 作業負荷の高い環境でパフォーマンスを向上させるには、Cohesity は NetBackup Snapshot Manager ホストをアプリケーションホストと同じ場所に配備することをお勧めします。
- エージェントレスオプションを使用している場合、Cohesityではアプリケーションホストの `/opt/VRTScloudpoint` ディレクトリに十分な領域を割り当てることをお勧めします。NetBackup Snapshot Manager はプラグイン構成ファイルを抽出するために、このディレクトリを使用します。
- 作業負荷の数によっては、NetBackup Snapshot Manager ホストから送信されるプラグインデータの量は、サイズがかなり大きくなる可能性があります。このような場合、ネットワーク遅延も重要な役割を担います。これらの要因によって、全体的なパフォーマンスが異なる場合があります。
- エージェントレスオプションを使用して複数の作業負荷を構成する場合、パフォーマンスは、アプリケーション作業負荷インスタンスに関するネットワーク帯域幅や NetBackup Snapshot Manager ホストの場所などの要因によって異なります。必要に応じて、NetBackup Snapshot Manager ホストの CPU、メモリ、ネットワーク構成を増やし、エージェントレスアプリケーションホストの並列設定でパフォーマンスを向上できます。
- 並列操作の数が、NetBackup Snapshot Manager ホスト構成の容量で処理できる数よりも多い場合は、NetBackup Snapshot Manager は自動的に操作をジョブキューに投入します。キューに投入されたジョブは、実行中の操作が完了した後にのみ取得されます。
- NetBackup は、NetBackup Snapshot Manager VM インスタンスで利用可能なディスク接続ポイントの数によって並列操作の数を自動的に制御します。

NetBackup Snapshot Manager 拡張機能のサイズの決定に関する推奨事項

NetBackup Snapshot Manager 拡張機能の目的は、パフォーマンス容量がピーク時に NetBackup Snapshot Manager 上で多数の要求を同時に実行するため、NetBackup Snapshot Manager ホストの容量を拡大縮小させることです。要件に応じて、1 つ以上の NetBackup Snapshot Manager 拡張機能をクラウドにインストールし、ホストに余分な負荷をかけることなくジョブを実行できます。拡張機能により、NetBackup Snapshot Manager の処理容量を増加できます。

NetBackup Snapshot Manager 拡張機能では、NetBackup Snapshot Manager ホストと同等以上の構成が可能です。

p.19 の「 システム要件への準拠」を参照してください。

サポート対象の NetBackup Snapshot Manager 拡張機能の環境:

メモ: NetBackup Snapshot Manager 10.0 以降の場合、VM ベースの拡張機能は Azure Stack ハブでサポートされ、Kubernetes ベースの拡張機能は Azure、AWS、および GCP でサポートされます。

Cohesity は、NetBackup Snapshot Manager 拡張機能の次の構成をお勧めします。

表 2-8 VM ベースの拡張機能 (Azure Stack) の一般的な NetBackup Snapshot Manager 拡張機能の構成

作業負荷メトリック	NetBackup Snapshot Manager 拡張機能の構成
最大 16 個の同時操作タスク	CPU: 4 個の CPU メモリ: 16 GB たとえば、Azure Stack では、NetBackup Snapshot Manager 拡張機能は AWS の t3.xlarge インスタンスと同等である必要があります。
最大 32 個の同時操作タスク	CPU: 8 個の CPU メモリ: 32 GB 以上 たとえば、Azure Stack では、NetBackup Snapshot Manager 拡張機能は AWS の t3.2xlarge 以上の形式のインスタンスと同等である必要があります。

表 2-9 Kubernetes ベースの拡張機能 (Azure、AWS、および GCP) の一般的な NetBackup Snapshot Manager 拡張機能の構成

作業負荷メトリック	NetBackup Snapshot Manager 拡張機能の構成
最大 24 個の同時操作タスク	2 CPU と 8 GB の RAM ノード構成の場合: CPU: 2 CPU 超 ノードあたりの RAM: 8 GB ノードあたりの最大ポッド数: 13 + 15 + 8*2=16 (動的ポッド) = 44 以上 自動スケールが有効な場合、最小値は 1、最大値は 3 スナップショットジョブからの 1 つのバックアップに対して、2 つのポッドが作成されます。ここで、15 は断続的な操作のバッファポッド数です。13 は、10 (Kubernetes と CSP ポッドの数) + 3 (リスナー + fluent コレクタ + fluent デーモンセット) として計算されます。
	2/4/6 個の CPU と 16 GB のノード構成の場合 ノードあたりの CPU: 2/4/6 CPU 超 ノードあたりの RAM: 16 GB ノードあたりの最大ポッド数: 13 + 15 + 16*2=32 (動的ポッド) = 60 以上 自動スケールが有効な場合、最小値は 1、最大値は 3 スナップショットジョブからの 1 つのバックアップに対して、2 つのポッドが作成されます。ここで、15 は断続的な操作のバッファポッド数です。13 は、10 (Kubernetes と CSP ポッドの数) + 3 (リスナー + fluent コレクタ + fluent デーモンセット) として計算されます

(EKS 固有) Kubernetes メトリクスサーバーのインストール

Kubernetes メトリクスサーバーはクラスタ内のリソース使用状況データのアグリゲータであり、Amazon EKS クラスタではデフォルトでは展開されません。次の手順では、Amazon EKS クラスタに Kubernetes メトリクスサーバーを配備する方法について説明します。

1 次のコマンドを使用してメトリクスサーバーを配備します。

```
kubectl apply -f
https://github.com/kubernetes-sigs/metrics-server/releases/latest/download/components.yaml
```

2 次のコマンドを使用して、metrics-server の配備で必要な数のポッドが実行されていることを確認します。

```
kubectl get deployment metrics-server -n kube-system
```

出力例は次のとおりです。

```
NAME              READY   UP-TO-DATE   AVAILABLE   AGE
metrics-server    1/1     1            1           6m
```

一般的な考慮事項とガイドライン:

NetBackup Snapshot Manager 拡張機能の構成を選択するときは、次の点を考慮してください。

- 作業負荷の高い環境でパフォーマンスを向上させるため、Cohesity は NetBackup Snapshot Manager 拡張機能をアプリケーションホストと同じ場所に配備することをお勧めします。
- 管理対象の Kubernetes クラスタにあるクラウドベースの拡張機能は、NetBackup Snapshot Manager ホストと同じ VNet に存在する必要があります。同じ VNet にない場合、Azure クラウドで利用可能な VNet ピアリングメカニズムを利用し、NetBackup Snapshot Manager ホストと拡張機能ノードで必要なポートを介して相互に通信させることができます
- 作業負荷の数によっては、NetBackup Snapshot Manager ホストから送信されるプラグインデータの量は、かなり大きくなる可能性があります。このような場合、ネットワーク遅延も重要な役割を担います。これらの要因によって、全体的なパフォーマンスが異なる場合があります。
- 同時並行処理の数が、NetBackup Snapshot Manager ホストと拡張機能を合わせて処理できる数よりも多い場合、NetBackup Snapshot Manager は自動的に操作をジョブキューに投入します。キューに投入されたジョブは、実行中の操作が完了した後にのみ取得されます。

MSDP-C キャッシュサイズの推奨事項

並列ストリーム/読み取りが有効になっている NetBackup 11.1 環境では、大きなディスク作業負荷のバックアップ処理が遅く見える場合があります。

並列ストリームクラウド VM バックアップのパフォーマンスは、ストレージサーバーで構成されている MSDP-C ストレージキャッシュサイズによって異なる場合があります。MSDP-C は専用のキャッシュボリュームを使用しません。代わりに、必要に応じて MSDP サーバー

で利用可能な空き容量を一時的に使用します。デフォルトでは、MSDP-C で少なくとも 1 TB の空き容量が必要になります。この容量は、contentrouter.cfg ファイルで構成できます。

クラウドデータのサイズ変更とパフォーマンスは、お客様の特定の環境や作業負荷に依存するため、正確な推奨事項は異なる場合があります。そのため、サイズ変更は個々のニーズに合わせて調整する必要があります。

MSDP のサイズ変更について詳しくは、『NetBackupバックアップ計画とパフォーマンスチューニングガイド』の「クラウド階層のサイズ変更とパフォーマンス」に関するトピックを参照してください。

NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備

NetBackup Snapshot Manager をパブリッククラウドに配備する場合、次の手順を実行します。

- NetBackup Snapshot Manager のインストール要件を満たすサポート対象の Ubuntu、RHEL、SLES または OEL インスタンスイメージを選択します。
  p.19 の「 システム要件への準拠」を参照してください。
- インストール要件を満たすように、インスタンスに十分なストレージを追加します。

コンテナプラットフォーム (Docker、Podman) のインストール

表 2-10 コンテナプラットフォームのインストール

プラットフォーム	説明
Ubuntu 上の Docker	サポート対象バージョン: Docker 18.09 以降 Ubuntu に Docker をインストールする方法について詳しくは、Ubuntu への Docker Engine のインストールに関する説明を参照してください。

プラットフォーム	説明

RHEL 9、8.x の Podman
OEL 9 と 8.8 の Podman
	サポート対象バージョン: Podman 4.0.2 以降
	NetBackup Snapshot Manager が AWS クラウドに配備される場合、追加の repo を有効にしてください。
	`# sudo yum-config-manager --enable rhui-REGION-rhel-server-extras`
	次のサービスが有効であり、実行中であることを確認します。
	`# systemctl enable podman-restart`
	`# systemctl start podman-restart`
	`# systemctl enable podman.socket`
	`# systemctl start podman.socket`
	NetBackup Snapshot Manager が OCI クラウドに配備されている場合:
	■ SELinux が有効になっている場合は、モードを permissive モードに変更します。`/etc/selinux/config` 構成ファイルを編集し、`SELINUX` パラメータ値を `SELINUX=permissive` に変更します。
	■ 変更を有効にするにはシステムを再起動します。
	■ SELinux モードの変更を、次のコマンドを使用して確認します。
	`# sudo sestatus`
	コマンド出力の `Current Mode` パラメータ値が、permissive として表示されるはずです。

NetBackup Snapshot Manager データを格納するボリュームの作成とマウント

クラウド環境に NetBackup Snapshot Manager または NetBackup Snapshot Manager 拡張機能を配備する前に、以下を確認してください。

- NetBackup Snapshot Manager データを格納するために少なくとも 50 GB のボリュームを作成してマウントする必要があります。ボリュームは、`/cloudpoint` にマウントされる必要があります。
- ホストまたは拡張機能を再起動するときにボリュームが自動マウントされるように、ボリュームとマウントポイント (`/cloudpoint`) の UUID が `/etc/fstab` に指定されていることを確認します。

メモ: このボリュームを接続せずにインスタンスを起動した場合 (たとえば、ボリュームを別のインスタンスに移動した後)、`nofail` マウントオプションを使用すると、ボリュームのマウントにエラーがあってもインスタンスを起動できます。

表 2-11 サポート対象の各クラウドベンダーのボリューム作成手順

ベンダー	手順
アマゾンウェブサービス (AWS)	**1** EC2 ダッシュボードで、[ボリューム (Volumes)]、[ボリュームの作成 (Create Volumes)]の順にクリックします。 **2** 画面に表示される指示に従って、次のように指定します。 ■ ボリュームの種類: 汎用 SSD ■ サイズ: 50 GB **3** 「Linux で Amazon EBS ボリュームを使用できるようにする」セクションにある手順を使用して、ファイルシステムを作成し、デバイスをインスタンスホストの `/cloudpoint` にマウントします。
Google Cloud Platform	◆ 仮想マシン用のディスクを作成し、初期化し、`/cloudpoint` にマウントします。 詳しくは、VM への永続ディスクの追加に関する説明を参照してください。
Microsoft Azure	**1** 新しいディスクを作成し、仮想マシンに接続します。詳しくは、「ポータルを利用し、データ ディスクを Linux VM に接続する」を参照してください。 管理対象ディスクオプションを選択する必要があります。詳しくは、「ポータルを利用し、データ ディスクを Linux VM に接続する」を参照してください。 **2** ディスクを初期化し、`/cloudpoint` にマウントします。詳しくは、「Linux VM へのディスクの追加」にある、Linux VM に接続して新しいディスクをマウントする方法に関するセクションを参照してください。
Microsoft Azure Stack Hub	**1** 新しいディスクを作成し、仮想マシンに接続します。詳しくは、「Azure Stack Hub で VM ディスク ストレージを作成する」を参照してください。 管理対象ディスクオプションを選択する必要があります。 **2** ディスクを初期化し、`/cloudpoint` にマウントします。詳しくは、「Linux VM へのディスクの追加」にある、Linux VM に接続して新しいディスクをマウントする方法に関するセクションを参照してください。

ベンダー	手順
Oracle Cloud Infrastructure	1 新しいディスクを作成して VM に接続します。詳しくは、Oracle のマニュアルを参照してください。 2 ディスクを初期化し、/cloudpoint にマウントします。詳しくは、Oracle のマニュアルの、Linux VM に接続して新しいディスクをマウントする方法に関するセクションを参照してください。

インスタンスまたは物理ホストで特定のポートが開いていることの確認

インスタンスまたは物理ホストで、次のポートが開いていることを確認してください。

表 2-12 NetBackup Snapshot Manager で使用するポート

ポート	説明
443	NetBackup Snapshot Manager ユーザーインターフェースでは、このポートがデフォルトの HTTPS ポートとして使用されます。 **メモ:** 配備時にカスタムポートを使用する場合は、ファイアウォールで同じカスタムポートを有効にする必要があります。
5671	NetBackup Snapshot Manager RabbitMQ サーバーでは、通信にこのポートが使用されます。複数のエージェント、拡張機能、スナップショットからのバックアップ、バックアップジョブからのリストアをサポートするには、このポートを開く必要があります。

次のことに注意してください。

- インスタンスがクラウド内にある場合は、クラウドに対して必要な受信の規則に従ってポート情報を設定します。
- NetBackup Snapshot Manager のインストール時にポートを設定すると、アップグレード時に変更できません。

NetBackup Snapshot Manager でのスナップショットジョブからのバックアップの準備

スナップショットジョブからのバックアップの場合、メディアサーバー 10.1 以降が必要です。

メモ: Cohesityでは、クラウド資産のスナップショットジョブからのバックアップを実行するために使用される NetBackup Snapshot Manager の拡張機能でスワップ領域を有効にすることをお勧めします。スワップ領域の推奨サイズは、システムメモリの 0.5 倍以上です。スワップ領域を有効にできない状況では、より大きなメモリ構成のシステムを使用することをお勧めします。

メモ: (*AKS* のみ) Kubernetes ベースの拡張機能における NetBackup のインストールと NetBackup Snapshot Manager の配備のために Azure Kubernetes クラスタのスワップ領域を有効にするには、「Azure Kubernetes Service (AKS) ノードプールのノード構成をカスタマイズする」に記載されている手順に従います。

必要なポート:

- NetBackup プライマリサーバーで必要なポート: 1556 および 443
- クライアント側の重複排除のため NetBackup メディアサーバーで必要なポート: 10082 と 10102

証明書のインストールおよび NetBackup との通信にプライベート名を使用し、`/etc/hosts` を使用して解決する必要がある場合は、次の手順に従います。

- `/cloudpoint/openv/etc/hosts` ファイルに `/etc/hosts` ファイルと同じ形式でエントリを追加します。
- NetBackup Snapshot Manager のインストール時と NetBackup Snapshot Manager の登録時にプライベート名を使用していることを確認します。

OCI - スナップショットジョブからのバックアップの iptables ルール

OCI では、Ubuntu ホストに NetBackup Snapshot Manager を配備するときに、いくつかのデフォルトの iptables ルールを再構成する必要があります。デフォルトの iptables ルールが原因で発生するサービス間のネットワーク接続の問題により、スナップショットからのバックアップ、インデックス付け、バックアップからのリストアの各ジョブが失敗する場合があります。`iptables` ファイルは次の場所にあります。

```
etc/iptables/rules.v4
```

メモ: IPv6 が構成された NetBackup Snapshot Manager は、OCI での配備ではサポートされません。

iptables ルールファイルの内容は、デフォルトで存在するルールをコメントアウトすると、次の例のようになります。

```
# CLOUD_IMG: This file was created/modified by the Cloud Image build
 process
# iptables configuration for Oracle Cloud Infrastructure

# See the Oracle-Provided Images section in the Oracle Cloud
Infrastructure
# documentation for security impact of modifying or removing these
rule

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [463:49013]
#:InstanceServices - [0:0]
#-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
#-A INPUT -p icmp -j ACCEPT
#-A INPUT -i lo -j ACCEPT
#-A INPUT -p udp --sport 123 -j ACCEPT
#-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
#-A INPUT -j REJECT --reject-with icmp-host-prohibited
#-A FORWARD -j REJECT --reject-with icmp-host-prohibited
#-A OUTPUT -d 169.254.0.0/16 -j InstanceServices
#-A InstanceServices -d 169.254.0.2/32 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.2.0/24 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.4.0/24 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.5.0/24 -p tcp -m owner --uid-owner
0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided
 Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.2/32 -p tcp -m tcp --dport 80 -m
comment --comment "See the Oracle-Provided Images section in the
Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 53
```

```
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p tcp -m tcp --dport 53
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.3/32 -p tcp -m owner --uid-owner
0 -m tcp --dport 80 -m comment --comment "See the Oracle-Provided
Images section in the Oracle Cloud Infrastructure documentation for
 security impact of modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.4/32 -p tcp -m tcp --dport 80 -m
comment --comment "See the Oracle-Provided Images section in the
Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p tcp -m tcp --dport 80
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 67
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 69
 -m comment --comment "See the Oracle-Provided Images section in the
 Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.169.254/32 -p udp --dport 123 -m
comment --comment "See the Oracle-Provided Images section in the
Oracle Cloud Infrastructure documentation for security impact of
modifying or removing this rule" -j ACCEPT
#-A InstanceServices -d 169.254.0.0/16 -p tcp -m tcp -m comment
--comment "See the Oracle-Provided Images section in the Oracle Cloud
 Infrastructure documentation for security impact of modifying or
removing this rule" -j REJECT --reject-with tcp-reset
#-A InstanceServices -d 169.254.0.0/16 -p udp -m udp -m comment
--comment "See the Oracle-Provided Images section in the Oracle Cloud
 Infrastructure documentation for security impact of modifying or
removing this rule" -j REJECT --reject-with icmp-port-unreachable
COMMIT
root@nbsm-host:/#
```

iptables ルールを変更した後、NetBackup Snapshot Manager インスタンスを再起動します。

3

コンテナイメージを使用した NetBackup Snapshot Manager for Cloud の配備

この章では以下の項目について説明しています。

NetBackup Snapshot Manager のインストールを開始する前に

NetBackup Snapshot Manager をインストールする前に次を完了していることを確認します。

- NetBackup Snapshot Manager をインストールする場所を決定します。
  p.15 の「NetBackup Snapshot Manager for Cloud を実行する場所の決定」を参照してください。

メモ: NetBackup Snapshot Manager を複数のホストにインストールすることを計画している場合は、このセクションをよく読み、この方法の影響を理解してください。

- 環境がシステム要件を満たしていることを確認します。
  p.19 の「 システム要件への準拠」を参照してください。
- NetBackup Snapshot Manager をインストールするインスタンスを作成します。
  p.34 の「NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備」を参照してください。
- コンテナプラットフォームのインストール
  p.34 の「コンテナプラットフォーム (Docker、Podman) のインストール」を参照してください。
- NetBackup Snapshot Manager データを格納するボリュームを作成してマウントします。
  p.35 の「NetBackup Snapshot Manager データを格納するボリュームの作成とマウント」を参照してください。
- インスタンスで特定のポートが開いていることを確認します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。

メモ: RedHat 8.x では、Docker エコシステムが Podman エコシステムに置き換えられました。

Docker/Podman 環境への NetBackup Snapshot Manager のインストール

NetBackup バージョン 10.3 以降、クレデンシャルベースの認証は、NetBackup プライマリサーバーと Snapshot Manager の間の証明書ベースの TLS 認証に置き換えられました。これには、NetBackup Snapshot Manager の配備中にユーザーが次の詳細を指定する必要があります。

- (NBCA の場合): プライマリサーバーのホスト名、セキュリティ認証トークン、および Snapshot Manager FQDN ホスト名などの必須オプション。
- (ECA の場合): CA、キー、チェーン、CRL パスなどの追加オプション。

TLS 証明書の最小キーサイズ要件は 2048 ビットです。これは、NetBackup Snapshot Manager がインストールされている Linux ホストの暗号化ポリシーによって制御されます。

(Red Hat Enterprise Linux 8 プラットフォームの場合) Red Hat のナレッジベースの記事を参照してください。

(その他のサポート対象のオペレーティングシステムプラットフォームの場合)オペレーティングシステムベンダーのマニュアルを参照してください。

メモ: NetBackup Snapshot Manager を配備するときは、次のコマンドをコピーしてコマンドラインインターフェースに貼り付けると便利です。これを実行する場合、これらの例の中で自分の環境と異なる製品とビルドのバージョン、ダウンロードディレクトリのパスなどを置き換えます。

Podman での NetBackup Snapshot Manager インストールの前提条件:

次のコマンドを実行して、必要なパッケージ (`podman-plugins`、`lvm2`、`systemd-udev`、`udica`、`policycoreutils-devel`) をホストにインストールします。

```
# yum install -y lvm2-<version>

# yum install -y systemd-udev-<version>

# yum install -y podman-plugins

# yum install -y udica policycoreutils-devel
```

NetBackup Snapshot Manager のインストール

Docker 環境か Podman 環境かに応じて、次の適切な手順を実行します。

NetBackup Snapshot Manager をインストールするには

1 NetBackup Snapshot Manager イメージを、NetBackup Snapshot Manager を配備するシステムにダウンロードします。Veritas Technical Support Web サイトに移動します。

メモ: サポートサイトにログオンして、tar.gz イメージファイルをダウンロードする必要があります。

[製品 (Products)]ドロップダウンで[NetBackup]を選択し、[バージョン (Version)]ドロップダウンで必要なバージョンを選択します。[参照 (Explore)]をクリックします。[ベースおよびアップグレードインストーラ (Base and upgrade installers)]をクリックします。

Docker および Podman 環境での NetBackup Snapshot Manager イメージ名は次のような形式です。

```
NetBackup_SnapshotManager_<version>.tar.gz
```

メモ: 実際のファイル名は、リリースバージョンによって異なる場合があります。

---

2 次のコマンドを使用してイメージファイルを展開します。

```
tar -xvf NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
```

次のコマンドを使用してコンテンツを一覧表示します。

```
# ls
NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
netbackup-flexsnap-11.1.x.x-xxxx.tar.gz
flexsnap_preinstall.sh
```

3 次のコマンドを実行して、NetBackup Snapshot Manager ホストのインストールを準備します。

```
# sudo ./flexsnap_preinstall.sh
```

4 次のコマンドオプションを使用してヘルプを構成し、インストールします。

構成: `# flexsnap_configure -h`

```
Usage: flexsnap_configure [OPTIONS] <COMMAND> [CMD_OPTIONS]
NetBackup Snapshot Manager (11.1.x.x-xxxx) configuration script


Options:
  -h, --help
        Print this message and exit

Command:
```

backup	Snapshot Manager メタデータのバックアップを作成するために使用します。
certs	証明書データを一覧表示して分析します。
crl	Snapshot Manager の CRL データベースを一覧表示または更新するために使用します。
dm	指定したデータムーバー ID を再作成してログインするために使用します。
install	Snapshot Manager スタックをホストにインストールまたはアップグレードするために使用します。
recover	指定した tar を使用して Snapshot Manager メタデータのバックアップをリカバリするために使用します。
renew	Snapshot Manager 証明書を更新するために使用します。
restart	ホストで Snapshot Manager サービスを再起動するために使用します。
serverinfo	CLI をトラブルシューティングして NetBackup および Snapshot Manager サーバー情報を取得します。
start	ホストで Snapshot Manager サービスを起動するために使用します。
status	Snapshot Manager または拡張機能の健全性状態を取得するために使用します。
stop	ホストで Snapshot Manager サービスを停止するために使用します。

truststore	Snapshot Manager トラストストアを一覧表示または更新します。
uninstall	Snapshot Manager スタックをホストからアンインストールするために使用します。
updatecil	権限拒否問題を解決するために SELinux ポリシーを更新するために使用します。
updatedb	NetBackup の詳細を使用して「クライアント」データベースを更新するために使用します。
verify	Snapshot Manager の内部証明書、外部証明書、または指定した証明書を検証するために使用します。
verifycert	証明書の検証チェックを実行するために使用します。

```
Run flexsnap_configure <COMMAND> --help for more information.
```

インストール: `# flexsnap_configure install -h`

```
Usage: flexsnap_configure install [OPTIONS]
```

オプション	説明
--add-host <string>	(オプション) カスタムホストから IP へのマッピング (`host:ip`) を追加します。`host:ip` の組み合わせごとに複数回渡すことができます。
--ca <ca>	ルート CA ファイルの絶対パス。
--chain <chain>	ルート CA 証明書を除いたすべての中間 CA とサーバー証明書を含む証明書チェーンの絶対パス。
--crlcheck <level>	CRL を使用して Snapshot Manager が証明書失効状態チェックを実行する方法を制御します。値には、0 (disable)、1 (leaf)、2 (chain) を指定できます。デフォルトは 1 (leaf) です。
--crlpath <directory>	CDP ベース以外の CRL 検証の CRL ディレクトリの場所を指定します。認証局に Snapshot Manager ホストからアクセスできない場合に便利です。
--extension	Snapshot Manager 拡張機能をインストールします。新規インストールの場合は、--extname と --snapshot-manager を指定する必要があります。
--extname <name>	Snapshot Manager 拡張機能の識別名。
--hostnames <IP/FQDN>	Snapshot Manager のカンマ区切りの IP/FQDN。
--http-proxy <URI>	(オプション) http プロキシを配備に渡します。 プロキシ入力形式: {http}://[username:password@]{fqdn|ip}[:port]
--https-proxy <URI>	(オプション) https プロキシを配備に渡します。 プロキシ入力形式: {https}://[username:password@]{fqdn|ip}[:port]
-i	対話形式インストールの場合。
--key <key>	サーバー証明書の秘密鍵のパス。
--no-proxy <URI>	(オプション) no プロキシを配備に渡します。
--no-proxy <hostnames>	(オプション) プロキシサーバーをバイパスできるホスト。たとえば、localhost,mycompany.com,<ip address> です。 --http-proxy と --https-proxy を指定する必要があります。
--level <level>	証明書の失効の確認方法を制御します。指定可能な値は leaf (デフォルト)、chain、または disable です。
--path <install_path>	Snapshot Manager のインストールパス (デフォルト: `/cloudpoint`)。

オプション	説明
--passphrase <file>	キーストアにアクセスする際に使用するパスフレーズを含むファイルのパスを指定します。ファイルの最初の行がパスフレーズとして使用されます。
--port <port_number>	Snapshot Manager の Nginx ポート (デフォルト: 443)。
--primary <IP/FQDN>	NetBackup のプライマリサーバー IP または FQDN。
--snapshot-manager <IP/FQDN>	NetBackup Snapshot Manager サーバーの IP、FQDN、またはプライベートホスト名。
--subnet4 <string>	(オプション) CIDR 形式の IPv4 サブネット。
--subnet6 <string>	(オプション) CIDR 形式の IPv6 サブネット。
--token <token>	再発行または標準トークン。Snapshot Manager 拡張機能の場合は、ワークフロートークンとして機能します。 (必須) 対話形式インストールの場合。 (オプション) Snapshot Manager 配備で NetBackup プライマリセキュリティ設定が中または低の場合。
--kind <kind>	chain オプションを指定している場合にのみ、証明書チェーンが表示されます。all オプションを指定している場合は、証明書の詳細が出力されます (デフォルト)。「basic」オプションを指定している場合は、証明書の最小の詳細が表示されます。

5 NetBackup Snapshot Manager の対話型および非対話型インストール:

NetBackup Snapshot Manager の対話型インストール (NBCA/ECA)

- NetBackup Snapshot Manager ホストがプロキシサーバーの背後にある場合:

```
# flexsnap_configure install -i --no-proxy <no_proxy_value>
--http-proxy <http_proxy_value> --https-proxy
<https_proxy_value>
```

- NetBackup Snapshot Manager/プライマリサーバーがプライベートホスト名で構成されている場合:

```
# flexsnap_configure install -i --add-host <nbsm_hostname>:<IP>
--add-host <primary_hostname>:<IP>
```

- カスタムパスでの NetBackup Snapshot Manager のインストール:

```
# flexsnap_configure install -i --path <installation_path>
```

メモ: flexsnap_configure CLI は、権限フラグを暗黙的に使用します (-u 0)。

対話型 CLI (NBCA) では、インストーラに次のようなメッセージが表示されます:

```
# flexsnap_configure install -i
Please provide NetBackup Primary details:
NetBackup primary server IP Address or FQDN: <nbu_primary_fqdn>
Start configuring with NetBackup CA certificate.
Provide NetBackup authentication token: <security_token>
NetBackup Snapshot Manager hostname for TLS certificate (64
char FQDN limit): <snapshot_manager_fqdn>
Port (default:443):
Configuration started at time: Wed Jan  3 05:33:08 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21)
 ...done
Configuration complete at time Wed Jan  3 05:37:54 UTC 2024!
Please register Snapshot Manager with NetBackup primary server
```

ECA の対話型 CLI では、インストーラに次のようなメッセージが表示されます:

```
# flexsnap_configure install -i
Please provide NetBackup Primary details:
NetBackup primary server IP Address or FQDN: <nbu_primary_fqdn>
Start configuring external CA certificate.
Absolute path of the root CA certificate file: <root_ca_file>
Absolute path of server private key file: <server_key_file>
```

```
Absolute path of server certificate chain: <server_chain_file>
Absolute path of key passphrase file (Press ENTER if keyfile
is non encrypted): <server_passphrase_file>
Absolute path of CRL directory (Press ENTER for CDP based CRL
 check): <crl_path>
CRL check level, Press ENTER for default 1 i.e. LEAF (0:
DISABLE, 1: LEAF and 2:CHAIN): <crl_level>
NetBackup Snapshot Manager hostname for TLS certificate (64
char FQDN limit): <snapshot_manager_fqdn>
Port (default:443): <snapshot_manager_port>
Configuration started at time: Tue Jan  2 10:44:07 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21)
 ...done
Configuration complete at time Tue Jan  2 10:49:02 UTC 2024!
Please register Snapshot Manager with NetBackup primary server
```

NetBackup CA (NBCA) を使用した NetBackup Snapshot Manager の非対話型インストール

- NetBackup プライマリサーバーのセキュリティレベルが MEDIUM であるか、Snapshot Manager ホスト名がプライマリサーバーで認識されている場合:

  ```
  # flexsnap_configure install --primary <primary> --hostnames
  <nbsm_ip_or_fqdn>
  ```

- NetBackup プライマリサーバーのセキュリティレベルが HIGH または VERY HIGH の場合:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn>
```

- NetBackup Snapshot Manager ホストがプロキシサーバーの背後にある場合:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn> --no-proxy
<no_proxy_value> --http-proxy <http_proxy_value> --https-proxy
<https_proxy_value>
```

- NetBackup Snapshot Manager/プライマリサーバーがプライベートホスト名で構成されている場合:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn> --add-host
<nbsm_hostname:IP> --add-host <primary_hostname:IP>
```

- カスタムパス/ポートでの NetBackup Snapshot Manager のインストール:

```
# flexsnap_configure install --primary <primary> --token
<standard_token> --hostnames <nbsm_ip_or_fqdn> --path
<installation_path> --port <port>
```

非対話型 CLI (NBCA) では、インストーラに次のようなメッセージが表示されます:

```
# flexsnap_configure install --primary <nbu_primary_fqdn>
--token <security_token> --hostnames <snapshot_manager_fqdn>
Start configuring with NetBackup CA certificate.
Configuration started at time: Wed Jan  3 05:33:08 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21)
```

```
 ...done
Configuration complete at time Wed Jan  3 05:37:54 UTC 2024!
Please register Snapshot Manager with NetBackup primary server
```

外部 CA (ECA) を使用した NetBackup Snapshot Manager の非対話型インストール

- 暗号化された秘密鍵:

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
--passphrase <file>
```

- 暗号化されていない秘密鍵:

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
```

- ユーザーが指定した CRL パスまたは CRL の確認を使用する場合:

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
--crlpath <directory> --crlcheck <level>
```

- NetBackup Snapshot Manager ホストがプロキシサーバーの背後にある場合:

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
--no-proxy <no_proxy_value> --http-proxy <http_proxy_value>
--https-proxy <https_proxy_value>
```

- NetBackup Snapshot Manager/プライマリサーバーがプライベートホスト名で構成されている場合:

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file>
--add-host <nbsm_hostname:IP> --add-host <primary_hostname:IP>
```

- カスタムパス/ポートでの NetBackup Snapshot Manager のインストール:

```
# flexsnap_configure install --primary <primary> --hostnames
<nbsm_ip_or_fqdn> --ca <path_of_root_CA> --key
<path_of_private_key_file> --chain <server_chain_file> --path
<installation_path> --port <port>
```

非対話型 CLI (ECA) では、インストーラに次のようなメッセージが表示されます:

```
# flexsnap_configure install --primary <nbu_primary_fqdn>
--hostnames <snapshot_manager_fqdn> --ca <root_ca_file> --key
 <server_key_file> --chain <server_chain_file> --passphrase
<server_passphrase_file> --crlpath <crl_path> --crlcheck
<level>
Start configuring external CA certificate.
Configuration started at time: Tue Jan  2 11:35:21 UTC 2024
Podman server version: 4.2.0
This is a fresh install of NetBackup Snapshot Manager
11.1.x.x-xxxx
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Creating container: flexsnap-postgresql ...done
Creating container: flexsnap-rabbitmq ...done
Creating container: flexsnap-certauth ...done
Creating container: flexsnap-api-gateway ...done
Creating container: flexsnap-coordinator ...done
Creating container: flexsnap-listener ...done
Creating container: flexsnap-agent ...done
Creating container: flexsnap-onhostagent ...done
Creating container: flexsnap-scheduler ...done
Creating container: flexsnap-policy ...done
Creating container: flexsnap-notification ...done
Creating container: flexsnap-nginx ...done
Waiting for Snapshot Manager configuration to complete (21/21)
 ...done
Configuration complete at time Tue Jan  2 11:40:12 UTC 2024!
Please register Snapshot Manager with NetBackup primary server
```

パラメータ	説明
次のパラメータは、インスタンスがプロキシサーバーを使用する場合にのみ必要です	
<http_proxy_value>	すべての接続に対して HTTP プロキシとして使用される値を表します。 たとえば、"http://proxy.mycompany.com:8080/" です。
<https_proxy_value>	すべての接続に対して HTTPS プロキシとして使用される値を表します。 たとえば、"http://proxy.mycompany.com:8080/" です。

パラメータ	説明
<no_proxy_value>	プロキシサーバーをバイパスできるアドレスを表します。このパラメータでは、ホスト名、IP アドレス、ドメイン名を指定できます。 複数のエントリを区切るにはカンマ (,) を使用します。たとえば、"localhost,mycompany.com,192.168.0.10:80" です。 注意: NetBackup Snapshot Manager がクラウドに配備される場合は、このパラメータで次の値をそれぞれ設定していることを確認します。 ■ AWS インスタンスの場合: 169.254.169.254 ■ GCP 仮想マシンの場合: 169.254.169.254,metadata,metadata.google.internal ■ Azure 仮想マシンの場合: 169.254.169.254 NetBackup Snapshot Manager はこれらのアドレスを使用して、インスタンスメタデータサービスからインスタンスメタデータを収集します。

SSL ベースのプロキシサーバーのルート CA 証明書の設定

(Azure ベースの VM の配備にのみ適用可能) プロキシのルート CA 証明書は、次のコマンドを使用して、NetBackup Snapshot Manager を配備した後に提供できます。

```
flexsnap_configure truststore --ca <Root CA Cert File>
```

6 ホストにロードされている docker イメージを表示するには、次の docker コマンドを使用します。

- (Docker の場合) # sudo docker images
- (Podman の場合) # sudo podman images

出力は次のようになります。

```
REPOSITORY             TAG             IMAGE ID       CREATED
   SIZE
veritas/flexsnap-deploy       11.1.x.x-xxxx   5260748d9eab   18
minutes ago   586MB
veritas/flexsnap-rabbitmq     11.1.x.x-xxxx   cff89dc78a2f   18
minutes ago   546MB
veritas/flexsnap-postgresql   11.1.x.x-xxxx   0b87fe88cf94   18
minutes ago   537MB
veritas/flexsnap-nginx        11.1.x.x-xxxx   ee1cf2a3159e   18
minutes ago   649MB
veritas/flexsnap-fluentd      11.1.x.x-xxxx   a384e3fc4167   19
```

```
minutes ago    681MB
veritas/flexsnap-core          11.1.x.x-xxxx    2393b221bf19    20
minutes ago    916MB
veritas/flexsnap-datamover     11.1.x.x-xxxx    8254c537bdb4    38
hours ago      1.18GB
```

7 コマンドプロンプトでプロンプトが表示されたら、次の詳細を入力します。

パラメータ	説明
認証トークン	NetBackup 認証局 (CA) を使用すると、セキュリティ証明書を正常に配備するために、インストーラで認証トークンが必要になります。
TLS 証明書のホスト名 (Host name for TLS certificate)	NetBackup Snapshot Manager ホストの IP アドレスまたは FQDN (完全修飾ドメイン名) を指定します。 指定した名前または IP アドレスは、NetBackup Snapshot Manager の構成に使用するホスト名のリストに追加されます。インストーラはこの名前を使用して、NetBackup Snapshot Manager ホストのサーバー証明書を生成します。
ポート (Port)	NetBackup Snapshot Manager が通信できるポートを指定します。デフォルトはポート 443 です。

インストーラに次のようなメッセージが表示されます。

```
Configuring admin credentials ...done
Waiting for Snapshot Manager configuration to complete (22/22)
...done
Configuration complete at time Thu Jun 9 06:15:43 UTC 2022!
```

メモ: NetBackup Snapshot Manager を配備した後、システムの IPv6 インターフェースが無効でないことを確認します。

---

8 これにより NetBackup Snapshot Manager の配備プロセスは終了します。次の手順では、NetBackup Snapshot Manager を Cohesity NetBackup プライマリサーバーに登録します。

NetBackup Snapshot Manager がクラウドに配備されている場合の手順については、『NetBackup Web UI クラウド管理者ガイド』を参照してください。

メモ: NetBackup Snapshot Manager を再起動する必要がある場合は、`flexsnap_configure restart` コマンドを使用して環境データが保持されるようにします。

p.66 の「NetBackup Snapshot Manager の再起動」を参照してください。

CRL パスの指定

- CDP ベース以外の CRL の検証: ユーザーは、インストール中に、外部 CA の失効した証明書を含むディレクトリへのパスを指定できます。*ECA_CRL_PATH* パラメータは `/cloudpoint/openv/netbackup/bp.conf` ファイルに追加されます。パスは、外部 CA の証明書失効リスト (CRL) が保存されている `/cloudpoint/eca/crl` ディレクトリのパスを常に指します。
- CDP ベースのインストール: Snapshot Manager は、CDP (CRL 配布ポイント) を使用してピアホストの証明書の失効状態を検証します。

メモ: Podman ベースの配備の CIL ポリシーは自動的にロードされ、RHEL 8 と 9 に適用されます。

CIS レベル 2 v2 で構成されたホストへの NetBackup Snapshot Manager のインストール

CIS (Center for Internet Security) は、さまざまなソフトウェアシステムに対して一連のベンチマークを提供します。これらのベンチマークは、ソフトウェアとシステムを強化するために使用されます。CIS にはレベル 1、2、3 のベンチマークがあります。

NetBackup Snapshot Manager 環境は、Red Hat Enterprise Linux 8 マシンの CIS レベル 2 v2 ベンチマークでサポートされるようになりました。

CIS レベル 2 v2 で構成されたホストに NetBackup Snapshot Manager をインストールするには

1. CIS レベル 2 v2 のベンチマークを使用した Red Hat Enterprise Linux 8 を準備します。
2. CIS ホストでは、iptables ファイアウォールがサポートされます。
3. 次のセクションで説明するすべての「NetBackup Snapshot Manager ホストの要件」を満たしていることを確認します。

   p.19 の「 システム要件への準拠」を参照してください。
4. IPv4 および IPv6 転送が有効になっていることを確認します。

5 OpenScap ツールを使用して、NetBackup Snapshot Manager でスキップされた次のルールセットでマシンを修復します。

```
xccdf_org.ssgproject.content_rule_package_iptables-services_removed
xccdf_org.ssgproject.content_rule_sysctl_net_ipv6_conf_all_forwarding
xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_ip_forward
xccdf_org.ssgproject.content_rule_accounts_tmout
xccdf_org.ssgproject.content_rule_auditd_data_retention_admin_space_left_action

xccdf_org.ssgproject.content_rule_auditd_data_retention_max_log_file_action

xccdf_org.ssgproject.content_rule_auditd_data_retention_space_left_action

xccdf_org.ssgproject.content_rule_banner_etc_issue
xccdf_org.ssgproject.content_rule_banner_etc_issue_net
xccdf_org.ssgproject.content_rule_grub2_uefi_password
xccdf_org.ssgproject.content_rule_mount_option_var_noexec
xccdf_org.ssgproject.content_rule_package_bind_removed
xccdf_org.ssgproject.content_rule_package_cups_removed
xccdf_org.ssgproject.content_rule_package_dhcp_removed
xccdf_org.ssgproject.content_rule_package_dovecot_removed
xccdf_org.ssgproject.content_rule_package_httpd_removed
xccdf_org.ssgproject.content_rule_package_mcstrans_removed
xccdf_org.ssgproject.content_rule_package_net-snmp_removed
xccdf_org.ssgproject.content_rule_package_openldap-clients_removed

xccdf_org.ssgproject.content_rule_package_rsync_removed
xccdf_org.ssgproject.content_rule_package_samba_removed
xccdf_org.ssgproject.content_rule_package_setroubleshoot_removed

xccdf_org.ssgproject.content_rule_package_squid_removed
xccdf_org.ssgproject.content_rule_package_talk_removed
xccdf_org.ssgproject.content_rule_package_telnet-server_removed

xccdf_org.ssgproject.content_rule_package_tftp-server_removed
xccdf_org.ssgproject.content_rule_package_vsftpd_removed
xccdf_org.ssgproject.content_rule_package_xinetd_removed
xccdf_org.ssgproject.content_rule_package_xorg-x11-server-common_removed

xccdf_org.ssgproject.content_rule_package_ypserv_removed
xccdf_org.ssgproject.content_rule_rsyslog_files_permissions
xccdf_org.ssgproject.content_rule_selinux_state
xccdf_org.ssgproject.content_rule_service_firewalld_enabled
```

```
xccdf_org.ssgproject.content_rule_set_firewalld_default_zone
xccdf_org.ssgproject.content_rule_sudo_require_authentication
xccdf_org.ssgproject.content_rule_sudo_require_reauthentication
```

次に、remediate オプションを指定して oscap コマンドを使用する例を示します。

```
# oscap xccdf eval --skip-rule <x> --skip-rule <y> --skip-rule
<z> --results demo-remediate2.xml --profile
xccdf_org.ssgproject.content_profile_cis --remediate
/usr/share/xml/scap/ssg/content/ssg-rhel8-ds-1.2.xml
```

上記の例で示すように、上記のすべてのルールを --skip-rule オプションに追加します。これにより、指定したルールがスキップされ、レポートが生成されます。

詳しくは、Red Hat のシステムデザインガイドを参照してください。

6 NetBackup Snapshot Manager をインストールし、NetBackup プライマリサーバーに登録します。

7 Podman の通信が正しく動作していることを確認します。Red Hat のナレッジベースの記事を参照してください。

8 CIS レベル 2 v2 VM の作業負荷を保護するためにエージェントレス構成を実行する場合は、次のセクションで説明する要件を満たしていることを確認し、エージェントレス VM 作業負荷の /tmp フォルダから noexec 権限を削除します。

p.239 の「エージェントレス構成の前提条件」を参照してください。

NetBackup Snapshot Manager の配備に成功した後、openscap CIS のスコア 97% を達成することができました。

NetBackup Snapshot Manager への接続のセキュリティ保護

- サポート対象のシナリオ:
  - プライマリサーバーと Snapshot Manager は、ECA または NBCA を使用している必要があります。
  - NBCA と ECA の混合モードの場合は、NetBackup Snapshot Manager インストールの ECA モードに進みます。
- サポート対象外のシナリオ: NBCA を使用したプライマリと、ECA を使用した NetBackup Snapshot Manager、およびその逆。

NetBackup Snapshot Manager では、外部 CA の CRL を /cloudpoint/eca/crl ファイルにアップロードできます。crl ディレクトリが存在しないか空の場合、アップロードした CRL は機能しません。

データムーバーコンテナの場合は、/cloudpoint/openv/netbackup/bp.conf ファイルの *ECA_CRL_PATH* パラメータに対して /cloudpoint/eca/crl のパスを追加します。

次の 3 つのパラメータを調整できます。/cloudpoint/flexsnap.conf ファイルの *eca* セクションにエントリを追加できます。

表 3-1 ECA パラメータ

パラメータ	デフォルト	値	注釈
eca_crl_check	0 (Disable)	0 (disable) 1 (leaf) 2 (chain)	証明書の確認レベル。オンプレミスまたはクラウドの作業負荷に接続している NetBackup Snapshot Manager ホストの CRL/OCSP 検証レベルを制御するために使用します。 ■ 0 (disable): 検証時に CRL/OCSP は実行されません ■ 1 (leaf): リーフにのみ CRL/OSCP 検証が実行されます。 ■ 2 (chain): チェーン全体に CRL/OSCP 検証が実行されます。
eca_crl_refresh_hours	24	0 から 4830 の間の数値	証明書の CDP URL を介して CA から NetBackup Snapshot Manager CRL キャッシュを更新する間隔 (時間)。/cloudpoint/eca/crl ファイルが存在し、CRL ファイルが含まれている場合、このオプションは適用できません。0 に設定すると、キャッシュは更新されません。
eca_crl_path_sync_hours	1	1 から 720 の間の数値	/cloudpoint/eca/crl ファイルの NetBackup Snapshot Manager CRL キャッシュを更新する時間間隔 (時間)。/cloudpoint/eca/crl ファイルが存在しない、または空の場合、このオプションは適用できません。

詳しくは『NetBackup™ セキュリティおよび暗号化ガイド』の次のセクションを参照してください。

- ホスト ID ベースの証明書失効リストについて
- 証明書配備中に認証トークンが必要である場合

メモ: /cloudpoint/flexsnap.conf ファイル内でいずれかの ECA 調整機能を手動で追加または修正すると、キャッシュは検証されません。

Snapshot Manager の証明書の無効化

NetBackup CA と証明書について詳しくは、『NetBackup™ セキュリティおよび暗号化ガイド』の「NetBackup CA と NetBackup 証明書」の章を参照してください。

次の表に、Snapshot Manager で証明書を無効化するために実行する再生成手順を示します。

使用例	コマンド

CA の移行	■ NBCA から ECA:
	`# flexsnap_configure renew --ca /eca2/trusted/cacerts.pem --key /eca2/private/key.pem --chain /eca2/cert_chain.pem`
	`Enrolling external CA certificates with NetBackup...`
	`Snapshot Manager certificate is renewed.`
	■ ECA から NBCA:
	`# flexsnap_configure renew --token <reissue-token>`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`

NBCA の場合の無効化後の証明書の再生成	`# flexsnap_configure renew --token <reissue-token>`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`

ECA の場合の無効化後の証明書の再生成	`# flexsnap_configure renew --ca /eca2/trusted/cacerts.pem --key /eca2/private/key.pem --chain /eca2/cert_chain.pem`
	`Enrolling external CA certificates with NetBackup...`
	`Snapshot Manager certificate is renewed.`

ECA/NBCA の場合の移行後の証明書の再生成	`# flexsnap_configure renew --hostnames new-nbsm.veritas.com --token <authentication-token>`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`
	`Please run 'flexsnap_configure renew --internal --hostnames <nbsm_fqdn>`
	`to renew Snapshot Manager's internal CA and certificates.`

使用例	コマンド
拡張機能の証明書の再生成	`# flexsnap_configure renew --extension --primary <nbsm_fqdn> --token <extension_token>`

証明書のローテーション	`# flexsnap_configure renew --force`
	`Generating new NetBackup Host-ID certificate...`
	`Snapshot Manager certificate is renewed.`

移行、ディザスタリカバリのシナリオの場合の内部 flexsnap CA 証明書	`# flexsnap_configure renew --internal --hostnames <nbsm_fqdn>`
	`Renewed Flexsnap CA ... skip`
	`Renewed rabbitmq certificate ... done`
	`Renewed postgresql certificate ... done`
	`Renewed listener certificate ... done`
	`Renewed workflow certificate ... done`
	`Renewed scheduler certificate ... done`
	`Renewed agent certificate ... done`
	`Renewed client certificate ... done`
	`Renewed certmaster certificate ... done`
	`Renewed agent certificate ... done`
	`Renewed notification certificate ... done`
	`Renewed client certificate ... done`
	`Renewed client certificate ... done`
	`Renewed mongodb certificate ... done`
	`Renewed coordinator certificate ... done`
	`Renewed config certificate ... done`
	`Renewed idm certificate ... done`
	`Renewed agent certificate ... done`
	`Renewed client certificate ... done`
	`Renewed policy certificate ... done`
	`Snapshot Manager's CA and certificates are renewed.`
	`Restart the Snapshot Manager stack using 'flexsnap_configure restart' to take effect.`

NetBackup HostID 証明書の秘密鍵を暗号化する NetBackup Snapshot Manager のパスフレーズのローテーション

BYO とクラウドスケールの配備では、パスフレーズを手動でローテーションする必要があります。

- BYO 配備の場合、NetBackup Snapshot Manager を停止し、次のオプションを指定して `flexsnap_configure` コマンドを使用します。

```
flexsnap_configure renew --rotate-passphrase
```

プロンプトが表示されたら、y キーを押して同意します。
この操作は、ホスト ID ベース証明書の秘密鍵を暗号化するパスフレーズのローテーションを実行します。

- Cloud Scale の配備の場合は、次のオプションを使用して `flexsnap_configure` を使用します。

```
kubctl exec -it <certauth pod> -n <namespace> flexsnap-config renew
--rotate-passphrase
```

- NetBackup Snapshot Manager を再起動します。

メモ: ECA 用に生成された秘密鍵は暗号化できる場合とできない場合があります。インストール時に暗号化された秘密鍵を提供するかどうかはユーザーが決めます。

NetBackup Snapshot Manager が正常にインストールされたことの確認

flexsnap_configure CLI を使用して構成の状態を確認するには、次のコマンドを実行します。

```
# flexsnap_configure status
```

コマンドの出力は次のようになります。

```
{ "healthy": "true", "start_time": "3 minutes ago", "uptime": "Up 3
 minutes ago", "status": "ok", "host": "localhost" }
```

または

物理マシンまたはインスタンスのコマンドラインで次のいずれかの操作を実行して、NetBackup Snapshot Manager が正常にインストールされたことを確認します。

- コマンドプロンプトで成功したことを示すメッセージが表示されることを確認します。

```
Configuration complete at time Fri Mar 13 06:15:43 UTC 2020!
```

メモ: NetBackup Snapshot Manager のインストールが失敗した場合、ユーザーはアンインストール手順を実行して古いコンテナと flexsnap ネットワークを削除し、インストールを再試行する必要があります。

p.302 の「NetBackup Snapshot Manager のアンインストールの準備」を参照してください。

- 次のコマンドを実行して、NetBackup Snapshot Manager サービスが稼働中であり、状態が UP として表示されることを確認します。

  Docker 環境の場合: `# sudo docker ps -a`

  Podman 環境の場合: `# sudo podman ps -a`

  コマンドの出力は次のようになります。

```
CONTAINER ID   IMAGE
COMMAND                  CREATED       STATUS
PORTS
                    NAMES
b13a96fbefa1   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"   4 hours ago   Up 4 hours

                    flexsnap-workflow-system-0-min
a3a6c801d7aa   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"   4 hours ago   Up 4 hours

                    flexsnap-workflow-general-0-min
b9cd09ab7797   veritas/flexsnap-nginx:11.1.x.x-xxxx
"/usr/sbin/nginx"        4 hours ago   Up 4 hours
0.0.0.0:443->443/tcp, :::443->443/tcp, 0.0.0.0:5671->5671/tcp,
:::5671->5671/tcp   flexsnap-nginx
7fd258cb575a   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-n…"   4 hours ago   Up 4 hours

                    flexsnap-notification
9c06318b001a   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-p…"   4 hours ago   Up 4 hours

                    flexsnap-policy
031f853377a5   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-s…"   4 hours ago   Up 4 hours

                    flexsnap-scheduler
dfbcaeda1463   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-a…"   4 hours ago   Up 4 hours

                    flexsnap-onhostagent
253e7284a945   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-a…"   4 hours ago   Up 4 hours

                    flexsnap-agent
d54eed8434fe   veritas/flexsnap-core:11.1.x.x-xxxx
```

```
"/usr/bin/flexsnap-l…"   4 hours ago   Up 4 hours

               flexsnap-listener
759e4ee9653b   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-c…"   4 hours ago   Up 4 hours

               flexsnap-coordinator
28c88bdc1ca2   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-g…"   4 hours ago   Up 4 hours
8472/tcp
                  flexsnap-api-gateway
dd5018d5e9f9   veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-c…"   4 hours ago   Up 4 hours
9000/tcp
                  flexsnap-certauth
0e7555e38bb9   veritas/flexsnap-rabbitmq:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours (healthy)
5671/tcp
                  flexsnap-rabbitmq
b4953f328e8d   veritas/flexsnap-postgresql:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours (healthy)
13787/tcp
                  flexsnap-postgresql
cf4a731c07a6   veritas/flexsnap-deploy:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours

               flexsnap-ipv6config
9407ea65a337   veritas/flexsnap-fluentd:11.1.x.x-xxxx
"/opt/VRTScloudpoint…"   4 hours ago   Up 4 hours
0.0.0.0:24224->24224/tcp, :::24224->24224/tcp
                  flexsnap-fluentd
```

メモ: イメージ名列に表示される数字 (`11.1.x.x-xxxx`) は、NetBackup Snapshot Manager のバージョンを表します。このバージョンは、インストールされる実際の製品バージョンによって異なる場合があります。

ここに表示されるコマンド出力は、ビューに合わせて切り捨てられる場合があります。実際の出力には、コンテナ名や使用されているポートなどの追加の詳細情報が含まれることがあります。

NetBackup Snapshot Manager の再起動

NetBackup Snapshot Manager を再起動する必要がある場合は、環境データが保持されるように正しく再起動することが重要です。

flexsnap_configure CLI を使用して Docker/Podman 環境で NetBackup Snapshot Manager を再起動するには、次のコマンドを実行します。

```
# flexsnap_configure restart
```

出力は次のようになります。

```
Restarting the services
Stopping services at time: Mon Jul 31 11:43:43 UTC 2023
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Mon Jul 31 11:44:04 UTC 2023
Starting services at time: Mon Jul 31 11:44:04 UTC 2023
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Starting container: flexsnap-rabbitmq ...done
Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Starting container: flexsnap-listener ...done
Starting services completed at time: Mon Jul 31 11:44:21 UTC 2023
```

4

NetBackup Snapshot Manager for Cloud 拡張機能の配備

この章では以下の項目について説明しています。

NetBackup Snapshot Manager 拡張機能のインストールを開始する前に

VM または管理対象の Kubernetes クラスタにインストールできる NetBackup Snapshot Manager 拡張機能は、計算インフラを柔軟に拡大して多数のジョブを処理し、ジョブの完了時に縮小できます。

メモ: NetBackup Snapshot Manager イメージバージョンと同じタグを使用していることを確認します。カスタムタグは使用できません。

NetBackup Snapshot Manager 拡張機能のインストールにも適用される、NetBackup Snapshot Manager をインストールする際の次の適切な準備手順を参照してください。

VM ベースの拡張機能の場合

- NetBackup Snapshot Manager 拡張機能をインストールする場所を決定します。
p.15 の「NetBackup Snapshot Manager for Cloud を実行する場所の決定」を参照してください。
- 環境がシステム要件を満たしていることを確認します。
p.19 の「 システム要件への準拠」を参照してください。
- NetBackup Snapshot Manager 拡張機能をインストールするインスタンスを作成するか、VM を準備します。
p.34 の「NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備」を参照してください。
- 拡張機能を配備する VM またはインスタンスに、Docker をインストールします。
p.34 の 表 2-10 を参照してください。
- NetBackup Snapshot Manager データを格納するボリュームを作成してマウントします。VM ベースの拡張機能の場合、ボリュームサイズは 30 GB になる場合があります。
p.35 の「NetBackup Snapshot Manager データを格納するボリュームの作成とマウント」を参照してください。
- インスタンスまたはメイン NetBackup Snapshot Manager ホストで特定のポートが開いており、必要なポートで拡張機能から保護対象のホストにアクセスできることを確認します。NetBackup Snapshot Manager ホストで RabbitMQ 通信を行う場合は、ポート 5671 および 443 を開く必要があります。

  メモ: ポート 443 の代わりにカスタムポートを使用する場合は、ファイアウォールでカスタムポートが開いていて、NetBackup Snapshot Manager 拡張機能と NetBackup Snapshot Manager 間の通信が許可されることを確認します。

拡張機能のインストールおよび構成処理について

Kubernetes ベースの拡張機能の場合

- *Azure の場合*: NetBackup Snapshot Manager ホストの容量を拡大縮小して多数の要求を同時に処理するために、NetBackup Snapshot Manager のクラウドベース拡張機能を Azure の管理対象 Kubernetes クラスタに配備できます。Azure でのホストと管理対象 Kubernetes クラスタの準備についての詳細:

p.75 の「Azure の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」を参照してください。

- *AWS の場合*: NetBackup Snapshot Manager ホストの容量を拡大縮小して多数の要求を同時に処理するために、NetBackup Snapshot Manager のクラウドベース拡張機能を AWS の管理対象 Kubernetes クラスタに配備できます。AWS でのホストと管理対象 Kubernetes クラスタの準備についての詳細:
  p.84 の「AWS の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」を参照してください。
- *GCP の場合*: NetBackup Snapshot Manager ホストの容量を拡大縮小して多数の要求を同時に処理するために、NetBackup Snapshot Manager のクラウドベース拡張機能を GCP の管理対象 Kubernetes クラスタ (GKE) に配備できます。GCP でのホストと管理対象 Kubernetes クラスタの準備についての詳細:
  p.93 の「GCP の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」を参照してください。

拡張機能のインストールおよび構成処理について

NetBackup Snapshot Manager 拡張機能をインストールして構成するには、ブラウザの NetBackup ユーザーインターフェースと、ローカルコンピュータまたはアプリケーションホストのコマンドラインインターフェースからタスクを実行します。

p.71 の「VM への拡張機能のインストール」を参照してください。

p.74 の「Azure の管理対象 Kubernetes クラスタ (AKS) への NetBackup Snapshot Manager 拡張機能のインストール」を参照してください。

p.83 の「AWS の管理対象 Kubernetes クラスタ (EKS) への NetBackup Snapshot Manager 拡張機能のインストール」を参照してください。

p.95 の「GCP (GKE) への拡張機能のインストール」を参照してください。

NetBackup Snapshot Manager 拡張機能のダウンロード

拡張機能をダウンロードするには

1. NetBackup Web UI にサインインします。
2. 左側で、[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択し、[Snapshot Manager]タブをクリックします。

   このペインには、プライマリサーバーに登録されているすべての NetBackup Snapshot Manager サーバーが表示されます。

3 目的の NetBackup Snapshot Manager 行で、右側の処理アイコンをクリックし、次に[拡張機能の追加 (Add extension)]を選択します。

メモ: VM ベースの拡張機能の場合、拡張機能をダウンロードする必要はありません。直接手順 7 と 8 に進み、トークンをコピーします。

4 管理対象 Kubernetes クラスタに拡張機能をインストールする場合は、[拡張機能の追加 (Add extension)]ダイアログボックスで、*[ダウンロード (download)]*ハイパーリンクをクリックします。

これにより、新しい Web ブラウザのタブが開きます。

[拡張機能の追加 (Add extension)]ダイアログボックスは、まだ閉じないでください。拡張機能を構成するときにこのダイアログボックスに戻り、検証トークンを生成します。

5 開いた新しいブラウザタブに切り替えて、[拡張機能の追加 (Add extension)]カードで[ダウンロード (Download)]をクリックします。拡張機能ファイル `nbu_flexsnap_extension.tar` がダウンロードされます。

6 ダウンロードしたファイルを NetBackup Snapshot Manager ホストにコピーし、コマンド `tar -xvf nbu_flexsnap_extension.tar` を実行して解凍します。

p.77 の「Azure (AKS) への拡張機能のインストール」を参照してください。

p.86 の「AWS (EKS) への拡張機能のインストール」を参照してください。

p.95 の「GCP (GKE) への拡張機能のインストール」を参照してください。

7 次に、検証トークンを生成するために、[拡張機能の追加 (Add extension)]ダイアログボックスで[トークンの作成 (Create Token)]をクリックします。

8 [トークンをコピー (Copy Token)]をクリックして、表示されたトークンをコピーします。次に、拡張機能の構成時にコマンドプロンプトでこのトークンを指定します。

メモ: トークンは 180 秒間のみ有効です。その時間枠内にトークンを使用しない場合は、新しいトークンを生成します。

VM への NetBackup Snapshot Manager 拡張機能のインストール

メモ: 現在、拡張機能は Azure Stack Hub 環境でのみサポートされます。

VM に拡張機能をインストールする際の前提条件

- NetBackup Snapshot Manager のインストール要件を満たすサポート対象の Ubuntu または RHEL システムで NetBackup Snapshot Manager イメージを選択し、ホストを作成します。
  p.34 の「NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備」を参照してください。
- リモートデスクトップを介してホストに接続できることを確認します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。
- ホストに Docker または Podman コンテナプラットフォームをインストールします。
  p.34 の 表 2-10 を参照してください。
- Veritas Technical Support Web サイトから OS 固有の NetBackup Snapshot Manager イメージをダウンロードします。
  Docker および Podman 環境での NetBackup Snapshot Manager イメージ名は次のような形式です。

  ```
  NetBackup_SnapshotManager_<バージョン>.tar.gz
  ```

  次のコマンドを実行して、NetBackup Snapshot Manager ホストのインストールを準備します。

  ```
  # sudo ./flexsnap_preinstall.sh
  ```

  メモ: 実際のファイル名は、リリースバージョンによって異なります。
- RHEL OS にインストールされている VM ベースの拡張機能の場合、SElinux のモードは「*permissive*」である必要があります。
- 保護対象ホストによって使用されるネットワークセキュリティグループは、指定されたポートで、拡張機能のインストール先となるホストからの通信を許可する必要があります。

VM への拡張機能のインストール

VM に NetBackup Snapshot Manager 拡張機能をインストールする前に、「「VM に拡張機能をインストールする際の前提条件」」を参照してください。

拡張機能をインストールするには

1 次の各コマンドを実行します。

- NetBackup Snapshot Manager 拡張機能の対話形式インストールの場合:

  ```
  # flexsnap_configure install --extension -i
  ```
- NetBackup Snapshot Manager 拡張機能の非対話形式インストールの場合:

```
# flexsnap_configure install --extension --snapshot-manager
<IP/FQDN> --token <extension_token> --extname <Extension_Name>
```

メモ: ベリタスでは、Snapshot Manager のインストールに flexsnap_configure CLI を使用することをお勧めします。Docker/Podman CLI を使用した Snapshot Manager のインストールは、RHEL 8/9 以外では非推奨となり、RHEL 8/9 では削除されています。

または

次の同等の Docker/Podman コマンドを使用して、Snapshot Manager 拡張機能をインストールします。

- Docker 環境の場合:

```
# sudo docker run -it --rm -u 0
-v /<absolute_path_of_cloudpoint_directory>:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<version> install_extension
```

- Podman 環境の場合:

```
# sudo podman run -it --rm -u 0
-v /<absolute_path_of_cloudpoint_directory>:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<version> install_extension
```

メモ: これは改行のない 1 つのコマンドです。

この手順で、NetBackup Snapshot Manager は次を実行します。

- 各 NetBackup Snapshot Manager サービスのコンテナを作成して実行します。

- nginx の自己署名のキーと証明書を作成します。

2 NetBackup Web UI に移動し、「NetBackup Snapshot Manager 拡張機能のダウンロード」セクションに記載されている手順 7 と 8 に従い、検証トークンと指紋を生成してコピーします。

p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

メモ: VM ベースの拡張機能の場合、拡張機能をダウンロードする必要はありません。直接手順 7 と 8 に進み、トークンをコピーします。

3 プロンプトが表示されたら、次の構成パラメータを指定します。

パラメータ	説明
IP address / FQDN	メイン NetBackup Snapshot Manager ホストの IP アドレスまたは FQDN を指定します。
Token	前の手順で取得したトークンを貼り付けます。
Extension Name Identifier	NetBackup UI に表示される拡張機能の識別名。
Fingerprint	前の手順で取得した指紋を貼り付けます。

インストーラに次のようなメッセージが表示されます。

```
Starting docker container: flexsnap-fluentd ...done
Starting docker container: flexsnap-ipv6config ...done
Starting docker container: flexsnap-listener ...done
```

これで、VM への NetBackup Snapshot Manager 拡張機能のインストールが完了しました。

拡張機能が正常にインストールされたことを確認するには

- コマンドプロンプトで成功したことを示すメッセージが表示されることを確認します。
- NetBackup Web UI で拡張機能が一覧表示されていることを確認します。
  [クラウド (Cloud)]、[NetBackup Snapshot Manager]タブの順に移動して[詳細設定 (Advanced Settings)]をクリックし、[NetBackup Snapshot Manager 拡張機能 (NetBackup Snapshot Manager extensions)]タブに移動して確認します。
- 次のコマンドを実行し、NetBackup Snapshot Manager コンテナが稼働中であり、状態に UP と表示されることを確認します。

  ```
  # sudo docker ps -a
  ```

  コマンドの出力は次のようになります。

```
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
e67550304195 veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"
13 minutes ago Up 13 minutes
flexsnap-core-system-b17e4dd9f6b04d41a08e3a638cd91f61-0
26472ebc6d39 veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-w…"
13 minutes ago Up 13 minutes
flexsnap-core-general-b17e4dd9f6b04d41a08e3a638cd91f61-0
4f24f6acd290 veritas/flexsnap-core:11.1.x.x-xxxx
"/usr/bin/flexsnap-l…"
13 minutes ago Up 13 minutes flexsnap-core
4d000f2d117d veritas/flexsnap-:11.1.x.x-xxxx "/root/ipv6_configur…"

13 minutes ago Exited (137) 13 minutes ago flexsnap-deploy
92b5bdf3211c veritas/flexsnap-fluentd:11.1.x.x-xxxx
"/root/flexsnap-flue…"
13 minutes ago Up 13 minutes 5140/tcp, 0.0.0.0:24224->24224/tcp
flexsnap-fluentd
db1f0bff1797 veritas/flexsnap-datamover:11.1.x.x-xxxx
"/entrypoint.sh -c d…"
13 minutes ago Up 13 minutes
flexsnap-datamover.134b6158ea5a443dba3c489d553098c5
c4ae0eb61fb0 veritas/flexsnap-datamover:11.1.x.x-xxxx
"/entrypoint.sh -c d…"
13 minutes ago Up 13 minutes
flexsnap-datamover.8e25f89f04e74b01b4fe04e7e5bf8644
1bcaa2b646fb veritas/flexsnap-datamover:11.1.x.x-xxxx
"/entrypoint.sh -c d…"
13 minutes ago Up 13 minutes
flexsnap-datamover.b08591bdde0f445f83f4ada479e6ddfd
```

Azure の管理対象 Kubernetes クラスタ (AKS) への NetBackup Snapshot Manager 拡張機能のインストール

NetBackup Snapshot Manager ホストの容量を拡大縮小して多数の要求を同時に処理するために、NetBackup Snapshot Manager のクラウドベース拡張機能を Azure の管理対象 Kubernetes クラスタに配備できます。

メモ: Veritas は、Kubernetes クラスタの Snapshot Manager に Kubernetes 拡張機能を登録することをお勧めしません。

概要

- 適切なネットワークおよび構成が設定され、特定の役割を持つ Azure の管理対象 Kubernetes クラスタがすでに配備されている必要があります。クラスタは NetBackup Snapshot Manager と通信できる必要があります。
  必要な役割は、`Azure Kubernetes Service RBAC` **ライター**、`AcrPush`、`Azure Kubernetes Service` **クラスタユーザーロール**です。
  サポートされる Kubernetes のバージョンについては、NetBackup Snapshot Manager のハードウェア互換性リスト (HCL) を参照してください。
- 既存の Azure コンテナレジストリを使用するか、新しいレジストリを作成します。また、管理対象 Kubernetes クラスタに、コンテナレジストリからイメージを取得するためのアクセス権があることを確認します。
- Azure の管理対象 Kubernetes クラスタで、手動で拡大縮小するか「自動スケール (Autoscaling)」を有効にした状態で、NetBackup Snapshot Manager 作業負荷の専用ノードプールを作成する必要があります。自動スケール機能を使用すると、必要に応じて自動的にノードのプロビジョニングとプロビジョニング解除を行って、ノードプールを動的に拡大縮小できます。
- NetBackup Snapshot Manager 拡張機能のイメージ (`flexsnap-deploy`、`flexsnap-core`、`flexsnap-fluentd`、`flexsnap-datamover`) を Azure コンテナレジストリにアップロードする必要があります。

Azure の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件

- NetBackup Snapshot Manager のインストール要件を満たすサポート対象の Ubuntu または RHEL システムで NetBackup Snapshot Manager イメージを選択し、ホストを作成します。
  p.34 の「NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備」を参照してください。
- ジョブの実行中にクラスタを拡大または縮小することはお勧めしません。これを行うと、ジョブが失敗する可能性があります。事前にクラスタサイズを設定してください。
- メイン NetBackup Snapshot Manager ホストでポート 5671 が開いていることを確認します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。
- ノードプールが構成されている仮想マシンスケールセットのパブリック IP は、保護対象の作業負荷でポート 22 を介して通信できる必要があります。

- Docker または Podman コンテナプラットフォームをホストにインストールし、コンテナサービスを起動します。
  p.34 の 表 2-10 を参照してください。
- Azure 環境内で NetBackup Snapshot Manager ホストが Kubernetes クラスタにアクセスするための準備を行います。
  - Azure CLI をインストールします。詳しくは、Azure のマニュアルを参照してください。
  - Kubernetes CLI をインストールします。詳しくは、Kubernetes のサイトを参照してください。
  - Azure 環境にログインし、Azure CLI で次のコマンドを実行して、Kubernetes クラスタにアクセスします。

    ```
    # az login --identity
    # az account set --subscription <subscriptionID>
    # az aks get-credentials --resource-group <resource_group_name>
    --name <cluster_name>
    ```
- NetBackup Snapshot Manager イメージのプッシュ (アップロード) 先となる Azure コンテナレジストリを作成するか、利用可能な場合は既存のレジストリを使用します。Azure のマニュアルを参照してください。
- ホストシステムから `kubectl` およびコンテナレジストリコマンドを実行するには、VM とクラスタに次の役割の権限を割り当てます。[共同作成者 (Contributor)]、[所有者 (Owner)]、またはすべてのリソースを管理するためのフルアクセス権を付与する任意のカスタム役割を割り当てられます。
  - 仮想マシンに移動し、左側の[ID (Identity)]をクリックします。
    [システム割り当て (System assigned)]タブで、[状態 (Status)]を[オン (ON)]に切り替えます。
    [Azure ロールの割り当て (Azure role assignment)]をクリックし、[ロールの割り当ての追加 (Add role assignments)]をクリックし、[スコープ (Scope)]として[サブスクリプション (Subscription)]または[リソースグループ (Resource Group)]を選択します。
    [役割 (Role)]を選択し、次の役割を割り当てます。
    Azure Kubernetes Service RBAC ライター、AcrPush、Azure Kubernetes Service クラスタユーザーロールを選択し、[保存 (Save)]をクリックします。
  - Kubernetes クラスタに移動し、左側の[アクセス制御 (IAM)(Access Control (IAM))]をクリックします。
    [ロールの割り当ての追加 (Add role assignments)]をクリックし、[役割 (Role)]を[コントリビュータ (Contributor)]として選択します。
    [仮想マシン (Virtual Machines)]として[アクセス権を割り当てる (Assign access to)]を選択し、ドロップダウンから VM を選択して[保存 (Save)]をクリックします。

- StorageClass を定義する際は、NFS プロトコルを使用した Azure ファイルに CSI プロビジョナを使用することを検討してください。
  例:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: test-sc
parameters:
  skuName: Premium_LRS
  protocol: nfs
provisioner: file.csi.azure.com
reclaimPolicy: Retain
volumeBindingMode: WaitForFirstConsumer
```

- ホストシステムのコマンドラインインターフェースから NetBackup Snapshot Manager の名前空間を作成します。

```
# kubectl create namespace cloudpoint-system
```

- 次に、Azure で新たに作成するか既存の管理対象 Kubernetes クラスタを使用して、NetBackup Snapshot Manager 専用の新しいノードプールを追加します。必要に応じて自動スケールを構成します。

- Azure プラグインが構成されていることを確認します。
  p.171 の「Microsoft Azure プラグインの構成に関する注意事項」を参照してください。

Azure (AKS) への拡張機能のインストール

Azure の管理対象 Kubernetes クラスタ (AKS) に NetBackup Snapshot Manager 拡張機能をインストールする前に次を実行してください。

- p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

- p.75 の「Azure の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」を参照してください。

拡張機能をインストールするには

1. 拡張機能スクリプト `nbu_flexsnap_extension.tar` をダウンロードします。

   p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

   メモ: 認証トークンは 180 秒間のみ有効なので、まだ作成しないでください。

2. NetBackup Snapshot Manager がインストールされているホストと拡張機能をインストールするホストが同じでない場合、NetBackup Snapshot Manager コンテナのイメージ (`flexsnap-deploy`、`flexsnap-core`、`flexsnap-fluentd`、`flexsnap-datamover`) を拡張機能のホストにロードします。

   イメージ名は次のような形式です。

   例: `veritas/flexsnap-deploy`

3. Azure コンテナレジストリにイメージをプッシュできるようにするため、イメージタグを作成し、ソースイメージをターゲットイメージにマッピングします。詳しくは、「「Azure の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」」を参照してください。

   次のパラメータを事前に収集します。

パラメータ	説明
`container_registry_path`	コンテナレジストリパスを取得するには、Azure のコンテナレジストリに移動し、[概要 (Overview)] ペインで [ログインサーバー (Login server)] をコピーします。 例: `mycontainer.azurecr.io`
`tag`	NetBackup Snapshot Manager イメージのバージョン。 例: `11.1.x.x-xxxx`

   - イメージをタグ付けするには、ホストで実行されているコンテナプラットフォームに応じて、各イメージに対して次のコマンドを実行します。
     Docker の場合: `# docker tag source_image:tag target_image:tag`
     Podman の場合: `# podman tag source_image:tag target_image:tag`
     コマンドの詳細:
     - ソースイメージタグ: `veritas/flexsnap-deploy:tag>`
     - ターゲットイメージタグ: `<container_registry_path>/<source_image_name>:<SnapshotManager_version_tag>`

例:

```
# docker tag veritas/flexsnap-deploy:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-deploy:11.1.x.x-xxxx
# docker tag veritas/flexsnap-core:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-core:11.1.x.x-xxxx
# docker tag veritas/flexsnap-fluentd:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-fluentd:11.1.x.x-xxxx
# docker tag veritas/flexsnap-datamover:11.1.x.x-xxxx
mycontainer.azurecr.io/veritas/flexsnap-datamover:11.1.x.x-xxxx
```

4 次に、コンテナレジストリにイメージをプッシュするには、ホストで実行されているコンテナプラットフォームに応じて、各イメージに対して次のコマンドを実行します。

Docker の場合: `# docker push target_image:tag`

Podman の場合: `# podman push target_image:tag`

例:

```
# docker push mycontainer.azurecr.io/veritas/
flexsnap-deploy:11.1.x.x-xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-core:11.1.x.x-xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-fluentd:11.1.x.x-xxxx
# docker push mycontainer.azurecr.io/veritas/
flexsnap-datamover:11.1.x.x-xxxx
```

5 イメージをコンテナレジストリにプッシュしたら、`kubectl` のインストール先のホストから、以前にダウンロードした拡張機能スクリプト `cp_extension.sh` を実行します。このスクリプトは、必要なすべての入力パラメータを 1 つのコマンドで指定するか、入力を求めるプロンプトが表示される対話形式で実行できます。

スクリプトを実行する前に、次のパラメータを収集します。

パラメータ	説明
`snapshotmanager_ip`	メイン NetBackup Snapshot Manager ホストの IP アドレスまたは FQDN を指定します。
`target_image:tag`	手順 3 で作成した `flexsnap-deploy` イメージのターゲットイメージタグ。 例: `mycontainer.azurecr.io/veritas/flexsnap-deploy:11.1.x.x-xxxx`
`namespace`	以前に準備手順で作成した NetBackup Snapshot Manager の `namespace`。

パラメータ	説明

tag_key=tag_val	tag_key と tag_val は、次のコマンドを使用して取得できます。
	1 ノードの名前を取得します。
	`# kubectl get nodes | grep <node_name>`
	2 タグの key=value ラベルを取得します。
	`# kubectl describe node <node_name> -n <namespace> | grep -i labels`
	出力例: `agentpool=cpuserpool`

storage_class	以前に準備手順で作成した Kubernetes ストレージクラス。 例: `cloudpoint-sc`
Size in GB	拡張の要件に従ってプロビジョニングされるボリュームサイズ。
workflow_token	NetBackup Web UI の[拡張機能の追加 (Add extension)]ダイアログから作成された認証トークン。 p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

メモ: NetBackup Snapshot Manager の Kubernetes 拡張機能を配備する際は、ストレージクラスを作成し、それを NetBackup Snapshot Manager 拡張機能のインストールスクリプトへの入力として指定します。デフォルトではファイルのプロパティが開いているため、カスタム属性を指定してストレージクラスを作成し、拡張機能で作成されたファイルまたはフォルダの権限を `/cloudpoint` ディレクトリに保持することをお勧めします。詳しくは、Azure 製品マニュアルのストレージクラスの作成に関するセクションを参照してください。

実行可能ファイルとしてスクリプトを実行する:

- 実行可能ファイルとしての実行をスクリプトに対して許可します。
  `# chmod +x cp_extension.sh`
- 上記の表で説明されているすべての入力パラメータを指定し、インストールコマンドを実行します。
  `./cp_extension.sh install -c <snapshotmanager_ip> -i <target_image:tag> -n <namespace> -p <tag_key=tag_val> -s <storage_class> -t <workflow_token> -k <Size (In GiB)>`
  例:

```
./cp_extension.sh install
Snapshot Manager image repository path.
Format=<Login-server/image:tag>:
```

```
 cpautomation.azurecr.io/veritas/flexsnap-deploy:11.1.x.x-xxxx
Snapshot Manager extension namespace: snapshot-manager
Snapshot Manager IP or fully-qualified domain name:
<ip-address>
Node group/pool label with format key=value: agentpool=extpool
Storage class name: azurefile
Size in GiB (minimum 30 GiB, Please refer NetBackup Snapshot
Manager
Install and Upgrade Guide for PV size): 50
Snapshot Manager extension token:
This is a fresh NetBackup Snapshot Manager Extension
Installation

Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/
cloudpoint-servers.veritas.com unchanged
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-yj
 created
clusterrolebinding.rbac.authorization.k8s.io/
cloudpoint-rolebinding-cloudpoint-yj created
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done

Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:

0 of 1 updated replicas are available...
deployment "flexsnap-operator" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
Waiting for all components to come up ...Done
```

対話形式のファイルとしてスクリプトを実行する:

- 次のコマンドを実行します。

  ```
  # ./cp_extension.sh install
  ```

- スクリプトを実行する際に、上記の表で説明されている入力パラメータを指定します。

```
./cp_extension.sh install
Snapshot Manager image repository path.
Format=<Login-server/image:tag>:
cpautomation.azurecr.io/veritas/flexsnap-deploy:11.1.x.x-xxxx
Snapshot Manager extension namespace: snapshot-manager
Snapshot Manager IP or fully-qualified domain name:
<ip-address>
Node group/pool label with format key=value: agentpool=extpool
Storage class name: azurefile
Size in GiB (minimum 30 GiB, Please refer NetBackup Snapshot
Manager
Install and Upgrade Guide for PV size): 50
Snapshot Manager extension token:
This is a fresh NetBackup Snapshot Manager Extension
Installation

Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/
cloudpoint-servers.veritas.com unchanged
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/
cloudpoint-cloudpoint-yj created
clusterrolebinding.rbac.authorization.k8s.io/
cloudpoint-rolebinding-cloudpoint-yj created
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done

Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:

 0 of 1 updated replicas are available...
deployment "flexsnap-operator" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
Waiting for all components to come up ...Done
```

メモ: この出力例は画面に合わせて整形されています。

これで、Azure クラウド内の管理対象 Kubernetes クラスタで、NetBackup Snapshot Manager 拡張機能のインストールが完了しました。

拡張機能が正常にインストールされたことを確認するには

- コマンドプロンプトで成功したことを示すメッセージが表示されることを確認します。
- NetBackup Web UI で拡張機能が一覧表示されていることを確認します。
  [クラウド (Cloud)]、[NetBackup Snapshot Manager]タブの順に移動して[詳細設定 (Advanced Settings)]をクリックし、[NetBackup Snapshot Manager 拡張機能 (NetBackup Snapshot Manager extensions)]タブに移動して確認します。
- 次のコマンドを実行し、`flexsnap-deploy-xxx`、`flexsnap-fluentd-xxx`、`flexsnap-listener-xxx`、`flexsnap-fluentd-collector-xxx`、`flexsnap-datamover-xxxx` という 5 つのポッドの状態が実行中であることを確認します。

  ```
  # kubectl get pods -n <namespace>
  ```

  例: `# kubectl get pods -n cloudpoint-system`

AWS の管理対象 Kubernetes クラスタ (EKS) への NetBackup Snapshot Manager 拡張機能のインストール

NetBackup Snapshot Manager ホストの容量を拡大縮小して多数の要求を同時に処理するために、NetBackup Snapshot Manager のクラウドベース拡張機能を AWS の管理対象 Kubernetes クラスタに配備できます。

概要

- 適切なネットワークおよび構成が設定され、特定の役割を持つ AWS の管理対象 Kubernetes クラスタがすでに配備されている必要があります。クラスタは NetBackup Snapshot Manager と通信できる必要があります。
  必要な役割は、`AmazonEKSClusterPolicy AmazonEKSWorkerNodePolicy AmazonEC2ContainerRegistryPowerUser AmazonEKS_CNI_Policy AmazonEKSServicePolicy` です。
  サポートされる Kubernetes のバージョンについては、NetBackup Snapshot Manager のハードウェア互換性リスト (HCL) を参照してください。
- 既存の AWS Elastic Container Registry を使用するか、新しいレジストリを作成します。また、EKS に Elastic Container Registry からイメージを取得するためのアクセス権があることを確認します。
- AWS の管理対象 Kubernetes クラスタで、NetBackup Snapshot Manager 作業負荷の専用ノードプールを作成する必要があります。ノードグループは、AWS の自動

スケールグループ機能を使用して、必要に応じて自動的にノードのプロビジョニングとプロビジョニング解除を行うことで、ノードプールを動的に拡大縮小できます。

- NetBackup Snapshot Manager 拡張機能のイメージ (`flexsnap-deploy`、`flexsnap-core`、`flexsnap-fluentd`、`flexsnap-datamover`) を AWS コンテナレジストリにアップロードする必要があります。

AWS の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件

- NetBackup Snapshot Manager のインストール要件を満たすサポート対象の Ubuntu または RHEL システムで NetBackup Snapshot Manager イメージを選択し、ホストを作成します。
  p.34 の「NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備」を参照してください。
- メイン NetBackup Snapshot Manager ホストでポート 5671 が開いていることを確認します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。
- Docker または Podman コンテナプラットフォームをホストにインストールし、コンテナサービスを起動します。
  p.34 の 表 2-10 を参照してください。
- NetBackup Snapshot Manager ホスト、K8s 拡張機能、NetBackup Snapshot Manager ホストの IAM ロール、ノードグループが、すべて同じアカウントと構成に存在する必要があります。
- ジョブの実行中は、クラスタノードグループのスケール設定を変更しないことをお勧めします。ジョブが実行されていないときに拡張機能を無効にしてから、スケール設定を変更し、新しいジョブの拡張機能を有効にします。
- AWS 環境内で NetBackup Snapshot Manager ホストが Kubernetes クラスタにアクセスするための準備を行います。
  - AWS CLI をインストールします。詳しくは、AWS コマンドラインインターフェースを参照してください。
  - Kubernetes CLI をインストールします。詳しくは、kubectl のインストールに関するマニュアルを参照してください。
  - NetBackup Snapshot Manager イメージのプッシュ (アップロード) 先となる AWS コンテナレジストリを作成するか、利用可能な場合は既存のレジストリを使用します。必要に応じて最小ノード数と最大ノード数を設定します。
    詳しくは、AWS のマニュアルにある Amazon Elastic Container Registry に関する説明を参照してください。

- AWS EKS クラスタの OIDC プロバイダを作成します。詳しくは、『Amazon EKS ユーザーガイド』の「クラスターの IAM OIDC プロバイダーを作成する」セクションを参照してください。
- AWS EKS クラスタの IAM サービスアカウントを作成します。詳しくは、『Amazon EKS ユーザーガイド』を参照してください。
- IAM 役割が EKS クラスタへのアクセス権を必要とする場合は、EKS クラスタへのアクセス権がすでに設定されているシステムから次のコマンドを実行します。

  ```
  kubectl edit -n kube-system configmap/aws-auth
  ```

  詳しくは、『Amazon EKS ユーザーガイド』の「クラスターへの IAM ユーザーおよびロールのアクセスを有効にする」セクションを参照してください。
- Amazon EFS ドライバをインストールします。詳しくは、『Amazon EKS ユーザーガイド』の「Amazon EFS CSI ドライバー」セクションを参照してください。
- AWS 環境にログインし、AWS CLI で次のコマンドを実行して、Kubernetes クラスタにアクセスします。

  ```
  # aws eks --region <region_name> update-kubeconfig --name
  <cluster_name>
  ```

- ストレージクラスを作成します。詳しくは、『Amazon EKS ユーザーガイド』の「ストレージクラス」セクションを参照してください。
- ホストシステムのコマンドラインから NetBackup Snapshot Manager の名前空間を作成します。

  ```
  # kubectl create namespace cloudpoint-system
  ```

- 次に、AWS で新たに作成するか既存の管理対象 Kubernetes クラスタを使用して、NetBackup Snapshot Manager 専用の新しいノードプールを追加します。必要に応じて自動スケールを構成します。
- StorageClass を定義するときに、`uid/gid` を root に設定します。
  StorageClass の例を次に示します。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: efs-sc1
parameters:
  basePath: /dynamic_provisioning
  directoryPerms: "700"
  fileSystemId: fs-03e18dc283779991e
  gid: "0"
  provisioningMode: efs-ap
  uid: "0"
provisioner: efs.csi.aws.com
```

```
reclaimPolicy: Delete
volumeBindingMode: Immediate
```

AWS (EKS) への拡張機能のインストール

NetBackup Snapshot Manager 拡張機能をインストールする前に

- p.84 の「AWS の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」を参照してください。
- p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

拡張機能をインストールするには

1. 拡張機能ファイル `nbu_flexsnap_extension.tar` を事前にダウンロードしておく必要があります。

   p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

   メモ: 認証トークンは 180 秒間のみ有効なので、まだ作成しないでください。

2. NetBackup Snapshot Manager がインストールされているホストと拡張機能をインストールするホストが同じでない場合、NetBackup Snapshot Manager コンテナのイメージ (`flexsnap-deploy`、`flexsnap-core`、`flexsnap-fluentd`、`flexsnap-datamover`) を拡張機能のホストにロードします。

   イメージ名は次のような形式です。

   例: `veritas/flexsnap-deploy`

3. AWS コンテナレジストリにイメージをプッシュできるようにするため、イメージタグを作成し、ソースイメージをターゲットイメージにマッピングします。

   p.84 の「AWS の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」を参照してください。

   次のパラメータを事前に収集します。

パラメータ	説明
container_registry_path	コンテナレジストリパスを取得するには、Amazon ECR に移動し、各リポジトリの URI をコピーします。 例: <accoint_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-datamover

パラメータ	説明
tag	NetBackup Snapshot Manager イメージのバージョン。 例: `11.1.x.x-xxxx`

- イメージをタグ付けするには、ホストで実行されているコンテナプラットフォームに応じて、各イメージに対して次のコマンドを実行します。
  Docker の場合: `# docker tag source_image:tag target_image:tag`
  Podman の場合: `# podman tag source_image:tag target_image:tag`
  コマンドの詳細:
  - ソースイメージタグ: `veritas/flexsnap-deploy:tag>`
  - ターゲットイメージタグ:
    `<container_registry_path>/<source_image_name>:<SnapshotManager_version_tag>`
    例:

```
docker tag veritas/flexsnap-deploy:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:11.1.x.x-xxxx
docker tag veritas/flexsnap-core:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-core:11.1.x.x-xxxx
docker tag veritas/flexsnap-fluentd:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-fluentd:11.1.x.x-xxxx
docker tag veritas/flexsnap-datamover:11.1.x.x-xxxx
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-datamover:11.1.x.x-xxxx
```

4 次に、コンテナレジストリにイメージをプッシュするには、ホストで実行されているコンテナプラットフォームに応じて、各イメージに対して次のコマンドを実行します。

Docker の場合: `# docker push target_image:tag`

Podman の場合: `# podman push target_image:tag`

例:

```
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-datamover:11.1.x.x-xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-deploy:11.1.x.x-xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-fluentd:11.1.x.x-xxxx
docker push <account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/
flexsnap-core:11.1.x.x-xxxx
```

メモ: コマンドまたは出力の例は、画面に収まるよう整形されている場合や末尾が切れ捨てられている場合があります。

5 イメージがコンテナレジストリにプッシュされたら、次の 2 つのうちいずれかの方法を使用して拡張機能をインストールできます。

- Kustomization およびカスタムリソース YAML ファイル: 提供されたサンプルに基づいて、`kustomization.yaml` ファイルと `cloudpoint_crd.yaml` ファイルを作成して適用します。
  p.101 の「kustomize および CR YAML を使用した拡張機能のインストール」を参照してください。
- 拡張機能スクリプト: 以前にダウンロードした「tar」ファイルにパッケージ化されている拡張機能スクリプト `cp_extension.sh` を実行します。このスクリプトは、必要なすべての入力パラメータを 1 つのコマンドで指定するか、入力を求めるプロンプトが表示される対話形式で実行できます。
  p.89 の「拡張機能スクリプトを使用した拡張機能のインストール」を参照してください。

上記の手順に従った後、拡張機能が正常にインストールされたかどうかを確認できます。

拡張機能が正常にインストールされたことを確認するには

- コマンドプロンプトで成功したことを示すメッセージが表示されることを確認します。
- NetBackup Web UI で拡張機能が一覧表示されていることを確認します。
  [クラウド (Cloud)]、[NetBackup Snapshot Manager]タブの順に移動します。
  [詳細設定 (Advanced Settings)]をクリックし、[NetBackup Snapshot Manager 拡張機能 (NetBackup Snapshot Manager extensions)]タブに移動して確認します。

- 次のコマンドを実行し、flexsnap-deploy-xxx、flexsnap-fluentd-xxx、flexsnap-listener-xxx、flexsnap-fluentd-collector-xxx という 4 つのポッドの状態が実行中であることを確認します。

  ```
  # kubectl get pods -n <namespace>
  ```

  例: `# kubectl get pods -n cloudpoint-system`

拡張機能スクリプトを使用した拡張機能のインストール

拡張機能スクリプトを実行する前に、次のパラメータを取得します。

パラメータ	説明
snapshotmanager_ip	NetBackup Snapshot Manager のホスト名または IP アドレスを指定します。
target_image:tag	flexsnap-deploy イメージに対して作成したターゲットイメージタグ。 例: <account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:11.1.x.x-xxxx
namespace	以前に準備手順で作成した、NetBackup Snapshot Manager の配備先となる名前空間。
tag_key= tag_val	tag_key と tag_val は、拡張機能をインストールするノードに定義されているラベルキーと値のペアです。ラベルキーと値のペアは、コマンド kubectl describe node <node_name> -n <namespace> を使用して取得できます。 例: eks.amazonaws.com/nodegroup=Demo-NG
storage_class	以前に準備手順で作成した Kubernetes ストレージクラス。 例: cloudpoint-sc
サイズ (GB)	拡張の要件に従ってプロビジョニングされるボリュームサイズ。
workflow_token	NetBackup Web UI の[拡張機能の追加 (Add extension)]ダイアログから作成された認証トークン。 p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

実行可能ファイルとしてスクリプトを実行する:

- 実行可能ファイルとしての実行をスクリプトに対して許可します。

  ```
  # chmod +x cp_extension.sh
  ```

- 上記の表で説明されているすべての入力パラメータを指定し、インストールコマンドを実行します。

```
./cp_extension.sh install -c <snapshotmanager_ip> -i
<target_image:tag> -n <namespace> -p <tag_key=tag_val> -f
<storage_class> -t <workflow_token>
```

例:

```
Executing extension script as an executable file:

./cp_extension.sh install -c <snapshotmanager_ip> -i
<account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:11.1.x.x-xxxx

-n cloudpoint-system -p eks.amazonaws.com/nodegroup=td-nodepool-dnd
 -s efs-sc -k 50
 -t <workflow_token>

This is a fresh NetBackup Snapshot Manager Extension Installation

Getting Snapshot Manager service file ...done
Getting Snapshot Manager CRD file ...done
Starting Snapshot Manager service deployment
namespace/cloudpoint-system configured
deployment.apps/flexsnap-deploy created
serviceaccount/cloudpoint-acc created

clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-system
 unchanged
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-system

unchanged
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 created

Snapshot Manager service deployment ...done

customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 condition
met
Generating Snapshot Manager Custom Resource Definition object
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...done
```

対話形式のファイルとしてスクリプトを実行する:

- 次のコマンドを実行します。

```
# ./cp_extension.sh install
```

- スクリプトを実行する際に、上記の表で説明されている入力パラメータを指定します。

例:

```
Executing script in interactive way:

./cp_extension.sh install

Snapshot Manager image repository path.
Format=<Login-server/image:tag>:
<account-id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy:11.1.x.x-xxxx

Snapshot Manager extension namespace: cloudpoint-system
Snapshot Manager IP or fully-qualified domain name:
<snapshotmanager_ip>
Node pool with format key=value:
eks.amazonaws.com/nodegroup=td-nodepool-dnd
Storage class name: efs-sc
Size (In GiB): 60
Snapshot Manager extension token:

This is a fresh NetBackup Snapshot Manager Extension Installation
This is a fresh NetBackup Snapshot Manager Extension Installation

Getting Snapshot Manager service file ...done
Getting Snapshot Manager CRD file ...done

Starting Snapshot Manager service deployment
namespace/cloudpoint-system configured
deployment.apps/flexsnap-deploy created
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-system
unchanged
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-system

unchanged
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 created

Snapshot Manager service deployment ...done
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 condition met
```

```
Generating Snapshot Manager Custom Resource Definition object
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...done
```

メモ: 出力例は、画面に収まるよう整形されている場合や末尾が切れている場合があります。

GCP の管理対象 Kubernetes クラスタ (GKE) への NetBackup Snapshot Manager 拡張機能のインストール

Google Kubernetes Engine (GKE) クラスタを構成するために必要な権限は次のとおりです。

- Google アーティファクトレジストリにイメージをプッシュする場合、ユーザーにはリポジトリにイメージをアップロードするための書き込み権限が必要です。
  `artifactregistry.writer` 役割には、必要な権限がすべて含まれています。
  イメージのプッシュについて詳しくは、「プロジェクト内のアーティファクトレジストリに最初のイメージを push する」を参照してください。
- Kubernetes 拡張機能を構成するには、ユーザーに cluster-admin IAM ロールが割り当てられている必要があります。
  ロールベースのアクセス制御について詳しくは、「Role または ClusterRole を使用して権限を定義する」を参照してください。
- GCP プロバイダの構成に関連付けられているアカウントには、GKE ベースの Kubernetes 拡張機能の操作に対する次の権限が必要です。
  - クラスタアクセスのための権限:
    `container.clusters.get`
  - 自動スケール機能のための権限:
    `compute.instanceGroupManagers.get`
    `compute.instanceGroupManagers.update`
    `container.clusters.get`
    `container.clusters.update`
    `container.operations.get`

GCP の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件

NetBackup Snapshot Manager ホストの容量を拡大縮小して多数の要求を同時に処理するために、NetBackup Snapshot Manager のクラウドベース拡張機能を GCP の管理対象 Kubernetes クラスタに配備できます。

- 適切なネットワークおよび構成が設定された、GCP の管理対象 Kubernetes クラスタがすでに配備されている必要があります。クラスタは NetBackup Snapshot Manager および filestore と通信できる必要があります。

  メモ: NetBackup Snapshot Manager とすべてのクラスタノードプールは同じゾーンにある必要があります。

  詳しくは、「GKE の概要」を参照してください。

- 既存のアーティファクトレジストリを使用するか、新しいレジストリを作成します。また、管理対象 Kubernetes クラスタに、アーティファクトレジストリからイメージを取得するためのアクセス権があることを確認します。

- GKE クラスタで自動スケールが有効になっているかどうかにかかわらず、NetBackup Snapshot Manager 作業負荷専用のノードプールを作成する必要があります。自動スケール機能を使用すると、必要に応じて自動的にノードのプロビジョニングとプロビジョニング解除を行って、ノードプールを動的に拡大縮小できます。自動スケールが有効になっている場合、[サイズ制限タイプ (Size limit type)] に [合計制限 (Total limits)]を選択し、スケーリングに必要な最小および最大ノード制限を指定していることを確認します。

- NetBackup Snapshot Manager 拡張機能のイメージ (flexsnap-core、flexsnap-datamover、flexsnap-deploy、flexsnap-fluentd) をアーティファクトレジストリにアップロードする必要があります。

GCP でホストと管理対象 Kubernetes クラスタを準備する

- NetBackup Snapshot Manager のインストール要件を満たすサポート対象の Ubuntu または RHEL システムで NetBackup Snapshot Manager イメージを選択し、ホストを作成します。
  p.34 の「NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備」を参照してください。

- メイン NetBackup Snapshot Manager ホストでポート 5671 が開いていることを確認します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。

- Docker または Podman コンテナプラットフォームをホストにインストールし、コンテナサービスを起動します。

p.34 の「コンテナプラットフォーム (Docker、Podman) のインストール」を参照してください。

- GCP 環境内で NetBackup Snapshot Manager ホストが Kubernetes クラスタにアクセスするための準備を行います。
  - gcloud CLI をインストールします。詳しくは、gcloud CLI のインストールに関する説明を参照してください。
  - Kubernetes CLI をインストールします。
    詳しくは、次のマニュアルを参照してください。
    kubectl をインストールしてクラスタアクセスを構成する
    Linux での kubectl のインストールと設定
  - NetBackup Snapshot Manager イメージのアップロード (プッシュ) 先となる gcr アーティファクトレジストリを作成するか、利用可能な場合は既存のレジストリを使用します。
    アーティファクトレジストリの概要。
  - `gcloud init` を実行してアカウントを設定します。このアカウントに、Kubernetes クラスタを構成するために必要な権限があることを確認します。
    必要な権限について詳しくは、「GCP の管理対象 Kubernetes クラスタ (GKE) への NetBackup Snapshot Manager 拡張機能のインストール」を参照してください。`gcloud` コマンドについて詳しくは、次のマニュアルを参照してください。
    gcloud init
  - 次のコマンドを使用してクラスタを接続します。

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

    詳しくは、「kubectl をインストールしてクラスタアクセスを構成する」を参照してください。
  - ホストシステムのコマンドラインから NetBackup Snapshot Manager の名前空間を作成します。

    ```
    # kubectl create namespace <namespace-name>
    # kubectl config set-context --current
    --namespace=<namespace-name>
    ```

    メモ: ユーザーは任意の名前空間名を指定できます。`cloudpoint-system` のように指定する必要があります。

永続ボリュームの作成

- 既存の filestore を再利用します。

filestore をマウントし、NetBackup Snapshot Manager のみが使用するディレクトリ (dir_for_this_cp など) を作成します。

- 次のような内容のファイル (PV_file.yaml など) を作成します。

```
apiVersion: v1
kind: PersistentVolume
metadata:
  name: <name of the pv>
spec:
  capacity:
    storage: <size in GB>
  accessModes:
  - ReadWriteMany
  nfs:
    path: <path to the dir created above>
    server: <ip of the filestore>
```

次のコマンドを実行して、永続ボリュームを設定します。

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

kubernetes クラスタでのファイルストアの使用について詳しくは、「Google Kubernetes Engine クラスタからのファイル共有へのアクセス」を参照してください。

GCP (GKE) への拡張機能のインストール

GCP の管理対象 Kubernetes クラスタ (GKE) に NetBackup Snapshot Manager 拡張機能をインストールする前に次を実行してください。

- p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。
- p.93 の「GCP の管理対象 Kubernetes クラスタに拡張機能をインストールする際の前提条件」を参照してください。

拡張機能をインストールするには

1 拡張機能スクリプト nbu_flexsnap_extension.tar をダウンロードします。

p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

メモ: 認証トークンは 180 秒間のみ有効なので、まだ作成しないでください。

2 NetBackup Snapshot Manager がインストールされているホストと拡張機能をインストールするホストが同じでない場合、NetBackup Snapshot Manager コンテナのイメージ (flexsnap-deploy、flexsnap-core、flexsnap-fluentd、flexsnap-datamover) を拡張機能のホストにロードします。

イメージ名は次のような形式です。

例: veritas/flexsnap-deploy

3 GCP アーティファクトレジストリにイメージをプッシュできるようにするため、イメージをタグ付けして、ソースイメージをターゲットイメージにマッピングします。

次のパラメータを事前に収集します。

パラメータ	説明
artifact_registry_path	アーティファクトレジストリパスを取得するには、GCP でアーティファクトレジストリに移動し、リポジトリを選択して[概要 (Overview)]から[コピーパス (Copy path)]を選択します。 例: ~~<us-east1-docker.pkg.dev/<project-name>/<repository-name>/veritas/flexsnap-deploy:<image-tag>~~ ここで、us-east1-docker.pkg.dev はコンテナイメージのアーティファクトレジストリホスト名です。
tag	NetBackup Snapshot Manager イメージのバージョン。 例: 11.1.x.x-xxxx

- イメージをタグ付けするには、ホストで実行されているコンテナプラットフォームに応じて、各イメージに対して次のコマンドを実行します。
  Docker の場合: # docker tag source_image:tag target_image:tag
  Podman の場合: # podman tag source_image:tag target_image:tag
  コマンドの詳細:
  - ソースイメージタグ: veritas/flexsnap-deploy:tag>
  - ターゲットイメージタグ:
    <artifact_registry_path>/<source_image_name>:<SnapshotManager_version_tag>

例:

```
# docker tag  veritas/flexsnap-deploy:11.1.x.x-xxx  <artifact
 registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx
# docker tag  veritas/flexsnap-core:11.1.x.x-xxx  <artifact
 registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-core:11.1.x.x-xxxx
# docker tag  veritas/flexsnap-fluentd:11.1.x.x-xxx
<artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-fluentd:11.1.x.x-xxxx
# docker tag  veritas/flexsnap-datamover:11.1.x.x-xxx
<artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-datamover:11.1.x.x-xxxx
```

4 アーティファクトレジストリにイメージをプッシュするには、ホストで実行されているコンテナプラットフォームに応じて、各イメージに対して次のコマンドを実行します。

Docker の場合: `# docker push target_image:tag`

Podman の場合: `# podman push target_image:tag`

例:

```
# docker push  <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx
# docker push  <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-core:11.1.x.x-xxxx
# docker push <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-fluentd:11.1.x.x-xxxx
# docker push <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-datamover:11.1.x.x-xxxx
```

5 最後に、以前にダウンロードしたスクリプト `cp_extension.sh` を実行します。

p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

このスクリプトは、必要なすべての入力パラメータを 1 つのコマンドで指定するか、入力を求めるプロンプトが表示される対話形式で実行できます。

スクリプトを実行する前に、次のパラメータを収集します。

パラメータ	説明
cloudpoint_ip	メイン NetBackup Snapshot Manager ホストの IP アドレスまたは FQDN を指定します。

パラメータ	説明
target_image:tag	手順 3 で作成した `flexsnap-deploy` イメージのターゲットイメージタグ。 例: `<artifact registry hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx`
namespace	以前に準備手順で作成した NetBackup Snapshot Manager の `namespace`。
tag_key= tag_val	`tag_key` と `tag_val` は、次のコマンドを使用して取得できます。 `# gcloud container node-pools list --cluster=<cluster-name> --zone=<zone-name>`
persistent_volume	以前に準備手順で作成した Kubernetes の永続ボリューム。
サイズ (GiB)	拡張の要件に従ってプロビジョニングされるボリュームサイズ。
workflow_token	NetBackup Web UI の[拡張機能の追加 (Add extension)]ダイアログから作成された認証トークン。 p.69 の「NetBackup Snapshot Manager 拡張機能のダウンロード」を参照してください。

メモ: NetBackup Snapshot Manager の Kubernetes 拡張機能を配備する際は、永続ボリュームを作成し、それを NetBackup Snapshot Manager 拡張機能のインストールスクリプトへの入力として指定します。

実行可能ファイルとしてスクリプトを実行する:

- 実行可能ファイルとしての実行をスクリプトに対して許可します。
  ```
  # chmod +x cp_extension.sh
  ```
- 上記の表で説明されているすべての入力パラメータを指定し、インストールコマンドを実行します。
  ```
  ./cp_extension.sh install -c <snapshotmanager-ip> -i
  <target-image:tag> -n <namespace> -p
  cloud.google.com/gke-nodepool=<nodepool-name> -v
  <persistent-volume-name> -k <size-in-GiB> -t <token>
  ```
  例:

  ```
  # ./cp_extension.sh install
  Snapshot Manager image repository path.
  Format=<Login-server/image:tag>:
  <artifact registry
  ```

```
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx
Snapshot Manager extension namespace: test-ns
Snapshot Manager IP or fully-qualified domain name: <ip
Address>
Node group/pool label with format key=value:
cloud.google.com/gke-nodepool=
test-pool-dnd
Persistent volume name: test-fileserver-pv
Size in GiB (minimum 30 GiB,
Please refer NetBackup Snapshot Manager Install and Upgrade
Guide for PV size): 30
Snapshot Manager extension token:
This is a fresh NetBackup Snapshot Manager Extension
Installation



Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 unchanged
serviceaccount/cloudpoint-acc unchanged
clusterrole.rbac.authorization.k8s.io/cloudpoint-shashwat-ns
configured
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-shashwat-ns

unchanged
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done



customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 condition met
Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:
 0 of 1 updated
replicas are available...
deployment "flexsnap-operator" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
[root@xxxx]# kubectl get pods
```

```
NAME                                              READY   STATUS
   RESTARTS   AGE
flexsnap-fluentd-collector-79f4dd8447-5lgrf   1/1     Running
   0          34s
flexsnap-fluentd-xl7px                        1/1     Running
   0          33s
flexsnap-listener-598f48d59b-crfjq            1/1     Running
   0          33s
flexsnap-operator-574dccc58f-fnkdf            1/1     Running
   0          104s
```

対話形式のファイルとしてスクリプトを実行する:

- 次のコマンドを実行します。

  ```
  # ./cp_extension.sh install
  ```

- スクリプトを実行する際に、上記の表で説明されている入力パラメータを指定します。

```
./cp_extension.sh install
Snapshot Manager image repository path.
Format=<Login-server/image:tag>: <artifact registry
hostname>/<project-name>/<repository-name>/veritas/flexsnap-deploy:11.1.x.x-xxxx
Snapshot Manager extension namespace: snapshot-manager
Snapshot Manager IP or fully-qualified domain name: xx.xxx.xx.xx
Node group/pool label with format key=value: agentpool=extpool
Persistent volume name:
Size in GiB (minimum 30 GiB,
Please refer NetBackup Snapshot Manager Install and Upgrade Guide
 for PV size): 50
Snapshot Manager extension token:
This is a fresh NetBackup Snapshot Manager Extension Installation

Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 unchanged
serviceaccount/cloudpoint-acc created
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-yj
created
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-yj
 created
deployment.apps/flexsnap-operator created
Snapshot Manager service deployment ...done
```

```
Generating Snapshot Manager Custom Resource Definition object
Waiting for deployment "flexsnap-operator" rollout to finish:0
of 1 updated replicas are available..
deployment "flexsnap-operator" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule created
Snapshot Manager extension installation ...
Operator operations passed
Waiting for all components to come up ...Done
Waiting for all components to come up ...Done
```

メモ: この出力例は画面に合わせて整形されています。

これで、GCP 内の管理対象 Kubernetes クラスタで、NetBackup Snapshot Manager 拡張機能のインストールが完了しました。

拡張機能が正常にインストールされたことを確認するには

- コマンドプロンプトで成功したことを示すメッセージが表示されることを確認します。
- NetBackup Web UI で拡張機能が一覧表示されていることを確認します。[クラウド (Cloud)]、[NetBackup Snapshot Manager]タブの順に移動して[詳細設定 (Advanced Settings)]をクリックし、[NetBackup Snapshot Manager 拡張機能 (NetBackup Snapshot Manager extensions)]タブに移動して確認します。
- 次のコマンドを実行し、`flexsnap-operator-xxx`、`flexsnap-fluentd-xxx`、`flexsnap-listener-xxx`、`flexsnap-deploy-xxx` および `flexsnap-fluentd-collector-xxx` という 5 つのポッドの状態が実行中であることを確認します。

  `# kubectl get pods -n <namespace>`

  例: `# kubectl get pods -n cloudpoint-system`

  `flexsnap-datamover-xxxx` ポッドは配備後にデフォルトでは実行されず、バックアップ操作がトリガされた場合にのみ作成されます。

kustomize および CR YAML を使用した拡張機能のインストール

拡張機能フォルダには次のサンプルファイルが含まれています。これらのサンプルファイルに基づき、環境に応じて関連する値を使用して新しい YAML を作成する必要があります。

- kustomization.yaml
- cloudpoint_crd.yaml

- node_select.yaml
- cloudpoint_service.yaml

kustomization.yaml

kustomization.yaml では、次の表に示すように images セクションのパラメータを関連する値で更新します。

パラメータ	説明
newName	NetBackup Snapshot Manager イメージ名をコンテナレジストリパスとともに指定します。 例: <account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy
newTag	配備する NetBackup Snapshot Manager イメージのタグを指定します。 例: 11.1.x.x-xxxx
namespace	以前に準備手順で作成した、NetBackup Snapshot Manager の配備先となる名前空間。

例:

```
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
resources:
- cloudpoint_service.yaml
patchesStrategicMerge:
- node_select.yaml
namespace: demo-cloudpoint-ns
images:
- name: CLOUDPOINT_IMAGE
  newName:
<account_id>.dkr.ecr.us-east-2.amazonaws.com/veritas/flexsnap-deploy

  newTag: 11.1.x.x-xxxx
vars:
- name: ServiceAccount.cloudpoint-acc.metadata.namespace
  objref:
    kind: ServiceAccount
    name: cloudpoint-acc
    apiVersion: v1
  fieldref:
    fieldpath: metadata.namespace
```

```
configurations:
- cloudpoint_kustomize.yaml
```

cloudpoint_service.yaml

GCP プラットフォームで拡張機能を配備する場合は、`cloudpoint_service.yaml` で storageClassName を volumeName に置き換えます。

cloudpoint_crd.yaml

`cloudpoint_crd.yaml` マニフェストファイルを次のように編集します。

- GCP プラットフォームの場合: storageClassName ワードを含む行を削除します。
- GCP プラットフォーム以外の場合: volumeName ワードを含む行を削除します。

次の表に示すように Spec セクションのパラメータを関連する値で更新します。

パラメータ	説明
cloudpointHost	NetBackup Snapshot Manager のホスト名または IP アドレスを指定します。
cloudpointExtensionToken	NetBackup Web UI の[拡張機能の追加 (Add extension)]ダイアログから以前にダウンロードした NetBackup Snapshot Manager トークンの内容を貼り付けます。
storageClassName	以前に準備手順で作成した Kubernetes ストレージクラス。 例: `efs-sc-new-root` **メモ:** GCP プラットフォームには必要ありません。
size	拡張の要件に従ってプロビジョニングされるボリュームサイズ (GB)。
namespace	以前に準備手順で作成した、NetBackup Snapshot Manager の配備先となる名前空間。
volumeName	以前に準備手順で作成した永続ボリュームの名前。 **メモ:** GCP プラットフォームには必要です。

例:

```
apiVersion: veritas.com/v1
kind: CloudpointRule
metadata:
  name: cloudpoint-config-rule
  namespace: demo-cloudpoint-ns
```

```
spec:
  CLOUDPOINT_HOST: 3.17.**.*** .
  CLOUDPOINT_EXTENSION_TOKEN: <extension_token>
  RENEW: false
  LOG_STORAGE:
    STORAGE_CLASS_NAME: efs-sc-new
    SIZE: 100
```

node_select.yaml

Spec セクションの nodeSelector に移動し、node_select.yaml ファイルの NODE_AFFINITY_KEY と NODE_AFFINITY_VALUE の値を置換します。ユーザーは、次のコマンドを使用してこれらの詳細を取得できます。

- 次のコマンドを使用して、拡張機能の専用ノードプールから任意のノードの名前を取得します。

  `# kubectl get nodes`

- 特定のクラウドプロバイダに応じ、tag key=value ラベルに基づいて次の各コマンドを使用します。
  - Azure の場合: `# kubectl describe node <node_name> | grep -i labels`
    出力例: `agentpool=azure-node-pool`
  - AWS の場合: `# kubectl describe node <node_name> | grep -i <node_group_name>`
    出力例: `eks.amazonaws.com/nodegroup=aws-node-pool`
  - GCP の場合: `# kubectl describe node <node_name> | grep -i <node_pool_name>`
    出力例: `cloud.google.com/gke-nodepool=gcp-node-pool`

パラメータ	説明
NODE_AFFINITY_KEY	■ AWS の場合: eks.amazonaws.com/nodegroup ■ Azure の場合: agentpool ■ GCP の場合: cloud.google.com/gke-nodepool
NODE_AFFINITY_VALUE	ノードプールの名前。 ■ AWS の場合: aws-node-pool ■ Azure の場合: azure-nood-pool ■ GCP の場合: gcp-node-pool

次に、YAML ファイルがあるフォルダから次のコマンドを実行します。

- Kustomization YAML を適用する場合: `kubectl apply -k <location of the kustomization.yaml file>`
- NetBackup Snapshot Manager CR を適用する場合: `kubectl apply -f cloudpoint_crd.yaml`

拡張機能の管理

VM ベースまたは管理対象 Kubernetes クラスタベースの拡張機能をインストールした後、拡張機能の無効化または有効化、停止、起動、再起動、またはそれらの証明書の更新が必要になる場合があります。

次の表で、これらのオプションを使用して拡張機能を管理する方法の説明を参照してください。

メモ: ベリタスでは、Snapshot Manager のインストールに flexsnap_configure CLI を使用することをお勧めします。Docker/Podman CLI を使用した Snapshot Manager のインストールは、RHEL 8 および 9 以外では非推奨となり、RHEL 8 および 9 では削除されています。

表 4-1 拡張機能のインストール後のオプション

オプション	手順
拡張機能の無効化または有効化: ■ VM ベースの拡張機能 ■ 管理対象 Kubernetes クラスタベースの拡張機能	NetBackup Web UI から拡張機能を無効または有効にできます。 [クラウド (Cloud)]、[NetBackup Snapshot Manager]タブの順に移動して[詳細設定 (Advanced Settings)]をクリックし、[NetBackup Snapshot Manager 拡張機能 (NetBackup Snapshot Manager extensions)]タブに移動して、必要に応じて拡張機能を無効または有効にし、[保存 (Save)]をクリックします。 無効になっている拡張機能でジョブはスケジュールされません。 **メモ:** NetBackup Snapshot Manager がアップグレードされると、すべての拡張機能が自動的に無効になります。
flexsnap_configure CLI を使用して VM ベースの拡張機能 (Docker/Podman) の証明書を停止、開始、再起動、または更新します	■ 拡張機能を停止するには: `# flexsnap_configure stop` ■ 拡張機能を起動するには: `# flexsnap_configure start` ■ 拡張機能を再起動するには: `# flexsnap_configure restart` ■ VM ベースの拡張機能の証明書を更新するには (対話型): `# flexsnap_configure renew --extension -i` ■ VM ベースの拡張機能の証明書を更新するには (非対話型): `# flexsnap_configure renew --extension --primary <nbsm_fqdn>`

オプション	手順

管理対象 Kubernetes クラスタベースの拡張機能の証明書の更新	**1** NetBackup Web UI から拡張機能のインストールスクリプト `cp_extension.sh` をダウンロードします。
	2 `kubectl` がインストールされているホストからスクリプトを実行します。次のコマンドを実行します。
	`# chmod +x cp_extension.sh`
	`# ./cp_extension.sh renew`
	3 次に、証明書の更新を開始するために、NetBackup Snapshot Manager IP/FQDN、拡張機能のトークン (NetBackup Web UI から生成可能)、拡張機能の名前空間を指定します。
	p.77 の「Azure (AKS) への拡張機能のインストール」を参照してください。

5

NetBackup Snapshot Manager for Cloud プロバイダ

この章では以下の項目について説明しています。

NetBackup Snapshot Manager クラウドプロバイダを構成する理由

クラウドの資産を保護する場合は、NetBackup Snapshot Manager クラウドプロバイダを適切なクラウド用に構成する必要があります。

クラウドプロバイダが構成されると、Snapshot Manager は、NetBackup Web UI を介して管理および保護されているクラウドの資産を検出できます。

クラウドプロバイダの構成方法については、『NetBackup Web UI クラウド管理者ガイド』を参照してください。

デフォルトでは、検出された資産で作成されたスナップショットでは、クラッシュ整合のみが実現されます。VM でファイルシステムとアプリケーションの整合性スナップショットまたは単一ファイルのリストアを実行するには、ユーザーは自分の VM 用にエージェントを構成する必要があります。エージェントの構成について詳しくは、次のセクションを参照してください。

p.217 の「NetBackup Snapshot Manager エージェントのインストールおよび構成」を参照してください。

AWS プラグインの構成に関する注意事項

AWS (アマゾンウェブサービス) プラグインを使用すると、Amazon クラウド内の次の資産のスナップショットを作成、リストア、および削除できます。

- EC2 (Elastic Compute Cloud) インスタンス
- EBS (Elastic Block Store) ボリューム
- Amazon RDS (Relational Database Service) インスタンス
- Aurora クラスタ
- Redshift クラスタ
- AWS DocumentDB
- AWS Neptune
- RDS Custom for SQL
- RDS Custom for Oracle

メモ: AWS プラグインを構成する前に、保護するリージョンが有効になっていることと、NetBackup Snapshot Manager で AWS 資産を操作できるようにするために適切なアクセス権が設定されていることを確認します。

NetBackup Snapshot Manager は、次の AWS リージョンをサポートします。

表 5-1 NetBackup Snapshot Manager でサポートされる AWS リージョン

AWS 商業リージョン	AWS GovCloud (米国) リージョン
■ us-east-1, us-east-2, us-west-1, us-west-2 ■ ap-east-1, ap-east-2, ap-south-1, ap-south-2, ap-northeast-1, ap-northeast-2, ap-northeast-3, ap-southeast-1, ap-southeast-2, ap-southeast-3, ap-southeast-4, ap-southeast-5, ap-southeast-6, ap-southeast-7 ■ eu-central-1, eu-central-2, eu-west-1, eu-west-2, eu-west-3, eu-north-1, eu-south-1, eu-south-2 ■ cn-north-1, cn-northwest-1 ■ ca-central-1 ■ me-south-1, me-central-1 ■ mx-central-1 ■ sa-east-1 ■ cn-north-1, cn-northwest-1 ■ af-south-1 ■ il-central-1 ■ FIPS サポート対象リージョン: us-east-1, us-east-2, us-west-1, us-west-2	■ us-gov-east-1 ■ us-gov-west-1

AWS 用の NetBackup Snapshot Manager プラグインを構成するには、次の情報が必要です。

NetBackup Snapshot Manager が AWS クラウドに配備されている場合:

表 5-2 AWS プラグインの構成パラメータ: クラウド配備

NetBackup Snapshot Manager の構成パラメータ	説明
ソースアカウントの構成	
Regions	AWS ソースアカウントに関連付けられた、クラウド資産を検出する 1 つ以上の AWS リージョン。 **メモ:** CFT (CloudFormation テンプレート) を使用して NetBackup Snapshot Manager を配備する場合、ソースアカウントはテンプレートベースの配備ワークフローの一部として自動的に構成されます。

NetBackup Snapshot Manager の構成パラメータ	説明
VPC Endpoint	ゾーンが指定されていない、AWS STS (セキュリティトークンサービス) エンドポイントサービスの最初の DNS 名。
クロスアカウントの構成	
Account ID	ソースアカウントに設定されている NetBackup Snapshot Manager インスタンスを使用して保護する資産を持つ、その他の AWS アカウント (クロスアカウント) のアカウント ID。
Role Name	他の AWS アカウント (クロスアカウント) に関連付けられている IAM ロール。
Regions	AWS クロスアカウントに関連付けられた、クラウド資産を検出する 1 つ以上の AWS リージョン。
VPC Endpoint	ゾーンが指定されていない、AWS STS (セキュリティトークンサービス) エンドポイントサービスの最初の DNS 名。 例: `vpce-044994fccdfd11b6f-k5hd5cx1.sts.us-east-2.vpce.amazonaws.com`

メモ: VPC エンドポイントを使用して AWS クラウドに配備されている既存の NetBackup Snapshot Manager の場合は、VPC エンドポイントエントリを追加して構成済みのプラグインを編集します。

p.126 の「VPC エンドポイントを使用した AWS プラグイン構成の前提条件」を参照してください。

NetBackup Snapshot Manager が AWS に接続すると、次のエンドポイントが使用されます。この情報を使用して、ファイアウォールで許可リストを作成できます。

メモ: アマゾンウェブサービスでは、グローバルエンドポイントではなく地域エンドポイントを使用することを推奨しています。

- ec2.*.amazonaws.com
- sts.*.amazonaws.com
- rds.*.amazonaws.com
- kms. *.amazonaws.com

- ebs.*.amazonaws.com
- iam.*.amazonaws.com
- eks.*.amazonaws.com
- autoscaling.*.amazonaws.com
- (DBPaaS 保護用) dynamodb.*.amazonaws.com, redshift.*.amazonaws.com
- (プロバイダ管理の一貫性用) ssm.*.amazonaws.com

さらに、次のリソースおよび処理を指定する必要があります。

- ec2.SecurityGroup.*
- ec2.Subnet.*
- ec2.Vpc.*
- ec2.createInstance
- ec2.runInstances

複数のネットワークインターフェース (NIC) のリストアのサポート

NetBackup Snapshot Manager には、AWS で元のネットワーク構成 (ソース VM のすべての NIC と IP アドレス) をリストアするオプションがあります。

- プライベート IP は、接続可能であれば、ソース VM 上にあったようにリストアされます。
- パブリック IP の場合、AssociatePublicIpAddress プロパティはソース VM に存在していたとおりにリストアされます。この属性に基づいて、パブリック IP が VM に割り当てられます。

複数のアカウント、サブスクリプション、またはプロジェクトの構成

- 同じプラグインに対して複数の構成を作成する場合は、それらが異なるリージョンの資産を管理していることを確認します。2 つ以上のプラグイン構成で、クラウド資産の同じセットを同時に管理しないようにする必要があります。
- 複数のアカウントが 1 台の NetBackup Snapshot Manager ですべて管理されている場合、単一の NetBackup Snapshot Manager インスタンスで管理する資産の数が多くなりすぎるため、分散したほうがよい場合があります。
- アプリケーションの整合性スナップショットが正常に機能するために、次のようにします。
  - プロバイダが管理する整合性の前提条件を満たしていることを確認します。詳しくは、AWS のマニュアルを参照してください。
  - 上記の前提条件を満たさない場合は、リモート VM インスタンスと NetBackup Snapshot Manager 間のエージェントまたはエージェントレスネットワーク接続が

必要です。これには、アカウント、サブスクリプション、およびプロジェクト間のネットワークを設定する必要があります。

AWS プラグインの考慮事項および制限事項

プラグインを構成する前に、次の点を考慮します。

- NetBackup Snapshot Manager では、NVMe (非揮発性メモリエクスプレス) デバイスとして公開されている EBS ボリュームを使用する AWS Nitro ベースのインスタンスはサポートされません。
  NetBackup Snapshot Manager が NVMe EBS ボリュームを使用する AWS Nitro ベースの Windows インスタンスを検出して保護できるようにするには、AWS NVMe ツールの実行可能ファイル `ebsnvme-id` が、AWS Windows インスタンスの次の場所のいずれかに存在することを確認します。
  - `%PROGRAMDATA%¥Amazon¥Tools`
    これは、ほとんどの AWS インスタンスのデフォルトの場所です。
  - `%PROGRAMFILES%¥Veritas¥Cloudpoint`
    この場所に実行可能ファイルを手動でダウンロードしてコピーします。
  - システムの PATH 環境変数
    システムの PATH 環境変数で、実行可能ファイルのパスを追加または更新します。
    NVMe ツールが、記載されている場所のいずれかに存在しない場合、NetBackup Snapshot Manager はそのようなインスタンスのファイルシステムの検出に失敗することがあります。
    ログに次のエラーが示されることがあります。

    ```
    "ebsnvme-id.exe" not found in expected paths!"
    ```

- カスタム/コミュニティ AMI から作成された Windows インスタンスの検出と保護を NetBackup Snapshot Manager で許可するには
  - カスタム AMI またはコミュニティ AMI に AWS NVMe ドライバがインストールされている必要があります。このリンクを参照してください。
  - `ebsnvme-id.exe` を `%PROGRAMDATA%¥Amazon¥Tools` または `%PROGRAMFILES%¥Veritas¥Cloudpoint` にインストールします。
  - わかりやすいデバイス名には部分文字列「NVMe」が含まれている必要があります。含まれていない場合はバックアップが作成されたすべての NVMe デバイスについて Windows レジストリで更新します。
    レジストリパス:
    `Computer¥HKEY_LOCAL_MACHINE¥SYSTEM¥ControlSet001¥列挙¥SCSI¥ディスク&Ven_NVMe&Prod_Amazon_Elastic_B¥`
    プロパティ名: `FriendlyName`

値: `NVMe Amazon Elastic B SCSI Disk Drive`

- 検出中に権限が見つからない例外: デフォルトでは、新しい AWS プロバイダプラグイン構成を追加するときに、AWS クラウド関連の操作に対して権限チェックは行われません。AWS プロバイダプラグインの構成中に権限チェックを有効にするには、`flexsnap.conf` ファイルの AWS セクションに skip_permissions_check = "no" パラメータを追加します。
- NetBackup Snapshot Manager が Redshift 資産を検出して保護できるようにするには、AWS ポータルで Redshift クラスタとデータベースが利用可能な状態である必要があります。Redshift クラスタが利用可能な状態の場合、資産は NetBackup UI で［アクティブ (Active)］とマークされます。それ以外の場合、資産は［非アクティブ (Inactive)］とマークされます。
- RDS インスタンス、Redshift クラスタ、Aurora クラスタの自動スナップショットは、NetBackup Snapshot Manager からは削除できません。
- AWS RDS アプリケーション間でのアプリケーションの一貫性は、AWS の動作によって異なります。(AWS は DB インスタンスのバックアップ中に I/O を一時停止します)。これは AWS からの制限事項であり、現在 NetBackup Snapshot Manager の範囲外にあります。
- すべての自動スナップショットの名前は、`rds:` というパターンで始まります。Redshift クラスタの場合は、`rs:` で始まります。
- NVMe EBS ボリュームを使用する AWS Nitro ベースの Windows インスタンスを検出して保護するようにプラグインを構成している場合は、AWS NVMe ツールの実行可能ファイル `ebsnvme-id.exe` が、AWS インスタンスの次の場所のいずれかに存在することを確認する必要があります。
  - `%PROGRAMDATA%¥Amazon¥Tools`
    これは、ほとんどの AWS インスタンスのデフォルトの場所です。
  - `%PROGRAMFILES%¥Veritas¥Cloudpoint`
    この場所に実行可能ファイルを手動でダウンロードしてコピーします。
  - システムの PATH 環境変数
    システムの PATH 環境変数で、実行可能ファイルのパスを追加または更新します。

  NVMe ツールが、記載されている場所のいずれかに存在しない場合、NetBackup Snapshot Manager はそのようなインスタンスのファイルシステムの検出に失敗することがあります。ログに次のエラーが示されることがあります。

  `"ebsnvme-id.exe" not found in expected paths!"`

  これは、AWS Nitro ベースの Windows インスタンスの場合にのみ必要です。また、コミュニティ AMI またはカスタム AMI を使用してこのインスタンスを起動する際は、ツールを手動でインストールする必要がある場合があります。

- NetBackup Snapshot Manager では、デフォルトの RDS 暗号化キー (AWS/RDS) を使用してスナップショットが暗号化されている場合、AWS RDS インスタンス、RDS クラスタ、または Redshift クラスタのアカウント間レプリケーションはサポートされません。AWS アカウント間では、このような暗号化されたスナップショットを共有できません。
  AWS アカウント間でそのようなスナップショットをレプリケートしようとすると、次のエラーで操作が失敗します。

  ```
  Replication failed The source snapshot KMS key [<key>] does not
  exist,
  is not enabled or you do not have permissions to access it.
  ```

  これは AWS からの制限事項であり、現在 NetBackup Snapshot Manager の範囲外にあります。
- AWS プラグイン構成からリージョンを削除すると、そのリージョンから検出されたすべての資産も、NetBackup Snapshot Manager 資産データベースから削除されます。削除された資産に関連付けられているアクティブなスナップショットがある場合、それらのスナップショットに対して操作を実行できないことがあります。
  このリージョンをプラグイン構成に再び追加すると、NetBackup Snapshot Manager ですべての資産が再度検出され、関連付けられているスナップショットの操作を再開できます。ただし、関連付けられたスナップショットに対してはリストア操作を実行できません。
- NetBackup Snapshot Manager は、商業リージョンおよび GovCloud (米国) リージョンをサポートします。AWS プラグインの構成中に、AWS の商業リージョンと GovCloud (US) リージョンの組み合わせを選択できる場合でも、最終的に構成は失敗します。
- NetBackup Snapshot Manager では、AWS RDS インスタンスの IPv6 アドレスはサポートされていません。これは、Amazon RDS 自体の制限事項であり、NetBackup Snapshot Manager には関連していません。
  詳しくは、AWS のマニュアルを参照してください。
- NetBackup Snapshot Manager は、ストレージプールから作成された仮想ディスクまたはストレージ領域を備えた Windows システムのアプリケーションの一貫したスナップショットと個別ファイルのリストアをサポートしません。Microsoft SQL Server のスナップショットジョブでストレージプールのディスクを使用すると、エラーが発生してジョブが失敗します。ただし、接続状態にある仮想マシンのスナップショットジョブがトリガされると、ジョブは正常に実行されることがあります。この場合、ファイルシステムの静止およびインデックス付けはスキップされます。このような個々のディスクを元の場所にリストアするジョブも失敗します。この状況では、ホストがリカバリ不可能な状態になる可能性があり、手動でのリカバリが必要になる場合があります。
- リストアを実行するアカウントが所有していないセキュリティグループでは、AWS 仮想マシンをリストアできません。これは、仮想マシンを作成するアカウントが所有していな

い共有 VPC のセキュリティグループで EC2 インスタンスの作成を制限する、AWS の制限事項があるためです。
詳しくは、『Amazon VPC ユーザーガイド』の VPC の共有に関するセクションを参照してください。

- AWS Systems Service Manager を使用したファイルシステム/アプリケーションの整合性スナップショットの場合:
  - 作成した SSM ドキュメントは、プラグインまたは NetBackup Snapshot Manager の削除時に手動で削除する必要があります。
  - `ext2` ファイルシステムがある VM 作業負荷のスナップショットは、カーネルまたはオペレーティングシステムのバージョンに応じた一貫性があります。
  - AWS CLI、AWS VSS コンポーネントモジュールが VM 作業負荷にインストールされていない場合、インストールにはインターネットが必要です。
  - プレスクリプトとポストスクリプトが提供されていない場合、Linux アプリケーションの整合性スナップショットでは、VM はアプリケーションプラグインが構成されて接続状態である必要があります。
- ソースアカウントの構成を使用して複数のクロスアカウントを保護する場合:
  - 構成を追加して資産の保護を開始したら、すべてのスナップショットが期限切れになって初めて、クロスアカウントをインラインポリシーから削除できるようになります。
  - 複数のアカウントをすべて同じプロバイダの構成で維持した場合、NetBackup Snapshot Manager の単一のプロバイダの構成で処理する資産の数が過剰になることがあります。そのため、多くの資産が含まれるアカウントに関しては、ソースアカウント設定で暗黙的に配置するのではなく、個別のクロスアカウントの構成を作成することをお勧めします。
  - 配備の種類に関係なく、複数のクロスアカウントを保護するように構成できるのは、そのような単一のソースアカウントの構成のみです。
  - 既存のクロスアカウントの構成は、保護するために単一のソースプロバイダの構成に移行することはできません。

AWS プラグイン構成の前提条件

NetBackup Snapshot Manager インスタンスが AWS クラウドに配備されている場合は、プラグインを構成する前に次の操作を実行します。

- AWS IAM ロールを作成し、NetBackup Snapshot Manager で必要なアクセス権を割り当てます。
  p.153 の「NetBackup Snapshot Manager の AWS アクセス権の構成」を参照してください。

IAM ロールの作成方法について詳しくは、AWS Identity および Access Management のドキュメントを参照してください。

- NetBackup Snapshot Manager インスタンスに IAM ロールを関連付けます。IAM ロールを関連付ける方法について詳しくは、AWS Identity および Access Management のドキュメントを参照してください。

メモ: CFT (CloudFormation テンプレート) を使用して NetBackup Snapshot Manager を配備した場合は、NetBackup Snapshot Manager スタックの起動時に IAM ロールが自動的にインスタンスに割り当てられます。

- DynamoDB の場合、`netbackup_<accountId>` という名前の S3 バケットを作成する必要があります。このバケットはステージング場所として使用され、その中に、各バックアップ操作に必要なディレクトリ階層が作成されます。
- クロスアカウントの構成については、AWS IAM コンソール ([IAM コンソール (IAM Console)]、[ロール (Roles)]の順に選択) から、次のように IAM ロールを編集します。
  - 新しい IAM ロールが作成され、他の AWS アカウント (ターゲットアカウント) に割り当てられます。また、そのロールに、ターゲットの AWS アカウントの資産にアクセスするために必要なアクセス権を持つポリシーを割り当てます。
  - その他の AWS アカウントの IAM ロールは、ソースアカウントの IAM ロールを信頼する必要があります ([ロール (Roles)]、[信頼関係 (Trust relationships)]タブの順に選択)。
  - ソースアカウントの IAM ロールには、ソースロールがその他の AWS アカウントのロール (`sts:AssumeRole`) を引き受けられるようにするインラインポリシー ([ロール (Roles)]、[アクセス権 (Permissions)]タブの順に選択) が割り当てられます。
  - ソースアカウントの IAM ロールがクロスアカウントの IAM ロールを引き受けている場合の、一時的なセキュリティクレデンシャルの有効性は、少なくとも 1 時間に設定されます ([最大 CLI/API セッションの期間 (Maximum CLI/API session duration)]フィールド)。

  p.117 の「クロスアカウントの構成を作成する前に」を参照してください。
- AWS クラウドの資産が AWS KMS CMK (カスタマ管理キー) を使用して暗号化されている場合は、次のことを確認する必要があります。
  - NetBackup Snapshot Manager プラグインを構成するための IAM ユーザーを選択する場合は、IAM ユーザーが CMK のキーユーザーとして追加されていることを確認します。
  - ソースアカウントの構成については、NetBackup Snapshot Manager インスタンスに関連付けられている IAM ロールが CMK のキーユーザーとして追加されていることを確認します。

- クロスアカウントの構成については、その他の AWS アカウント (クロスアカウント) に関連付けられている IAM ロールが CMK のキーユーザーとして追加されていることを確認します。

これらの IAM ロールとユーザーを CMK キーユーザーとして追加すると、これらのユーザーは、資産の暗号化操作に直接 AWS KMS CMK キーを使用できます。詳しくは、AWS のドキュメントを参照してください。

- NetBackup Snapshot Manager インスタンスでインスタンスメタデータサービス (IMDsv2) が有効になっている場合、VM の HttpPutResponseHopLimit パラメータが 2 に設定されていることを確認します。

  HttpPutResponseHopLimit パラメータの値が 2 に設定されていない場合、AWS はマシンに作成された NetBackup Snapshot Manager コンテナからメタデータをフェッチする呼び出しに失敗します。

  IMDsv2 サービスについて詳しくは、『IMDSv2 の使用』を参照してください。

クロスアカウントの構成を作成する前に

NetBackup Snapshot Manager のクロスアカウントの構成では、構成を作成する前に次の追加タスクを実行する必要があります。

- 他の AWS アカウント (ターゲットアカウント) への新しい IAM ロールの作成
- IAM ロール用の新しいポリシーの作成と、そのロールに、ターゲットの AWS アカウントの資産にアクセスするために必要なアクセス権を持つポリシーが割り当てられていることの確認
- ソースとターゲットの AWS アカウント間での信頼関係の確立
- ソース AWS アカウントで、ソース AWS アカウントの IAM ロールがターゲット AWS アカウントの IAM ロールを引き受けることができるポリシーの作成
- ターゲットの AWS アカウントで、最大 CLI/API セッション期間を 1 時間以上に設定

次の手順を実行します。

1 AWS 管理コンソールを使用して、NetBackup Snapshot Manager で保護する資産が含まれる追加の AWS アカウント (ターゲットアカウント) に、IAM ロールを作成します。

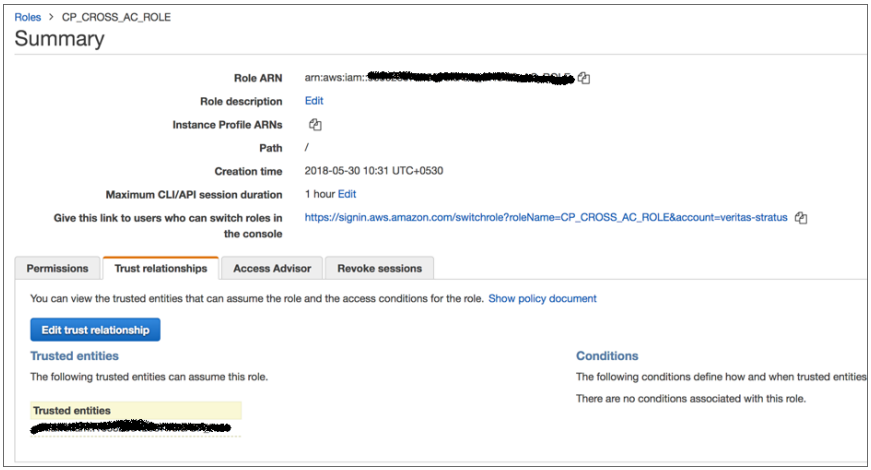
IAM ロールを作成するときに、別の AWS アカウントとしてロールタイプを選択します。

2 前の手順で作成した IAM ロールのポリシーを定義します。

IAM ロールがターゲットの AWS アカウントのすべての資産 (EC2、RDS など) にアクセスするために必要なアクセス権を、ポリシーが持っていることを確認します。

3 ソースとターゲットの AWS アカウント間で信頼関係を設定します。

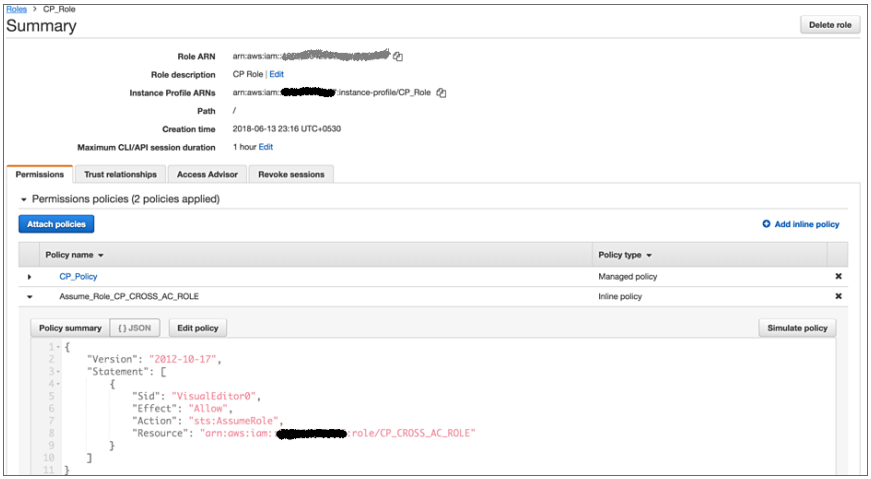
ターゲットの AWS アカウントで、信頼関係を編集し、ソースアカウント番号とソースアカウントのロールを指定します。



この処理によって、ソースアカウントの IAM ロールに関連付けられているクレデンシャルを使用して、ソースの AWS アカウントでホストされている NetBackup Snapshot Manager インスタンスのみがターゲットロールを引き受けられます。他のエンティティはこのロールを引き受けることはできません。

4 ソース AWS アカウントにターゲットロールへのアクセス権を付与します。

ソース AWS アカウントの[概略 (Summary)]ページで、インラインポリシーを作成し、ソースの AWS アカウントがターゲットロール (`sts:AssumeRole`) を引き受けられるようにします。



5 ターゲットアカウントの[概略 (Summary)]ページで、[最大 CLI/API セッションの期間 (Maximum CLI/API session duration)]フィールドを編集して、期間を 1 時間以上に設定します。

この設定によって、ソースアカウントの IAM ロールが、ターゲットアカウントの IAM ロールが有効であるとみなすときに取得する一時的なセキュリティクレデンシャルの期間が決まります。

単一のソースプロバイダの構成を使用した複数のクロスアカウントの保護

ソースアカウントを使用して構成された単一のプロバイダ構成を使用して、複数のクロスアカウントの資産を保護できます。

この機能を使うには、NetBackup Snapshot Manager と NetBackup プライマリサーバーが 11.1 以降にアップグレードされていることを確認します。

メモ: 他の既存のクロスアカウントの構成を使用して、すでに保護されているクロスアカウントは変更できません。

同じソースプラグイン構成を使用してクロスアカウントを構成する方法

1. 他の AWS アカウント (ターゲットアカウント) に新しい IAM ロールを作成します。
2. IAM ロール用の新しいポリシーを作成し、そのロールに、ターゲット AWS アカウントの資産にアクセスするために必要なアクセス権が割り当てられていることを確認します。
3. ソースとターゲットの AWS アカウント間で信頼関係を確立させます。

   たとえば、その信頼ポリシーで、プロバイダの構成に使用されるソースアカウントのロールに[役割の引き受け (Assume Role)]処理を許可します。この信頼ポリシーの構成の例を次に示します。

```
{
            "Effect": "Allow",
            "Principal": {
                "AWS":
"arn:aws:iam::<source-account-id>:role/source-role"
            },
            "Action": "sts:AssumeRole",
}
```

インラインポリシーを作成および編集する方法

1 クロスアカウントをソースアカウントから保護できるインラインポリシーを作成します。

ソースアカウントで、Implicitly_Protected_Accounts という名前のインラインポリシーを作成します。これにより、他のアカウントの役割で[役割の引き受け (Assume Role)]処理が許可されます。黙示的な保護対象アカウントごとに 1 つのエントリを作成します。

例:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [

                 "sts:AssumeRole"

             ]
            "Resource": [


"arn:aws:iam::<cross-account-1-id>:role/cross-role-1",


"arn:aws:iam::<cross-account-2-id>:role/cross-role-2"

            ]

        }
    ]
}
```

メモ: ソースアカウントの既存の役割を編集し、Implicitly_Protected_Accounts のような正確な名前を持つインラインポリシーを追加します。

2 ソースアカウントの構成にインラインポリシーの読み取りを許可するには、次の追加の IAM 権限を指定します。

```
iam:GetPolicyRole
```

3 インラインポリシーを編集して保存し、保護対象のすべてのクロスアカウントを追加して、同じソースアカウントの構成を割り当てます。このインラインポリシーで、クロスアカウントの役割に［役割の引き受け (Assume Role)］処理を許可します。黙示的な保護対象アカウントごとに 1 つのエントリを作成します。

AWS Systems Service Manager を使用したアプリケーションの整合性スナップショットの前提条件

VM の作業負荷の AWS SSM (Systems Service Manager) を使用してファイルシステムまたはアプリケーションの整合性スナップショットを作成する前に、次の操作を実行していることを確認します。

- VM の作業負荷に SSM エージェントをインストールし、AWS SSM エージェントサービスをアクティブにする必要があります。
  詳しくは、「SSM Agent の手動インストール」を参照してください。
- VM 作業負荷に関連付けられている IAM ロールは、次の権限を持つポリシーと AmazonSSMManagedInstanceCore ポリシーで更新する必要があります。

```
{
            "Sid": "providerManagedConsistency",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots",
                "ec2:CreateTags",
                "ec2:CreateSnapshot"
            ],
            "Resource": [
                "*"
            ]
    }
```

p.126 の「NetBackup Snapshot Manager に必要な AWS アクセス権」を参照してください。

- **Windows の場合**

  - 4.1.144 以上の AWSPowerShell バージョン (AWS PowerShell)
  - 2.3.2 以上のバージョンの AWS VSS コンポーネント (VSS パッケージのインストール)

  メモ: 上記のモジュールがインストールされていない場合、NetBackup Snapshot Manager は、VM の作業負荷がインターネットにアクセスできればそれらをインストールします。

  サポート対象の Windows OS バージョンと AWS VSS コンポーネントパッケージの完全なリストについては、AWS VSS ソリューションのバージョン履歴を参照してください。

Linux の場合

AWS CLI の最新版をインストールまたは更新します。

AWS CLI の最新版のインストールまたは更新

Windows の場合

デフォルトではアプリケーションの整合性スナップショットが作成されます。

Linux の場合

ファイルシステムの整合性スナップショットが作成されます。

アプリケーションの整合性スナップショットを作成する必要がある場合は、次の手順を実行します。

- ディレクトリ (`/etc/veritas`) が Linux VM の作業負荷に存在する必要があります (存在しない場合は作成します)。
- `/etc/veritas` ディレクトリ内に `provider_managed_consistency.conf` ファイルを次のように作成します。

  ```
  # cat
  /etc/veritas/provider_managed_consistency.conf


  PRE_SCRIPT_LOCATION =
  "/preScript.sh"
  PRE_SCRIPT_PARAMS = ""
  POST_SCRIPT_LOCATION =
  "/postScript.sh"
  POST_SCRIPT_PARAMS = ""
  ```

- プリスクリプトとポストスクリプトを作成し、その絶対パスを `provider_managed_consistency.conf` ファイルに追加する必要があります。
  プリスクリプトは、ネイティブアプリケーション API を呼び出し、IO を静止し、メモリ内のコンテンツをディスクにフラッシュします。これらの処理によって、スナップショットがアプリケーション整合であることを確認できます。
  ポストスクリプトはネイティブアプリケーション API を使用して IO を解凍します。これは、VM スナップショット後にアプリケーションが通常の操作を再開することを可能にします。
- プリスクリプトパラメータを `PRE_SCRIPT_PARAMS` に渡し、ポストスクリプトパラメータを `POST_SCRIPT_PARAMS` キーに渡す必要があります。
- ファイルの権限を次のように変更します。
  `chmod 700 /preScript.sh /postScript.sh`

上記の前提条件が満たされている場合、デフォルト NetBackup Snapshot Manager では VM の作業負荷のファイルシステムまたはアプリケーション整合のスナップショットが作成されます。AWS クラウドプロバイダプラグインが構成されている場合、指定した AWS アカウントと領域に Veritas-Consistent-Snapshot という名前の新しい SSM ドキュメントが作成されます。この SSM ドキュメントは、NetBackup Snapshot Manager が管理し、ユーザーが変更することはできません。

ログは、次の該当する場所にあります。

- Snapshot Manager: /cloudpoint/logs/flexsnap.log
- ホスト VM: Amazon SSM ログを確認します (SSM エージェントログの表示)

VPC エンドポイントを使用した AWS プラグイン構成の前提条件

VPC エンドポイントサービスを使用して AWS プラグインを構成する前に、次の操作を実行していることを確認します。

表 5-3 VPC エンドポイントサービスを使用するための前提条件

ソースアカウントの構成	クロスアカウントの構成
AWS STS (セキュリティトークンサービス) のエンドポイントを作成します。	ソースアカウント (NetBackup Snapshot Manager が存在するアカウント) で STS サービスのエンドポイントを作成します。
必要に応じて他のエンドポイントサービスを作成します。AWS サービスリストについて詳しくは、AWS のマニュアルの AWS PrivateLink と統合する AWS サービスのセクションを参照してください。	
NetBackup Snapshot Manager は、VPC エンドポイントを使用してプラグインが構成されるのと同じリージョンに存在する必要があります。	

インストールされている NetBackup Snapshot Manager が FIPS 対応の場合は、VPC エンドポイントベースの構成の作成は必要ありません。

NetBackup Snapshot Manager に必要な AWS アクセス権

次の表に、AWS プラグインの構成と資産の検出、スナップショットの管理などの機能を NetBackup Snapshot Manager に追加できる IAM ロール定義に必要な権限を一覧表示します。

表 5-4 NetBackup Snapshot Manager の機能と AWS クラウドプロバイダの権限

機能	タスク/操作	必要な権限:
VM ベース		

機能	タスク/操作	必要な権限:
KMS (暗号化および復号)	さまざまな操作中にKMSキーを一覧表示します。	kms:ListKeys
	NetBackup Snapshot Manager によって提供される KMS 機能。	kms:Encrypt kms:Decrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext kms:CreateGrant
	暗号化されたスナップショットのレプリケーションに AWS で内部的に必要です。	kms:ReEncryptTo kms:ReEncryptFrom
	特定の KMS キーの情報を取得します。	kms:DescribeKey
	さまざまな操作中に KMS キーエイリアスを一覧表示します。	kms:ListAliases

機能	タスク/操作	必要な権限:
RDSリソースの保護	RDS データベーススナップショットを一覧表示します (検出)。	rds:DescribeDBSnapshots
	RDS データベースクラスタを一覧表示します (検出)。	rds:DescribeDBClusters
	RDS データベースクラスタスナップショットを一覧表示します (検出)。	rds:DescribeDBClusterSnapshots
	RDS データベーススナップショットを削除します (スナップショットの失効)。	rds:DeleteDBSnapshot
	RDS データベーススナップショットを作成します。	rds:CreateDBSnapshot
	RDS データベースクラスタスナップショットを作成します。	rds:CreateDBClusterSnapshot
	クロスアカウントレプリケーションのために、RDS データベーススナップショットを別のアカウントと共有または共有解除します。	rds:ModifyDBSnapshotAttribute
	RDS データベースサブネットグループを一覧表示します (検出)。	rds:DescribeDBSubnetGroups
	RDS データベースインスタンスを一覧表示します (検出)。	rds:DescribeDBInstances
	レプリケーションに使用するために、リージョン間で RDS データベーススナップショットをコピーします。	rds:CopyDBSnapshot
	レプリケーションに使用するために、リージョン間で RDS データベースクラスタスナップショットをコピーします。	rds:CopyDBClusterSnapshot
	属性を読み取るために、クロスアカウントスナップショットのリストアまたはレプリケート操作中に暗黙的に必要です。	rds:DescribeDBSnapshotAttributes
	すべての RDS プロキシを一覧表示します。	rds:DescribeDBProxies
	特定のプロキシの RDS データベースインスタンスを一覧表示します。	rds:DescribeDBProxyTargets

機能	タスク/操作	必要な権限:
	RDS データベースクラスタスナップショットを削除します (スナップショットの失効)。	`rds:DeleteDBClusterSnapshot`
	RDS リソースのタグを一覧表示します。	`rds:ListTagsForResource`
	スナップショット、レプリケーション、リストア中に、RDS リソースのタグを追加します。	`rds:AddTagsToResource`
	指定した RDS プロキシのプロキシエンドポイントを一覧表示します。	`rds: DescribeDBProxyEndpoints`
	暗号化されたデータを取得および復号する権限を付与します。	`secretsmanager:GetSecretValue`
	ある場所で提供されるインスタンスタイプの詳細を取得します。RDS データベースのバックアップまたはリストア中の並列処理を決定するために使用します。	`ec2:DescribeInstanceTypes`

機能	タスク/操作	必要な権限:
RDSリソースのリカバリ	RDS データベースインスタンスの設定を変更します。 リストア中にセキュリティグループを変更します。	rds:ModifyDBInstance
	クロスアカウントレプリケーションのために、RDS データベースクラスタスナップショットを別のアカウントと共有または共有解除します。	rds:ModifyDBClusterSnapshotAttribute
	スナップショットからRDSデータベースインスタンスを作成します (スナップショットのリストア)。	rds:RestoreDBInstanceFromDBSnapshot
	RDS データベースクラスタの設定を変更します。	rds:ModifyDBCluster
	スナップショットからRDSデータベースクラスタを作成します (スナップショットのリストア)。	rds:RestoreDBClusterFromSnapshot
	RDS クラスタのリストア中に RDS データベースインスタンスを作成します。	rds:CreateDBInstance
	RDS データベースクラスタをリストアするために AWS で内部的に必要です。	rds:RestoreDBClusterToPointInTime
	RDSデータベースセキュリティグループを作成するには、デフォルトのセキュリティグループを使用してRDSをリストアします。	rds:CreateDBSecurityGroup
	RDSデータベースクラスタを作成します。	rds:CreateDBCluster
	RDS データベースインスタンスをリストアするために AWS で内部的に必要です。	rds:RestoreDBInstanceToPointInTime
	RDS クラスタスナップショットのリストア時にパラメータグループに関する情報を取得します。	rds:DescribeDBClusterParameterGroups

機能	タスク/操作	必要な権限:
EC2 リソースのバックアップ	API 要求の作成に使用されているユーザーまたは役割に関する情報を取得します (これを使用して CSP を構成します)。	`sts:GetCallerIdentity`
	これは、クロスアカウントプロバイダの構成を、クロスアカウントの役割に必要なその他の前提条件と共に構成するために、ソースアカウントの役割で必要です。	`sts:AssumeRole`
	EBS ボリュームスナップショットを作成します。	`ec2:CreateSnapshot`
	EC2 インスタンススナップショットを作成します (接続されているすべてのディスクのスナップショット)。	`ec2:CreateSnapshots`
	EC2 インスタンスを一覧表示します (検出)。	`ec2:DescribeInstances`
	指定した EC2 インスタンスの状態を取得します。	`ec2:DescribeInstanceStatus`
	クロスアカウントレプリケーションのために、EBS スナップショットを別のアカウントと共有または共有解除します。	`ec2:ModifySnapshotAttribute`
	1 つのリージョンから別のリージョンに EBS スナップショットをレプリケートします。 EC2 インスタンスのスナップショットをディスク別にレプリケートします。	`ec2:CopySnapshot`
	EBS スナップショットを一覧表示します (検出)。	`ec2:DescribeSnapshots`
	指定した EBS ボリュームの状態を取得します。	`ec2:DescribeVolumeStatus`
	EBS ボリュームを一覧表示します (検出)。	`ec2:DescribeVolumes`
	EC2 インスタンススナップショットのリストア時に使用され、AMI が中間で登録され、EC2 インスタンスが起動されます。	`ec2:RegisterImage`

機能	タスク/操作	必要な権限:
	さまざまな操作中に指定した EBS ボリュームの特定の属性を取得します。	ec2:DescribeVolumeAttribute
	サブネットを一覧表示します (検出)。	ec2:DescribeSubnets
	VPC を一覧表示します (検出)。	ec2:DescribeVpcs
	EC2 インスタンスのリストア時に登録した中間 AMI を登録解除します	ec2:DeregisterImage
	EBS スナップショットを削除します (スナップショットの失効/スナップショットの作成エラー時のクリーンアップ)。	ec2:DeleteSnapshot
	指定した EC2 インスタンスの特定の属性を取得します。	ec2:DescribeInstanceAttribute
	リージョンを一覧表示します。	ec2:DescribeRegions
	可用性ゾーンを一覧表示します (検出)。	ec2:DescribeAvailabilityZones
	クロスアカウントレプリケーション中に変更された、指定したスナップショットの権限設定をリセットします。	
	クロスアカウントレプリケーション中に変更された、指定したスナップショットの権限設定をリセットします。	ec2:ResetSnapshotAttribute
	専用ホストを一覧表示します (検出)。	ec2:DescribeHosts
	AMI (NetBackup Snapshot Manager によって作成された EC2 インスタンススナップショット) を一覧表示します (検出)	ec2:DescribeImages
	セキュリティグループを一覧表示します (検出)。	ec2:DescribeSecurityGroups
	EC2 インスタンスのネットワークインターフェースを一覧表示します。EC2 インスタンスの検出に必要です。	ec2:DescribeNetworkInterfaces
	特定のリソースで作成されたタグを取得します。	ec2:DescribeTags
		ec2:DescribeInstanceTypes

機能	タスク/操作	必要な権限:
	ある場所で提供されるインスタンス情報の詳細を取得します。	

機能	タスク/操作	必要な権限:
EC2 リソースのリカバリ	EC2 インスタンスを作成します (ホストスナップショットのリストア)。	`ec2:RunInstances`
	特定のインスタンスに指定されたネットワークインターフェースを接続するために AWS によって内部的に使用されます。ホストスナップショットのリストアに必要です。	`ec2:AttachNetworkInterface`
	ロールバックリストア時に EC2 インスタンスから EBS ボリュームを切断します。また、GRT ワークフロー中に、最初に接続された中間ボリュームは後で切断されます。	`ec2:DetachVolume`
	ロールバックリストアの場合に、新しい EBS ボリュームを EC2 インスタンスに接続します。また、EC2 インスタンスへのボリュームスナップショットのリストア時に、新たに作成されたディスクは、指定されたインスタンスに接続されます。	`ec2:AttachVolume`
	EC2 リソースのタグを削除します。NetBackup Snapshot Manager の一部の内部タグは、後で削除する必要があるさまざまな操作中に作成されます。	`ec2:DeleteTags`
	EC2 リソースのタグを作成します。作成またはリストアされたリソースに、NetBackup Snapshot Manager メタデータタグとソースリソースタグを使用してタグ付けするために必要です。	`ec2:CreateTags`
	指定されたインスタンスの電源をオンにします。リストア後にインスタンスを開始または停止するオプションが指定されているリストアフロー中に必要です。	`ec2:StartInstances`
	指定されたインスタンスの電源をオフにします。リストア後にインスタンスを開始または停止するオプションが指定されているリストアフロー中に必要です。	`ec2:StopInstances`

機能	タスク/操作	必要な権限:
	リストア操作が失敗した場合に EC2 インスタンスを削除します。また、バックアップコピーからのリストア中に作成された中間 EC2 インスタンスを削除する場合にも必要です。	ec2:TerminateInstances
	EBS ボリュームをスナップショットから作成します。ボリュームスナップショットのリストアおよびインスタンススナップショットロールバックのリストア時に使用されます。	ec2:CreateVolume
	リストア操作が失敗した場合に EBS ボリュームを削除します。ロールバックリストアが正常に行われる場合は、切断されたボリュームを削除します。GRT 操作中に作成された中間ボリュームを削除します。バックアップコピーからのリストア中に作成された中間 EC2 インスタンスと一緒にボリュームを削除します。	ec2:DeleteVolume
	リストアされたインスタンスに関連付けられている IAM ロールの IAM インスタンスプロファイルの関連付けの状態を取得します。	ec2:DescribeIamInstanceProfileAssociations
	IAM ロールをリストアされた EC2 インスタンスに接続します。	ec2:AssociateIamInstanceProfile
	リストア時に EC2 インスタンスまたはネットワークインターフェースにエラスティック IP を関連付けます。	ec2:AssociateAddress
	リストアされた EC2 インスタンスと関連付けるためにユーザーが指定したキーペアを検証するための SSH キーペアを一覧表示します。	ec2:DescribeKeyPairs
	EC2 インスタンスのリストアのために選択したサブネットに関連付けられている可用性ゾーンが、インスタンスタイプをサポートしているかどうかを確認します。	ec2:DescribeInstanceTypeOfferings
		ec2:GetEbsEncryptionByDefault

機能	タスク/操作	必要な権限:
	現在のリージョンのアカウントに対して EBS 暗号化がデフォルトで有効になっているかどうかを確認するために、AWS によって内部的に使用されます。	
	リストアされた EC2 インスタンスの元のインスタンスに従ってブロックデバイスマッピングを変更します。	ec2:ModifyInstanceAttribute
スナップショットからのバックアップ	バックアップ対象のスナップショットのブロックを一覧表示します。	ebs:ListSnapshotBlocks
	特定のスナップショットブロックのデータを取得するには、スナップショットブロックを読み込みます。	ebs:GetSnapshotBlock
	同じ EBS ボリュームの 2 つのスナップショット間で変更されたブロックを一覧表示します。	ebs:ListChangedBlocks
バックアップコピーからのリストア	すべてのブロックを書き込んだ後にスナップショットを完了としてマークするには、リストア後にスナップショットを閉じます。	ebs:CompleteSnapshot
	バックアップからのリストア時に、新しく作成されたスナップショットにブロックを書き込みます。	ebs:PutSnapshotBlock
	バックアップコピーからのリストア用のブロック書き込みに使用する空のスナップショットを作成します。	ebs:StartSnapshot

機能	タスク/操作	必要な権限:
ID の管理と認証	CSP で構成されている AWS アカウントのエイリアスを取得します。これは、インテリジェントグループを含むさまざまなコンテキストで利用可能な AWS アカウントの表示名に使用されます。	`iam:ListAccountAliases`
	一連の操作に対して IAM ポリシーと権限をシミュレートします。CSP 構成で使用されているユーザーまたは役割に必要な権限があるかどうかを確認するために使用します。	`iam:SimulatePrincipalPolicy`
	ソースアカウントの構成にインラインポリシーの読み取りを許可するには、この追加の IAM 権限を指定します。	`iam:GetPolicyRole`

機能	タスク/操作	必要な権限:
PaaS 作業負荷の保護 (DynamoDB)	検出中に使用される DynamoDB テーブルを一覧表示します。	dynamodb:ListTables
	バックアップ中に特定の DynamoDB テーブルの情報を取得します。	dynamodb:DescribeTable
	リストア時にテーブルを作成します。	dynamodb:CreateTable
	dynamodb テーブルのリストア中にバッチ書き込みを実行します。	dynamodb:BatchWriteItem
	バックアップ中に、dynamodb テーブルの連続バックアップを一覧表示します。	dynamodb:DescribeContinuousBackups
	バックアップ中に s3 へのバックアップを続行する dyanmodb テーブルの指定した時点へのリストアを実行します。	dynamodb:ExportTableToPointInTime
	dynamodb テーブルの s3 への連続バックアップのエクスポートの状態を確認します。	dynamodb:DescribeExport
	リストア中にエラーが発生した場合にテーブルを削除します。	dynamodb:DeleteTable
	dynamodb テーブルのメタデータを更新します。	dynamodb:UpdateTable
	まだ設定されていない場合は、テーブルの連続バックアップを設定します。	dynamodb:UpdateContinuousBackups
	S3 からテーブルをインポートします	dynamodb:ImportTable
	インポート操作を説明します	dynamodb:DescribeImport

機能	タスク/操作	必要な権限:
S3 (DynamoDB) を使用した CloudWatch ログのリストア	ロググループを作成して、S3 からの DynamoDB インポート操作のログをリストアします。	`logs:CreateLogGroup`
	S3 からの DynamoDB インポート操作のログの読み取りと書き込みに使用するログストリームを作成します。	`logs:CreateLogStream`
	S3 からの DynamoDB インポート操作中に作成されたロググループを説明します。	`logs:DescribeLogGroups`
	S3 からの DynamoDB インポート操作中に作成されたログストリームを説明します。	`logs:DescribeLogStreams`
	S3 からの DynamoDB インポート操作のログイベントを書き込みます。	`logs:PutLogEvents`
	S3 からの DynamoDB インポート操作中に作成されるログのログ保持ポリシーを設定します。	`logs:PutRetentionPolicy`

機能	タスク/操作	必要な権限:
PaaS 作業負荷の保護 (Redshift データベース)	Redshift クラスタのデータベースを一覧表示します。データベース名とそのメタデータに関する情報を取得します。この権限はクラスタレベルの権限です。	`redshift:ListDatabases`
	IAM を使用して Redshift クラスタデータベースに接続します。	`redshift:GetClusterCredentialsWithIAM`
	Redshift クラスタデータベースで問い合わせを実行します。	`redshift-data:ExecuteStatement`
	redshift API エンドポイントとは別のエンドポイントである redshift-data API を介して Redshift クラスタのデータベースを一覧表示します。この権限は、サーバーなしで Redshift を実行する場合に必要です。	`redshift-data:ListDatabases`
	Redshift クラスタデータベースで実行された SQL ステートメントの一時的にキャッシュされた結果をフェッチします。	`redshift-data:GetStatementResult`
	Redshift クラスタのプロパティを取得します。	`redshift:DescribeClusters`
	NetBackup ジョブのキャンセル中に使用した Redshift クラスタデータベースで実行された問い合わせを取り消します。	`redshift-data:CancelStatement`
	Redshift クラスタデータベースに接続します。	`redshift:GetClusterCredentials`
	Amazon Redshift Data API で問い合わせが実行される場合に、特定のインスタンスに関する詳細を取得するために必要です。	`redshift-data:DescribeStatement`

機能	タスク/操作	必要な権限:
PaaS 作業負荷の保護 (Redshift クラスタ)	Redshift クラスタのデータベースを一覧表示します。データベース名とそのメタデータに関する情報を取得します。この権限はクラスタレベルの権限です。	redshift:ListDatabases
	Redshift クラスタのプロパティを取得します。	redshift:DescribeClusters
	Redshift クラスタのタグを作成します。	redshift:CreateTags
	指定したクラスタの手動スナップショットを作成します。	redshift:CreateClusterSnapshot
	クラスタスナップショットのプロパティを取得します。	redshift:DescribeClusterSnapshots
	クラスタスナップショットを削除します。	redshift:DeleteClusterSnapshot
	クラスタサブネットグループを取得します。	redshift:DescribeClusterSubnetGroups
	クラスタスナップショットからリストアします。	redshift:RestoreFromClusterSnapshot
	インターネットゲートウェイにアクセスします。	ec2:DescribeInternetGateways
	インターフェースの割り当てとプライベート IP を一覧表示します	ec2:DescribeAddresses
	可用性ゾーンを一覧表示します。	ec2:DescribeAvailabilityZones
	VPC を一覧表示します。	ec2:DescribeVpcs
	アカウント属性リストを取得します。	ec2:DescribeAccountAttributes
	サブネットを一覧表示します。	ec2:DescribeSubnets
	セキュリティグループを一覧表示します。	ec2:DescribeSecurityGroups
	IAM ロールにアクセスします。	iam:GetRole

機能	タスク/操作	必要な権限:
PaaS 作業負荷の保護 (Neptune)	AWS Neptune スナップショットを一覧表示します - 検出	neptune:DescribeDBSnapshots
	AWS Neptune クラスタを一覧表示します - 検出	neptune:DescribeDBClusters
	AWS Neptune スナップショットを削除します	neptune:DeleteDBSnapshot
	AWS Neptune クラスタを一覧表示します	neptune:DescribeDBClusters
	Neptune データベーススナップショットを作成します	neptune:CreateDBSnapshot
	Neptune データベースクラスタを作成します	neptune:CreateDBCluster
	Neptune データベースサブネットグループを一覧表示します	neptune:DescribeDBSubnetGroups
	Neptune データベースクラスタスナップショットを削除します	neptune:DeleteDBSnapshot
	AWS Neptune クラスタスナップショットを一覧表示します	neptune:DescribeDBSnapshots

機能	タスク/操作	必要な権限:
PaaS 作業負荷の保護 (DocumentDB)	AWS DocumentDB スナップショットを一覧表示します - 検出	rds:DescribeDBSnapshots
	AWS DocumentDB クラスタを一覧表示します - 検出	rds:DescribeDBClusters
	AWS DocumentDB スナップショットを削除します	rds:DeleteDBSnapshot
	AWS DocumentDB クラスタを一覧表示します	rds:DescribeDBClusters
	DocumentDB データベーススナップショットを作成します	rds:CreateDBSnapshot
	DocumentDB データベースクラスタを作成します	rds:CreateDBCluster
	DocumentDB データベースサブネットグループを一覧表示します	rds:DescribeDBSubnetGroups
	DocumentDB データベースクラスタスナップショットを削除します	rds:DeleteDBSnapshot
	Amazon DocumentDB クラスタスナップショットを一覧表示します	rds:DescribeDBClusterSnapshots
PaaS 作業負荷の保護 (RDS Custom for Oracle と RDS Custom for SQL)	AWS アカウントの API アクティビティを記録する証跡を設定するために、リソースの使用状況、セキュリティイベント、ユーザー操作を追跡して監視できるようにします。	cloudtrail:CreateTrail
	AWS CloudTrail 証跡のログを有効にします。	cloudtrail:StartLogging

機能	タスク/操作	必要な権限:
PaaS 作業負荷の保護 (S3)	DynamoDB、Custom for SQL、Custom for Oracle、および Redshift のバックアップまたはリストア時に必要な s3 バケットを作成します。	`s3:CreateBucket`
	DynamoDB、Custom for SQL、Custom for Oracle、および Redshift のバックアップまたはリストア時に使用されたバケットがすでに存在するかどうかを確認します。	`s3:ListBucket`
	DynamoDB、Custom for SQL、Custom for Oracle、および Redshift のバックアップ中にバケットに格納された s3 オブジェクト (ファイル) の ACL を取得します。	`s3:GetObjectAcl`
	DynamoDB、Custom for SQL、Custom for Oracle、および Redshift のバックアップ中にバケットに格納された s3 オブジェクト (ファイル) のコンテンツを取得します。	`s3:GetObject`
	DynamoDB および Redshift のバックアップまたはリストア時に必要な s3 バケットからオブジェクトを削除します。	`s3:DeleteObject`
	DynamoDB および Redshift のリストア時に必要な s3 バケットにデータをアップロードします。	`s3:PutObject`

機能	タスク/操作	必要な権限:
オブジェクトのリストアロックの構成 (S3)	オブジェクトにオブジェクトの保持構成を配置します。	`s3:PutObjectRetention`
	Custom for Oracle と Custom for SQL のバックアップ中に Amazon S3 バケットのバケットポリシーを変更します。	`s3:PutBucketPolicy`
	Custom for Oracle と Custom for SQL のバックアップ中に Amazon S3 バケットのオブジェクトロック構成を構成または変更します。	`s3:PutBucketObjectLockConfiguration`
	Custom for Oracle と Custom for SQL のバックアップ中に Amazon S3 バケットのバージョンを有効化または変更します。	`s3:PutBucketVersioning`
	Custom for Oracle および Custom for SQL のバックアップ中に、Amazon S3 バケット内のオブジェクトに関連付けられたタグを取得します。	`s3:GetObjectTagging`

機能	タスク/操作	必要な権限:
プロバイダ管理の整合性スナップショット	SSM で構成されたインスタンスにコマンドを送信するために、SSM ドキュメントを実行してスナップショットを取得します。	ssm:SendCommand
	SSM ドキュメントの詳細を取得し、アプリケーションの整合性スナップショットを作成するために NetBackup Snapshot Manager によって作成されたドキュメントの存在を確認します。	ssm:DescribeDocument
	SSM で構成されたオンラインのインスタンスのリストを取得します。この情報は、インスタンスのプラットフォームのフェッチにも使用されます。	ssm:DescribeInstanceInformation
	NetBackup Snapshot Manager によって作成された SSMドキュメントのデフォルトバージョンを更新します。	ssm:UpdateDocumentDefaultVersion
	アップグレードの場合に、SSMドキュメントの内容を最新のものに更新します。	ssm:UpdateDocument
	アプリケーションの整合性スナップショットを作成するために使用する SSM ドキュメントを作成します。	ssm:CreateDocument
	コマンドの状態と出力 (つまりドキュメントの実行)と、スナップショットの応答を取得します。	ssm:GetCommandInvocation
	アプリケーションの整合性スナップショットを取得します。	ssm:listCommand
単一のソースアカウントの構成を使用した複数のクロスアカウントの保護	インラインポリシーを読み取ります。これはクロスアカウントとそれぞれの役割をマッピングするために必要です。	iam:GetPolicyRole
プロバイダ管理の整合性スナップショット 役割/ポリシー: AmazonSSMManagedInstanceCore		

機能	タスク/操作	必要な権限:
作業負荷 VM の権限	SSM ドキュメントが実行されている作業負荷 VM の整合性スナップショットを作成します。	`ec2:CreateSnapshots`
	SSM ドキュメントで作成したスナップショットのタグを作成します。	`ec2:CreateTags`
	ディスク別に VM ディスクのスナップショットを作成します。	`ec2:CreateSnapshot`
Kubernetes クラスタベース 役割/ポリシー: AmazonEKSClusterPolicy、AmazonEKSWorkerNodePolicy、AmazonEC2ContainerRegistryPowerUser、AmazonEKS_CNI_Policy、AmazonEKSServicePolicy		
EKS	スケーリング構成に関する Kubernetes クラスタのノードグループの詳細を取得します。	`eks:DescribeNodegroup`
	クラスタで行われたスケーリングの状態を取得します。	`eks:DescribeUpdate`
	Kubernetes クラスタをスケーリングするには、ノードグループのサイズを更新します。	`eks:UpdateNodegroupConfig`
	Kubernetes クラスタを一覧表示するには、クラスタを検出します。	`eks:ListClusters`
	指定した Kubernetes クラスタの情報を取得するには、クラスタ属性を検出します。	`eks:DescribeCluster`
	EKS クラスタ内のノードグループのリストを取得します。	`eks:ListNodegroups`
マーケットプレイス配備		

機能	タスク/操作	必要な権限:
高可用性	EKS およびマーケットプレイスの配備に必要です。	autoscaling:UpdateAutoScalingGroup
		autoscaling:AttachInstances
	マーケットプレイスを通じて DR を実行します。	autoscaling:DescribeScalingActivities
		autoscaling:TerminateInstanceInAutoScalingGroup
	DR 中に通知を送信します。	sns:Publish
		sns:GetTopicAttributes
配備	指定したアウトバウンド (エグレス) ルールを、リストア時にセキュリティグループに追加します。	ec2:AuthorizeSecurityGroupEgress
	指定したインバウンド (イングレス) ルールを、リストア時にセキュリティグループに追加します。	ec2:AuthorizeSecurityGroupIngress

JSON 形式の IAM ロールに必要な権限を次に示します。

```
{
    "PLUGIN_CONFIGURATION": {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "KMS",
                "Effect": "Allow",
                "Action": [
                    "kms:ListKeys",
                    "kms:Encrypt",
                    "kms:Decrypt",
                    "kms:ReEncryptTo",
                    "kms:DescribeKey",
                    "kms:ListAliases",
                    "kms:GenerateDataKey",
                    "kms:GenerateDataKeyWithoutPlaintext",
                    "kms:ReEncryptFrom",
                    "kms:CreateGrant"
                ],
                "Resource": [
                    "*"
```

```
        ]
    },
    {
        "Sid": "RDSBackup",
        "Effect": "Allow",
        "Action": [
            "rds:DescribeDBSnapshots",
            "rds:DescribeDBClusters",
            "rds:DescribeDBClusterSnapshots",
            "rds:DeleteDBSnapshot",
            "rds:CreateDBSnapshot",
            "rds:CreateDBClusterSnapshot",
            "rds:ModifyDBSnapshotAttribute",
            "rds:DescribeDBSubnetGroups",
            "rds:DescribeDBInstances",
            "rds:CopyDBSnapshot",
            "rds:CopyDBClusterSnapshot",
            "rds:DescribeDBSnapshotAttributes",
            "rds:DeleteDBClusterSnapshot",
            "rds:ListTagsForResource",
            "rds:AddTagsToResource"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "RDSRecovery",
        "Effect": "Allow",
        "Action": [
            "rds:ModifyDBInstance",
            "rds:ModifyDBClusterSnapshotAttribute",
            "rds:RestoreDBInstanceFromDBSnapshot",
            "rds:ModifyDBCluster",
            "rds:RestoreDBClusterFromSnapshot",
            "rds:CreateDBInstance",
            "rds:RestoreDBClusterToPointInTime",
            "rds:CreateDBCluster",
            "rds:RestoreDBInstanceToPointInTime",
            "rds:DescribeDBClusterParameterGroups"
        ],
        "Resource": [
            "*"
```

```
    ]
},
{
    "Sid": "EC2Backup",
    "Effect": "Allow",
    "Action": [
        "sts:GetCallerIdentity",
        "ec2:CreateSnapshot",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:ModifySnapshotAttribute",
        "ec2:CreateImage",
        "ec2:CopyImage",
        "ec2:CopySnapshot",
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes",
        "ec2:RegisterImage",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRegions",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeAvailabilityZones",
        "ec2:ResetSnapshotAttribute",
        "ec2:DescribeHosts",
        "ec2:DescribeImages",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:CreateSnapshots",
        "ec2:GetEbsEncryptionByDefault",
        "ec2:DescribeKeyPairs"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "EC2Recovery",
    "Effect": "Allow",
```

```
        "Action": [
            "ec2:RunInstances",
            "ec2:AttachNetworkInterface",
            "ec2:DetachVolume",
            "ec2:AttachVolume",
            "ec2:DeleteTags",
            "ec2:CreateTags",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:CreateVolume",
            "ec2:DeleteVolume",
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:AssociateIamInstanceProfile",
            "ec2:AssociateAddress",
            "ec2:DescribeInstanceTypeOfferings",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "EBS",
        "Effect": "Allow",
        "Action": [
            "ebs:ListSnapshotBlocks"
        ],
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "IAM",
        "Effect": "Allow",
        "Action": [
            "iam:ListAccountAliases",
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": [
            "*"
        ]
    }
```

```
    ]
},
"CLUSTER_ACCESS": {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EKSAccess",
            "Effect": "Allow",
            "Action": [
                "eks:ListClusters",
                "eks:DescribeCluster",
                "eks:DescribeNodegroup"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
},
"CLUSTER_AUTOSCALE": {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EKSScaleUp",
            "Effect": "Allow",
            "Action": [
                "eks:UpdateNodegroupConfig",
                "eks:DescribeUpdate"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "EKSScaleDown",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                 "autoscaling:TerminateInstanceInAutoScalingGroup",

                "autoscaling:DescribeScalingActivities"
            ],
            "Resource": [
```

```
                    "*"
                ]
            }
        ]
    }
}
```

NetBackup Snapshot Manager の AWS アクセス権の構成

AWS (アマゾンウェブサービス) 資産を保護するには、最初に NetBackup Snapshot Manager がそれらにアクセスできる必要があります。AWS 資産に対する作業を行う各 NetBackup Snapshot Manager ユーザーにアクセス権ポリシーを関連付ける必要があります。

NetBackup Snapshot Manager がさまざまな操作を実行できるように、NetBackup Snapshot Manager に関連付けられている IAM ロールが EC2 サービスを信頼する必要があります。EC2 サービスを信頼するには、次のように IAM ロールを追加または更新します。

AWS コンソールの、NetBackup Snapshot Manager に関連付けられている IAM ロールの[信頼関係 (Trust relationships)]で、信頼ポリシーを編集し、EC2 サービスがこの IAM ロールを引き受けることを許可して、次のように新しいステートメントを追加します。

```
{
  "Version": "2024-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com" },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

ユーザーアカウントまたはロールに、NetBackup Snapshot Manager に必要な最小限のアクセス権が割り当てられていることを確認します。

p.126 の「NetBackup Snapshot Manager に必要な AWS アクセス権」を参照してください。

アマゾンウェブサービスのアクセス権を構成するには

1. IAM (Identity and Access Management) から、AWS ユーザーアカウントを作成または編集します。
2. 次のいずれかを実行します。
   - 新しい AWS ユーザーアカウントを作成するには、次の手順を実行します。

- IAM で[ユーザー (Users)]ペインを選択し、[ユーザーの追加 (Add user)]をクリックします。
- [ユーザー名 (User name)]フィールドに、新しいユーザーの名前を入力します。
- [アクセス (Access)]タイプを選択します。この値は、AWS がアクセス権ポリシーにアクセスする方法を決定します。(この例では、プログラムによるアクセスを使用しています)。
- [次へ: アクセス権 (Next: Permissions)]を選択します。
- [*username* の権限を設定 (Set permissions for username)]画面で、[既存のポリシーを直接接続 (Attach existing policies directly)]を選択します。
- 以前に作成されたアクセス権ポリシー (以下を参照) を選択して、[次へ: レビュー (Next: Review)]を選択します。
- [アクセス権の概略 (Permissions summary)]ページで、[ユーザーの作成 (Create user)]を選択します。
- 新しく作成されたユーザーのアクセスキーとシークレットキーを取得します。

- AWS ユーザーアカウントを編集するには、次の手順を実行します。
  - [アクセス権の追加 (Add permissions)]を選択します。
  - [権限の付与 (Grant permissions)]画面で、[既存のポリシーを直接接続 (Attach existing policies directly)]を選択します。
  - 以前に作成されたアクセス権ポリシー (以下を参照) を選択して、[次へ: レビュー (Next: Review)]を選択します。
  - [アクセス権の概略 (Permissions summary)]画面で、[権限の追加 (Add permissions)]を選択します。

3 作成または編集したユーザー用の AWS プラグインを構成するには、プラグインの構成に関する注意事項を参照してください。

p.108 の「AWS プラグインの構成に関する注意事項」を参照してください。

Google Cloud Platform プラグインの構成に関する注意事項

Google Cloud Platform プラグインを使用すると、Google Cloud が存在するすべてのリージョンのディスクおよびホストベースのスナップショットを作成、削除、リストアできます。

NetBackup Snapshot Manager は、次の GCP リージョンをサポートします。

表 **5-5** NetBackup Snapshot Manager でサポートされる GCP リージョン

GCP リージョン
■ africa-south1
■ asia-east1 ■ asia-east2 ■ asia-northeast1 ■ asia-northeast2 ■ asia-south1 ■ asia-southeast1
■ australia-southeast1
■ europe-north1 ■ europe-north2 ■ europe-west1 ■ europe-west2 ■ europe-west3 ■ europe-west4 ■ europe-west6 ■ europe-west10
■ northamerica-northeast1 ■ southamerica-east1
■ us-central1 ■ us-east1 ■ us-east4 ■ us-west1 ■ us-west2 ■ us-west3- Utah ■ us-west4 Nevada ■ us-east5 (Columbus) ■ us-south1(Dallas)

GCP リージョン
■ asia-south ■ australia-southeast2 ■ europe-central2 ■ europe-west12 (Turin) ■ northamerica-northeast2 ■ northamerica-south1 ■ southamerica-west1 ■ me-west1 (Tel Aviv) ■ me-central1 (Doha) ■ me-central2 (Dammam)

メモ: マルチリージョン暗号化キーを一覧表示して使用する場合、サポート対象の GCP リージョン/ロケーションのオプションは、global、us、europe、asia です。

NetBackup Snapshot Manager での Google Cloud Platform プラグインの構成

Google Cloud Platform プラグインは、サービスアカウントまたはクレデンシャルを使用して、NetBackup Snapshot Manager で構成できます。

サービスアカウント構成の場合

- [プロジェクト ID (Project ID)]パラメータは、NetBackup Snapshot Manager がインストールされているプロジェクト以外のプロジェクトの構成に必要です。
  プロジェクト ID: リソースの管理元であるプロジェクトの ID。JSON ファイルには `project_id` として記載されています。
- プラグインを実行する[地域 (Region)]を指定します。
- [保存 (Save)]をクリックします。

クレデンシャルの構成の場合

- [クレデンシャル形式 (Credential type)]として[クレデンシャル (Credential)]を選択し、次のパラメータの値を指定します。

NetBackup Snapshot Manager の構成パラメータ	Google の同等の用語と説明
プロジェクト ID (Project ID)	リソースの管理元であるプロジェクトの ID。`project_id` として JSON ファイルに記載されています。
クライアントの電子メール (Client Email)	クライアント ID の電子メールアドレス。`client_email` として JSON ファイルに記載されています。

NetBackup Snapshot Manager の構成パラメータ	Google の同等の用語と説明
秘密鍵 (Private Key)	秘密鍵。JSON ファイルには `private_key` として記載されています。 **メモ:** このキーは引用符なしで入力する必要があります (一重引用符も二重引用符も利用不可)。鍵の先頭または末尾にスペースや改行文字を入力しないでください。

- プラグインを実行する[地域 (Region)]を指定します。
- [保存 (Save)]をクリックします。

複数のアカウント、サブスクリプション、またはプロジェクトの構成

- 同じプラグインに対して複数の構成を作成する場合は、それらが異なるリージョンの資産を管理していることを確認します。2 つ以上のプラグイン構成で、クラウド資産の同じセットを同時に管理しないようにする必要があります。
- 複数のアカウントが 1 台の NetBackup Snapshot Manager ですべて管理されている場合、単一の NetBackup Snapshot Manager インスタンスで管理する資産の数が多くなりすぎるため、分散したほうがよい場合があります。
- アプリケーションの整合性スナップショットを実現するには、リモート VM インスタンスと NetBackup Snapshot Manager との間で、オンホストエージェントのネットワーク接続が必要です。

GCP プラグインの考慮事項および制限事項

このプラグインを構成する前に、次の点を考慮します。

- GCP プラグイン構成からリージョンを削除すると、そのリージョンから検出されたすべての資産も、NetBackup Snapshot Manager 資産データベースから削除されます。削除された資産に関連付けられているアクティブなスナップショットがある場合、それらのスナップショットに対して操作を実行できないことがあります。
  このリージョンをプラグイン構成に再び追加すると、NetBackup Snapshot Manager ですべての資産が再度検出され、関連付けられているスナップショットの操作を再開できます。ただし、関連付けられたスナップショットに対してはいずれのリストア操作も実行できません。
- 検出中に権限が見つからない例外: デフォルトでは、新しい GCP プロバイダプラグイン構成を追加するときに、GCP クラウド関連の操作に対して権限チェックは行われません。GCP プロバイダプラグインの構成中に権限チェックを有効にするには、`flexsnap.conf` ファイルの GCP セクションに skip_permissions_check = "no" パラメータを追加します。

- GCP インスタンスのアタッチメントポイントの最大値は 128 で、NetBackup Snapshot Manager ホストはそのうち 2 つを使用し、残りの 126 がバックアップ/リストアジョブ用になります。つまり NetBackup Snapshot Manager は、126 のアタッチメントポイントが利用可能な間は、いつでもインスタンスをバックアップまたはリストアできます。アタッチメントポイントが枯渇すると、バックアップジョブまたはリストアジョブは失敗するようになり、次のエラーメッセージが表示されます。

  ```
  Failed to attach disk.
  ```

- GCP インスタンスにアタッチできるラベルの最大数は 64 で、NetBackup Snapshot Manager が 2 つ使用します。ラベルが 62 を超えるインスタンスがある場合、バックアップまたはリストアが失敗することがあります。
- リージョンが同じか重複していてクレデンシャルの種類が異なるサービスアカウントベースの GCP プロバイダプラグイン構成の再構成はサポートされません。

p.159 の「NetBackup Snapshot Manager で必要な Google Cloud Platform アクセス権」を参照してください。

p.169 の「NetBackup Snapshot Manager の GCP サービスアカウントの構成」を参照してください。

p.167 の「プラグイン構成のための GCP サービスアカウントの準備」を参照してください。

クレデンシャルとサービスアカウントオプションを使用して GCP プラグインを構成するための前提条件

- Google Cloud Platform プラグインを構成する前に、Google Cloud コンソールの［APIs & Services］で次の API を有効にします。
  - Cloud Resource Manager API
  - Compute Engine API
  - Cloud KMS (Key Management Service) API
  - Google OAuth2 API
- Kubernetes クラスタ拡張機能の構成時に提供されるノードプールには、同じリージョンのすべてのノードが必要です。つまり、ノードプールは単一ゾーンである必要があります。
- NetBackup Snapshot Manager ホストとノードプールのリージョンは同じである必要があります。
- スナップショットからバックアップする使用例では、NetBackup Snapshot Manager はクラウドにのみインストールする必要があります。NetBackup Snapshot Manager がインストールされているリージョンにプロバイダを構成する必要があります。NetBackup Snapshot Manager が us-west1-b ゾーンにインストールされている場合は、us-west1-b リージョンのプロバイダを構成する必要があります。

- NetBackup Snapshot Manager を手動インストールする (Marketplace 以外) 場合、LVM の LV の自動アクティブ化を無効にします。これは、auto_activation_volume_list パラメータを空のリストまたは自動アクティブ化する必要がある特定のボリュームグループ名のリストに設定して実現できます。auto_activation_volume_list パラメータは `lvm.conf` 設定ファイルで設定できます。

サービスアカウントオプションを使用して GCP プラグインを構成するための追加の前提条件

(サービスアカウントを使用して GCP プラグインを構成する場合にのみ該当) 次の操作を実行していることを確認します。

- [API and Identity Management]を変更するには、GCP 仮想マシンが[STOP]状態である必要があります。
- [API and Identity Management]を使用して必要なサービスアカウントを接続します。サービスアカウントには GCP プラグインを構成するために必要なプラグイン権限が必要です。
- NetBackup Snapshot Manager 仮想マシンに、[Set access for each API]を使用して、次の API アクセススコープを付与する必要があります。
  - サービス制御: 有効
  - サービス管理: 読み取り書き込み
  - クラウドプラットフォーム: 有効
  - 計算エンジン: 読み取り書き込み

メモ: API アクセススコープの変更が利用できない場合は、自動的に[Allow full access to all Cloud APIs]を設定する必要があります。

NetBackup Snapshot Manager で必要な Google Cloud Platform アクセス権

NetBackup Snapshot Manager が GCP (Google Cloud Platform) の資産にアクセスするために使用するサービスアカウントに次のアクセス権を割り当てます。

メモ: 次の表では、アスタリスク (*) が付いた権限は必須です。

表 **5-6** NetBackup Snapshot Manager の機能と GCP クラウドプロバイダの権限

機能	タスク/操作	必要な権限:
VM ベース		

機能	タスク/操作		必要な権限:
VM の保護	バックアップ、リストア、インデックス付け + GRT *	指定したディスク形式をフェッチします	compute.diskTypes.get
		指定した永続ディスクを削除します	compute.disks.delete
		ディスクをインスタンスに接続するときに使用します。	compute.disks.use
		既存のディスクリソースをインスタンスに接続します	compute.instances.attachDisk
		インスタンスからディスクを切断します	compute.instances.detachDisk
	クロスプロジェクトリストア	指定したプロジェクトで永続的なディスクを作成します	compute.disks.create
	スナップショット/ (クロスプロジェクト/リージョン) リストア *	指定したプロジェクトでスナップショットを作成します	compute.snapshots.create
		指定したスナップショットリソースを削除します	compute.snapshots.delete
	リストア/バックアップ/スナップショット/インデックス付け + GRT *	ディスクのラベルを設定します	compute.disks.setLabels
		指定したスナップショットリソースを返します	compute.snapshots.get
		指定したゾーン固有の操作リソースを取得します	compute.zoneOperations.get
	スナップショット、(クロスプロジェクト/クロスリージョン) リストア *	指定した永続ディスクのスナップショットを作成します	compute.disks.createSnapshot
	スナップショット/バックアップ/リストア *	指定した操作のリソースを取得します	compute.globalOperations.get
	クロスプロジェクトリストア、BFS *	同じまたは異なるプロジェクトのスナップショットからディスクを作成します	compute.snapshots.useReadOnly
			compute.networks.getEffectiveFirewalls

機能	タスク/操作		必要な権限:
	共有 VPC の構成*	特定のネットワークの有効なファイアウォールをフェッチします	
		指定したプロジェクトで利用可能なネットワークのリストを取得します	compute.networks.list
		指定したプロジェクトリソースを返します	compute.projects.get
		指定したサブネットワークを返します	compute.subnetworks.get
		指定したプロジェクトで利用可能なサブネットワークのリストを取得します	compute.subnetworks.list
		サブネットを使用してリソースを作成します	compute.subnetworks.use
		外部 IP を使用してリソースを作成します	compute.subnetworks.useExternalIp
		指定した名前で識別されるプロジェクトを取得します	resourcemanager.projects.get
		指定したファイアウォールを返します	compute.firewalls.get
	スナップショット *	スナップショットのラベルを設定します	compute.snapshots.setLabels
	プラグインの構成 *	指定したリージョンのリソースを返します	compute.regions.get
	CP 機能の計算、リストア *	指定したマシン形式を返します	compute.machineTypes.get
		指定したプロジェクトで利用可能なマシンの種類の一覧を取得します	compute.machineTypes.list
	検出 *	指定した永続ディスクをフェッチします	compute.disks.get
		指定したゾーン内に含まれる永続的なディスクのリストを取得します	compute.disks.list

機能	タスク/操作		必要な権限:
		指定されたインスタンスのリソースをフェッチします	compute.instances.get
		指定したゾーン内に含まれるインスタンスのリストを取得します	compute.instances.list
		Google Compute Engine のスナップショットを一覧表示します	compute.snapshots.list
	リストア *	指定したプロジェクトでインスタンスのリソースを作成します	compute.instances.create
		指定されたインスタンスのリソースを削除します	compute.instances.delete
		指定したインスタンスのメタデータを設定します	compute.instances.setMetadata
		インスタンスのサービスアカウントを設定します	compute.instances.setServiceAccount
		インスタンスのラベルを設定します	compute.instances.setLabels
		指定したインスタンスのネットワークタグを設定します	compute.instances.setTags
		Compute Engine インスタンスを起動します	compute.instances.start
		実行中のインスタンスを停止するために、正常にシャットダウンします	compute.instances.stop
		指定したネットワークを返します	compute.networks.get
		サービスアカウントをリソースに接続します	iam.serviceAccounts.actAs

機能	タスク/操作		必要な権限:
CMK 暗号化ディスクのリストア	リストア	特定の CryptoKey とそのプライマリ CryptoKeyVersion のメタデータを取得します	cloudkms.cryptoKeys.get
		特定の CryptoKeyVersion のメタデータを取得します	cloudkms.cryptoKeyVersions.get
		CryptoKey を一覧表示します	cloudkms.cryptoKeys.list
		KeyRing を一覧表示します	cloudkms.keyRings.list
		暗号化されたディスクの読み取り中にデータを復号します	cloudkms.cryptoKeyVersions.useToDecrypt
		リストアされたディスク上のデータを暗号化します	cloudkms.cryptoKeyVersions.useToEncrypt
		場所に関する情報を取得します	cloudkms.locations.get
		このサービスのサポート対象の場所に関する情報を一覧表示します	cloudkms.locations.list
	クロスプロジェクトリストア	他のプロジェクトのデータを暗号化または復号します	Cloud KMS CryptoKey Encrypter/Decrypter

機能	タスク/操作	必要な権限:
SQL データベースの保護	特定のプロジェクト内のクラウド SQL インスタンスを一覧表示します	cloudsql.instances.list
	データベースのリストを取得します	cloudsql.databases.list
	データベースの詳細を取得します	cloudsql.databases.get
	バックアップ用にデータベースからデータをエクスポートします	cloudsql.instances.export
	インスタンスの詳細を取得します	cloudsql.instances.get
	バックアップされたファイルをデータベースにインポートします	cloudsql.instances.import
	インスタンスのリストを取得します	cloudsql.instances.list
	バケットを作成します	storage.buckets.create
	バケットを取得します	storage.buckets.get
	必要なサービスアカウントのバケットに対する権限を取得します	storage.buckets.getIamPolicy
	必要なサービスアカウントのバケットに対する権限を設定します	storage.buckets.setIamPolicy
	バックアップファイルをバケットに保存します	storage.objects.create
	バケットからバックアップファイルをクリーンアップします	storage.objects.delete
	バケットからバックアップファイルの詳細を取得します	storage.objects.get
	バケットからファイルのリストを取得します	storage.objects.list

機能	タスク/操作	必要な権限:
PaaS 作業負荷の保護 (GCP BigQuery)	構成についての詳細を取得します	bigquery.config.get
	新しい空のデータセットを作成します	bigquery.datasets.create
	データセットを削除します	bigquery.datasets.delete
	データセットに関するメタデータと権限を取得します	bigquery.datasets.get
	GCP コンソールでのメタデータ表示権限	bigquery.datasets.getIamPolicy
	プロジェクト内でジョブ (クエリーを含む) を実行します	bigquery.jobs.create
	任意のジョブのデータとメタデータを取得します	bigquery.jobs.get
	すべてのジョブを一覧表示し、任意のユーザーが送信したジョブのメタデータを取得します。他のユーザーが送信したジョブの場合は、詳細とメタデータが編集されます。	bigquery.jobs.list
	すべてのジョブを一覧表示し、任意のユーザーが送信したジョブのメタデータを取得します	bigquery.jobs.listAll
	ジョブを取り消します	bigquery.jobs.update
	ルーチンの定義とメタデータを取得します	bigquery.routines.get
	ルーチンとルーチンのメタデータを一覧表示します	bigquery.routines.list
	新しいテーブルを作成します	bigquery.tables.create
	新しいテーブルスナップショットを作成します	bigquery.tables.createSnapshot
	テーブルを削除します	bigquery.tables.delete
	テーブルスナップショットを削除します	bigquery.tables.deleteSnapshot
	BigQuery からテーブルデータをエクスポートします	bigquery.tables.export
	テーブルメタデータを取得します	bigquery.tables.get
	テーブルデータを取得します	bigquery.tables.getData
	テーブルとテーブルのメタデータを一覧表示します	bigquery.tables.list

機能	タスク/操作	必要な権限:
	テーブルのメタデータを更新します	bigquery.tables.update
	テーブルデータを更新します	bigquery.tables.updateData
	プロジェクトで新しいバケットを作成します	storage.buckets.create
	バケットのメタデータを IAM ポリシーを除いて読み取り、バケットの Pub/Sub 通知構成を一覧表示または読み取ります。	storage.buckets.get
	バケットの IAM ポリシーを読み取ります	storage.buckets.getIamPolicy
	バケットの IAM ポリシーを更新します	storage.buckets.setIamPolicy
	バケットに新しいオブジェクトを追加します	storage.objects.create
	オブジェクトを削除します	storage.objects.delete
	ACL を除くオブジェクトデータとメタデータを読み取ります。	storage.objects.get
	バケット内のオブジェクトを一覧表示します。また、一覧表示する時に ACL を除くオブジェクトメタデータを読み取ります。	storage.objects.list
Kubernetes クラスタベース		
Kubernetes 拡張機能/自動スケーリング	クラスタの情報を取得します	container.clusters.get
	管理対象インスタンスグループに関する詳細を取得します	compute.instanceGroupManagers.get
Kubernetes 拡張機能/自動スケーリング	管理対象インスタンスグループを更新します	compute.instanceGroupManagers.update
Kubernetes 拡張機能/自動スケーリング	クラスタのノードプールを更新します	container.clusters.update
	GKE クラスタで実行した操作を管理します	container.operations.get

プラグイン構成のための GCP サービスアカウントの準備

NetBackup Snapshot Manager GCP プラグイン構成の準備をするには

1 NetBackup Snapshot Manager で必要な GCP 構成パラメータを収集します。

p.154 の「Google Cloud Platform プラグインの構成に関する注意事項」を参照してください。

次の手順を実行します。

- Google Cloud コンソールから、[IAM & 管理 (IAM & admin)]、[サービスアカウント (Service accounts)]の順に移動します。
- 割り当てられたサービスアカウントをクリックします。右側の 3 つの縦のボタンをクリックし、[キーの作成 (Create key)]を選択します。
- [JSON]を選択し、[作成 (CREATE)]をクリックします。
- ダイアログボックスでクリックしてファイルを保存します。このファイルには、Google Cloud プラグインを構成するために必要なパラメータが含まれています。次に、コンテキスト内の各パラメータを示す JSON ファイルの例を示します。
  `private-key` は、読みやすくするために切り詰められています。

```
{
  "type": "service_account",
  "project_id": "some-product",
  "private_key": "-----BEGIN PRIVATE KEY-----¥n
N11EvA18ADAN89kq4k199w08AQEFAA5C8KYw9951A9EAAo18AQCnvpuJ3oK974z4¥n
.
.
.
weT9odE4ryl81tNU¥nV3q1XNX4fK55QTpd6CNu+f7QjEw5x8+5ft05DU8ayQcNkX¥n
4pXJoDol54N52+T4qV4WkoFD5uL4NLPz5wxf1y¥nNWcNfru8K8a2q1/9o0U+99==¥n
-----END PRIVATE KEY-----¥n",
  "client_email": "email@xyz-product.iam.gserviceaccount.com",

  "auth_uri": "https://accounts.google.com/o/oauth2/auth",
  "token_uri": "https://accounts.google.com/o/oauth2/token",
  "auth_provider_x509_cert_url": "https://www.googleapis.com
¥
   /oauth2/v1/certs",
  "client_x509_cert_url": "https://www.googleapis.com/robot/v1
 ¥
   /metadata/x509/ email%40xyz-product.iam.gserviceaccount.com"
}
```

2 テキストエディタを使用して、NetBackup Snapshot Manager ユーザーインターフェースに入力できるように、`private_key` を再フォーマットします。作成したファイルを検索すると、秘密鍵の各行は `¥n` で終了します。`¥n` の各インスタンスを実際の改行で置き換える必要があります。次のいずれかを実行します。

- UNIX 管理者の場合は、vi で次のコマンドを入力します。次の例で、^ は Ctrl キーを示します。コマンドラインには ^M のみ表示されることに注意してください。

  :g/¥¥n/s//^V^M/g

- Windows 管理者は、ワードパッドまたは同様のエディタを使用して、¥n で各インスタンスを検索して手動で置換します。

3 NetBackup ユーザーインターフェースからプラグインを構成する場合は、再フォーマットされた秘密鍵をコピーして[秘密鍵 (Private Key)]フィールドに貼り付けます。再フォーマットされた private_key は次のようになります。

```
-----BEGIN PRIVATE KEY-----¥
N11EvA18ADAN89kq4k199w08AQEFAA5C8KYw9951A9EAAo18AQCnvpuJ3oK974z4
.
.
.
weT9odE4ryl81tNU¥nV3q1XNX4fK55QTpd6CNu+f7QjEw5x8+5ft05DU8ayQcNkX
4pXJoDol54N52+T4qV4WkoFD5uL4NLPz5wxf1y¥nNWcNfru8K8a2q1/9o0U+99==
-----END PRIVATE KEY-----
```

NetBackup Snapshot Manager の GCP サービスアカウントの構成

GCP (Google Cloud Platform) で資産を保護するには、これらのクラウド資産にアクセスして操作を実行できるアクセス権が NetBackup Snapshot Manager に必要です。カスタムロールを作成し、NetBackup Snapshot Manager で必要な最小限のアクセス権を付けて割り当てる必要があります。その後、NetBackup Snapshot Manager 用に作成したサービスアカウントにそのカスタムロールを関連付けます。

次の手順を実行します。

1 GCP でカスタム IAM ロールを作成します。ロールを作成するときに、NetBackup Snapshot Manager で必要なすべてのアクセス権を追加します。

p.159 の「NetBackup Snapshot Manager で必要な Google Cloud Platform アクセス権」を参照してください。

カスタムロールの作成と管理について詳しくは、Google のマニュアルの「カスタムロールの作成と管理」セクションを参照してください。

2 GCP でサービスアカウントを作成します。

サービスアカウントに次のロールを付与します。

- 前の手順で作成したカスタムの IAM ロール。これは、GCP リソースにアクセスするために NetBackup Snapshot Manager で必要なすべてのアクセス権を持つロールです。

- `iam.serviceAccountUser` ロール。これにより、サービスアカウントのコンテキストを使用して、サービスアカウントが GCP に接続できるようになります。

サービスアカウントの作成と管理について詳しくは、Google のマニュアルの「サービスアカウントの作成と管理」セクションを参照してください。

GCP クロスプロジェクト構成

メモ: NetBackup Snapshot Manager のゾーンと、拡張機能のノードプールは同じである必要があります。

クロスプロジェクト操作の場合は、NetBackup Snapshot Manager がインストールされているリージョンにプロバイダを構成する必要があります。NetBackup Snapshot Manager が us-west1-b ゾーンにインストールされている場合は、us-west1-b リージョンのプロバイダを構成する必要があります。

NetBackup Snapshot Manager をインストールした最初のプロジェクトの詳細が次のような内容だとします。

- Service-account = cp-host-service-account
- Project-name = cp-host-project

2 番目のプロジェクトの詳細が次にような内容だとします。

- Service-account = other-service-account
- Project-name = other-project

GCP クロスプロジェクト構成を使用して VM をバックアップおよびリストアするには

1. 次の権限を使用して、other-project にクロスプロジェクトの役割を作成します。
   - `compute.snapshots.useReadOnly`
   - `compute.disks.create`
   - `Cloud KMS CryptoKey Encrypter/Decrypter`
2. 上の役割を other-project プロジェクトの cp-host-service-account に割り当てます。

GCP 共有 VPC 構成

共有 VPC 構成では、カスタム共有 VPC ロールを NetBackup Snapshot Manager プロバイダ構成で使用されるサービスアカウントに割り当てる必要があります。

たとえば、GCP 共有 VPC 構成を使用して VM をリストアするための共有 VPC ネットワークを一覧表示するには、以下の詳細を検討します。

- NetBackup Snapshot Manager プロバイダ構成サービスアカウントの場合: nbsm-service-account
- 共有 VPC プロジェクト名: shared-vpc-project

GCP 共有 VPC 構成を使用して VM をリストアするための共有 VPC ネットワークを一覧表示するには

1. 次の権限を使用して、shared-vpc-project に共有 VPC ロールを作成します。
   - `compute.networks.getEffectiveFirewalls`
   - `compute.networks.list`
   - `compute.projects.get`
   - `compute.subnetworks.get`
   - `compute.subnetworks.list`
   - `compute.subnetworks.use`
   - `compute.subnetworks.useExternalIp`
   - `resourcemanager.projects.get`
   - `compute.firewalls.get`
2. 上の役割を shared-vpc-project プロジェクトの nbsm-service-account に割り当てます。

Microsoft Azure プラグインの構成に関する注意事項

Microsoft Azure プラグインでは、仮想マシンレベルと管理対象ディスクレベルでスナップショットを作成、削除、リストアできます。

複数のネットワークインターフェース (NIC) のリストアのサポート

NetBackup では、Azure 上の VM に接続されているすべての NIC と静的 IP アドレスのリストアがサポートされています。サポートされるシナリオにおける特定の動作を次に示します。

- プライベート IP アドレスでは、次の割り当て方法を使用できます。
  静的: IP アドレスが静的に割り当てられている場合、完全なプライベート IP アドレスがリストアされます。
  動的: IP アドレスが動的に割り当てられている場合、動的 IP アドレスが NIC に割り当てられ、完全な IP アドレスは適用されません。
- パブリック IP アドレスの場合、使用する割り当て方法に関係なく、パブリック IP リソースに関連付けられる実際のパブリック IP アドレスを指定することはできません。

そのため、パブリック IP リソースが作成され、関連する NIC に関連付けられます。パブリック IP リソースの他のプロパティは、バックアップ時と同じままです。

ADE (Azure ディスク暗号化) が有効な VM のサポート

NetBackup は、Azure ディスク暗号化 VM のサポートを提供します。ADE が有効な VM は、Web UI の資産の詳細で Azure ディスク暗号化のフラグが True として表示されます。次のシナリオがサポートされます。

- ロールバックリストア
- VM のスナップショットおよびバックアップからのスナップショット作成、バックアップ、およびリストア。
- スナップショットの作成時に Azure ディスク暗号化拡張機能が存在する場合、VM がスナップショットからリストアされた後は、拡張機能のみが存在します。
- サポート対象のオペレーティングシステム:
  Linux VM の場合: サポート対象の VM とオペレーティングシステム
  Windows の場合: サポート対象の VM とオペレーティングシステム

NetBackup Snapshot Manager でのプライベートディスクアクセスのサポート

NetBackup Snapshot Manager は、ディスクアクセスオブジェクトを使用したプライベートディスクアクセスが可能なディスクをサポートします。プライベートディスクアクセスを保護するときは、次の点を考慮してください。

- スナップショットからのバックアップをサポートするには、VM の Azure 管理対象ディスクでパブリックまたはプライベートのディスクアクセスが有効になっている必要があります。
  - Azure は、スナップショット操作中に作成された VM リストアポイントに同じ設定を伝播します。
  - その後、VM リストアポイントのディスクスナップショットに SAS URI を使用して、スナップショットの内容が安全に読み取られます。
  - プライベートディスクアクセスがディスクアクセスオブジェクトと、関連するプライベートエンドポイントを使用して設定されている場合、Azure の制限により、ディスクアクセスオブジェクトあたり 5 つより多くディスクとスナップショットをエクスポートすることはできません。そのため、2 つを超えるディスクが同じディスクアクセスオブジェクトを共有しないようにします。そうしないと、スナップショットからのバックアップは次のエラーで失敗します。

    ```
    (DiskAccessObjectHasTooManyActiveSASes) Too many simultaneous
    imports or exports using disk access object. The current cap
    is 5. Revoke some active access tokens before creating more
    access requests
    ```

- この機能により、ユーザーはプライベートディスクアクセスが有効になっているディスクのスナップショット作成とリストアを実行できます。リストアされたディスクには、同じディスクアクセスオブジェクトの関連付けも行われます。
- ユーザーは、プライベートディスクアクセスを持つ VM のスナップショット作成、バックアップ、リストアを実行できます。リストアされた VM には、同じディスクアクセスオブジェクトを使用して有効化されたプライベートディスクを持つディスクも含まれます。プライベートディスクアクセスを持つ VM をスナップショットまたはバックアップコピーを使用してリストアする場合は、ディスクアクセスオブジェクトあたりのディスク数が増加して、ディスクアクセスオブジェクトあたりディスク 5 つの前提条件に従っていない可能性があることを確認します。ユーザーはリストアされた VM を保護するために適切な処理を実行する必要があります。
- バックアップコピーからのクロスサブスクリプションリストアまたはクロスリージョンリストアの場合、または元の VM に存在していたディスクアクセスオブジェクトが削除された場合、リストアされた VM のディスクのパブリックアクセスとプライベートアクセスは無効になります。クライアントは、要件に従って既存または新しく作成されたディスクアクセスオブジェクトを割り当てる必要があります。
- NetBackup Snapshot Manager が 1 つのサブスクリプションに含まれていて、保護対象の VM が異なるサブスクリプションにある場合は、Snapshot Manager サブスクリプション内に作成された適切なプライベートエンドポイントをディスクアクセスオブジェクトに関連付ける必要があります。

Azure リカバリポイントを使用したアプリケーション整合性のサポート

デフォルトでは、Snapshot Manager のスナップショット作成操作では、スナップショットの代わりにリカバリポイントが作成されます。スナップショットがアプリケーション整合になるように Azure リカバリポイントを使用するには、次の表を参照して Azure クラウドで VM に接続して構成します。

Windows の場合	Linux の場合
VM に接続して構成する必要はありません。	■ Linux の場合: デフォルトでは、スナップショットは Azure でファイルシステム整合性を持ちます。 ■ Linux 上の Oracle の場合: ■ VM が接続状態である必要があります。 または ■ アプリケーションの整合性を保つための事前スクリプトまたはポストスクリプトは、「Azure Linux VM のアプリケーション整合性バックアップ」の説明に記載されているとおりに Linux VM 用に構成する必要があります。

メモ: スナップショットを作成およびリストアしている間に、Azure で作成されるスナップショットの代わりにリストアポイントが作成されます。

スナップショットの作成

- Snapshot Manager では、VM に対して最初のスナップショットが作成されると、VM リストアポイントを使用してリストアポイントコレクションが作成されます。
- 各 VM リストアポイントには、VM スナップショット操作でスナップショットが作成されたすべてのディスクのディスクリストアポイントが含まれます。
- VM で取得された各スナップショットは、最初のスナップショットが取得されたときに作成されたリストアポイントコレクションの Azure に保存されます。
- 後続のリストアポイントは増分バックアップです。

スナップショットのリストア

- Snapshot Manager バージョン 10.2 より前のバージョンで取得したスナップショットの場合、スナップショットは Azure のスナップショットからリストアされます。
- Snapshot Manager バージョン 10.2 で取得したスナップショットの場合、スナップショットはリストアポイントからリストアされます。

次の点に注意してください。

- リストアポイントを見つけます。
  次のように、NetBackup で、作成されたスナップショットのジョブの詳細でスナップショット ID を取得します。

  ```
  Snapshot ID: azure-snapvmrp-<subscription name>+<RG name>+<restore
   point collection name>+<restore point>
  ```

  リストアポイントを見つけるには、Azure ポータルで［Subscription］、［Resource Group (RG)］、［Restore Point Collection (RPC)］、［Restore Point］の順に選択します。
- ログを見つけます。
  - Snapshot Manager: `/cloudpoint/flexsnap.log`
  - ホスト VM:
    - Linux:
      `/var/log/azure/Microsoft.Azure.RecoveryServices.VMSnapshotLinux/extension.log`
    - Windows の場合:
      `C:¥WindowsAzure¥Logs¥Plugins¥Microsoft.Azure.RecoveryServices.VMSnapshot¥<version>`

前提条件

Azure プラグインを構成する前に、次の準備手順を完了します。

- (ユーザーがアプリケーションサービスプリンシパルルートを続行する場合のみ適用) Azure プラグインの AAD (Azure Active Directory) アプリケーションを作成するには、Microsoft Azure ポータルを使用します。
- リソースにアクセスするために必要な権限を役割に割り当てます。

NetBackup Snapshot Manager で必要とされる Azure プラグインの権限について詳しくは、「p.179 の「Microsoft Azure でのアクセス権の設定」を参照してください。」を参照してください

Azure では、次のいずれかの方法でリソースに権限を割り当てることができます。

- サービスプリンシパル: この権限は、ユーザー、グループ、またはアプリケーションに割り当てることができます。
- マネージド ID: マネージド ID により、Azure Active Directory (Azure AD) 認証をサポートするリソースに接続するときに使用される、Azure Active Directory で自動的に管理される ID がアプリケーションに提供されます。マネージド ID には次の 2 種類があります。
  - システム割り当て
  - ユーザー割り当て

詳しくは、Azure のマニュアルにある手順に従ってください。

表 5-7 Microsoft Azure プラグインの構成パラメータ

NetBackup Snapshot Manager の構成パラメータ	Microsoft 製品の同等の用語と説明
クレデンシャルの種類: アプリケーションサービスプリンシパル **メモ:** アプリケーションサービスプリンシパルに役割を割り当てます。	
テナント ID (Tenant ID)	アプリケーションを作成した Azure AD ディレクトリの ID。
クライアント ID (Client ID)	アプリケーション ID。
シークレットキー (Secret Key)	アプリケーションのシークレットキー。
クレデンシャルの種類: システム管理 ID **メモ:** システム管理 ID に役割を割り当てます。	
Azure の NetBackup Snapshot Manager ホストでシステム管理 ID を有効にします。	
クレデンシャルの種類: ユーザー管理 ID **メモ:** ユーザー管理 ID に役割を割り当てます。	
クライアント ID (Client ID)	NetBackup Snapshot Manager ホストに接続されているユーザー管理 ID のクライアント ID。

NetBackup Snapshot Manager の構成パラメータ	Microsoft 製品の同等の用語と説明
次のパラメータは、上記のすべてのクレデンシャルタイプに適用されます。	
リージョン (Regions)	クラウド資産を検出する 1 つ以上の地域。 **メモ:** 行政クラウドを設定する場合は、US Gov アリゾナ、US Gov テキサス、または US Gov バージニアを選択します。
リソースグループの接頭辞 (Resource Group prefix)	資産用に作成されたスナップショットを、資産が存在するリソースグループとは別のリソースグループに格納するために使用される接頭辞。 たとえば、NetBackup Snapshot Manager にある資産とリソースグループの接頭辞が snap の場合、NetBackup Snapshot Manager リソースグループにある資産のスナップショットは、snapNetBackup Snapshot Manager リソースグループに格納されます。
接頭辞が付いたリソースグループが見つからない場合でも資産を保護 (Protect assets even if prefixed Resource Groups are not found)	このチェックボックスにチェックマークを付けると、リソースグループが存在しない場合に NetBackup Snapshot Manager ではスナップショット操作が失敗しません。元のリソースグループにスナップショットを格納しようとします。 **メモ:** 接頭辞が付いたリソースグループのリージョンは、元のリソースグループのリージョンと同じである必要があります。

複数のアカウント、サブスクリプション、またはプロジェクトの構成

- 同じプラグインに対して複数の構成を作成する場合は、それらが異なるサブスクリプションの資産を管理していることを確認します。2 つ以上のプラグイン構成で、クラウド資産の同じセットを同時に管理しないようにする必要があります。
- 複数のアカウントが 1 台の NetBackup Snapshot Manager サーバーですべて管理されている場合、単一の NetBackup Snapshot Manager インスタンスによって管理される資産の数が多くなることがあります。したがって、負荷分散の改善のため、資産を複数の NetBackup Snapshot Manager サーバーに分離させたほうがよい場合があります。
- アプリケーションの整合性スナップショットを実現するには、リモート VM インスタンスと NetBackup Snapshot Manager サーバーとの間で、エージェントまたはエージェントレスのネットワーク接続が必要です。これには、アカウント、サブスクリプション、およびプロジェクト間のネットワークを設定する必要があります。

Azure プラグインの考慮事項および制限事項

Azure プラグインを構成する前に、次の点を考慮します。

- プラグインの現在のリリースでは、BLOB のスナップショットはサポートされていません。

- NetBackup Snapshot Manager では、現在、管理対象ディスクによってバックアップされた、Azure 管理対象ディスクと仮想マシンのスナップショットの作成とリストアのみをサポートしています。
- 同じプラグインに対して複数の構成を作成する場合は、それらが異なるテナント ID の資産を管理していることを確認します。2 つ以上のプラグイン構成で、クラウド資産の同じセットを同時に管理しないようにする必要があります。
- スナップショットを作成するときに、Azure プラグインは各スナップショットに Azure 固有のロックオブジェクトを作成します。スナップショットは、Azure コンソールから、または Azure CLI または API 呼び出しからの予期しない削除を防ぐためにロックされます。ロックオブジェクトは、スナップショットと同じ名前になります。また、ロックオブジェクトには、スナップショットが属する、対応する VM または資産の ID が含まれる「notes」という名前のフィールドも含まれています。
  スナップショットロックオブジェクトの notes フィールドが変更または削除されていないことを確認してください。変更または削除されていると、対応する元の資産からスナップショットの関連付けが解除されます。
  Azure プラグインは、ロックオブジェクトの notes フィールドの ID を使用して、たとえば「元の場所」へのリストア操作の一環として、ソースディスクを置換または削除するインスタンスにスナップショットを関連付けます。
- Azure プラグインは次の GovCloud (US) 地域をサポートします。
  - US Gov アリゾナ
  - US Gov テキサス
  - US Gov バージニア
  - US Gov アイオワ
  - US DoD 中部
  - US DoD 東部
- Azure プラグインは次のインド地域をサポートします。
  - Jio India West
  - Jio India Central
- Azure プラグインの追加地域のサポート: イタリア北部、ポーランド中部、カタール中部、イスラエル中部、ニュージーランド北部 (アジア太平洋)、インドネシア中部 (ジャカルタ - インドネシア)、マレーシア西部 (クアラルンプール - マレーシア)
- NetBackup Snapshot Manager Azure プラグインは次の Azure リージョンをサポートしません。

場所	リージョン
米国	■ US DoD 中部 ■ US DoD 東部 ■ US Sec 西部
中国 NetBackup Snapshot Manager は、中国のどのリージョンもサポートしていません。	■ 中国東部 ■ 中国東部 2 ■ 中国北部 ■ 中国北部 2
ドイツ	■ ドイツ中部 (ソブリン) ■ ドイツ北東部 (ソブリン)

- NetBackup Snapshot Manager は Microsoft Azure 第 2 世代の仮想マシンもサポートします。
- NetBackup Snapshot Manager は、ストレージプールから作成された仮想ディスクまたはストレージ領域を備えた Windows システムのアプリケーションの一貫したスナップショットと個別ファイルのリストアをサポートしません。Microsoft SQL Server のスナップショットジョブでストレージプールのディスクを使用すると、エラーが発生してジョブが失敗します。ただし、接続状態にある仮想マシンのスナップショットジョブがトリガされると、ジョブは正常に実行されることがあります。この場合、ファイルシステムの静止およびインデックス付けはスキップされます。このような個々のディスクを元の場所にリストアするジョブも失敗します。この状況では、ホストがリカバリ不可能な状態になる可能性があり、手動でのリカバリが必要になる場合があります。
- Snapshot Manager は、MariaDB サーバー用の Azure データベースのマネージド ID データベース認証をサポートしません。
- ADE (Azure Disk Encryption) が有効な VM のスナップショットについては、次の点を考慮します。
  - ADE が有効な VM でのインデックス付けはサポートされません。ユーザーが GRT を有効にした保護計画を持っている場合、ADE が有効な VM のこの保護計画へのサブスクライブは無効になります。
  - VM が GRT が有効な保護計画にサブスクライブされ、後で同じ VM で ADE を有効にすると、そのような VM のインデックス付けはエラー 9997 で失敗します。
  - ADE が有効な VM が GRT から成る保護計画にサブスクライブされているインテリジェントグループの一部である場合、ADE が有効な VM のインデックス付けはエラー 9997 で失敗します。
  - 非 ADE VM から ADE が有効な VM に対して単一ファイルリストアを実行できます。

- ユーザーが VM を別のリソースグループにリストアしようとしている場合は、Key Vault への適切なアクセス権を他のリソースグループに割り当てる必要があります。
- スナップショットとリストアは、ADE が有効な VM に配備されたアプリケーションではサポートされません
- Azure Disk Encryption が OS またはデータディスクに適用されている場合、暗号化形式 PMK を他の暗号化形式に変更することはできません。
- オペレーティングシステムのディスクが Azure Disk Encryption で暗号化され、PMK 以外で暗号化されたデータディスクを後から VM に接続した場合は、正常にリストアするためにデータディスクの暗号化を PMK に変更します。

- NetBackup Snapshot Manager がファイアウォールの背後で実行されている場合は、資産の検出が成功するように、ポート 443 で次のエンドポイントとメタデータ IP が許可されていることを確認します。
  - エンドポイント:
    *.management.azure.com
    *.login.microsoftonline.com
    *.storage.azure.net
    *.vault.azure.net
  - メタデータ IP: 169.254.169.254
  - NetBackup Snapshot Manager がプロキシ設定で構成されている場合は、次のセクションで詳細を参照してください。
    p.27 の「プロキシサーバーの要件」を参照してください。
- NetBackup バージョン 10.5.0.1 以降では、ADE が有効な VM のバックアップがサポートされますが、次の制限事項があります。
  すでに ADE で暗号化されている VM に追加のデータディスク (暗号化されていない) が追加されると、スナップショット作成とバックアップ操作は成功しますが、リストア後に追加の非 ADE ディスクのデータが失われるか、存在しなくなる場合があります。

  メモ: 現在回避方法はありません。対応する新しいディスクはリストアされた VM に存在しますが、それらにデータは存在しません。

Microsoft Azure でのアクセス権の設定

NetBackup Snapshot Manager で Microsoft Azure 資産を保護できるようにするには、事前に Microsoft Azure 資産へのアクセス権が必要です。NetBackup Snapshot Manager ユーザーが Azure 資産と連携するために使用できるカスタム役割を関連付ける必要があります。

次のことを NetBackup Snapshot Manager に可能にするカスタム役割の定義を、以下に JSON 形式で示します。

- Azure プラグインを構成し、資産を検出します。
- ホストとディスクのスナップショットを作成します。
- 元の場所または新しい場所にスナップショットをリストアします。
- スナップショットを削除します。

表 5-8 NetBackup Snapshot Manager の機能と Microsoft Azure クラウドプロバイダの権限

機能	タスク/操作	必要な権限:
VM ベース		
スナップショットからのバックアップ	スナップショットからのバックアップ用に共有アクセスシグネチャ URI を作成します。	`Microsoft.Storage/*/read`
	スナップショットからのバックアップ用に共有アクセスシグネチャ URI を生成します。	`Microsoft.Compute/restorePointCollections/restorePoints/retrieveSasUris/action`
	アクセス権を取得して、スナップショットからのバックアップでバックアップコピーを作成するために、ディスクリストアポイントから読み取ります。	`Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/beginGetAccess/action`
	スナップショットからのバックアップが正常に完了した後に、リストアポイントへのアクセス終了を取得します。	`Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/endGetAccess/action`
スナップショットからのバックアップ作成	スナップショットデータへのアクセス権を取得します。	`Microsoft.Compute/snapshots/beginGetAccess/action`
	スナップショットのデータがバックアップにコピーされた後に URI を終了します。	`Microsoft.Compute/snapshots/endGetAccess/action`

機能	タスク/操作	必要な権限:
スナップショットからのバックアップからのリストア	管理対象ディスクの共有アクセスシグネチャ URI を作成します。	Microsoft.Compute/disks/beginGetAccess/action
	スナップショットからのバックアップの後、共有アクセスシグネチャ URI を削除します。	Microsoft.Compute/disks/endGetAccess/action
仮想マシンの保護	VM、VM スケールセット、接続されたディスクを一覧表示します。	Microsoft.Compute/*/read
SQL データベースの保護	保護対象の Azure SQL データベースを一覧表示します。	Microsoft.Sql/*/read
スナップショットまたはリストアポイントからのディスクのリストア	リストア用のディスクを作成します。	Microsoft.Compute/disks/write
ロールバックリストア/リストアのクリーンアップ	ロールバックリストアで VM をリストアします。 または リストアワークフローでエラーが発生した場合にクリーンアップします。	Microsoft.Compute/virtualMachines/delete
ディスクのリストア	ディスクまたはファイルをリストアするために利用可能なディスクの接続ポイントを識別します。	Microsoft.Compute/virtualMachines/vmSizes/read

機能	タスク/操作	必要な権限:
クリーンアップ	リストアワークフローのクリーンアップでエラーが発生した場合に、パブリック IP を削除します。元の VM にパブリック IP があり、代替の場所へのリストアが失敗した場合。	Microsoft.Network/publicIPAddresses/delete
	スナップショットの作成ワークフローが失敗したためにロールバックした場合に、RPC を削除します。	Microsoft.Compute/restorePointCollections/delete
リソースの一覧表示 (検出)	リソースグループと場所の情報を取得します。	Microsoft.Resources/*/read
検出	保護対象の資産を一覧表示するために使用できるサブスクリプションを一覧表示します。	Microsoft.Subscription/*/read
スナップショットとリストア	タグが Snapshot Manager で作成されていることを示すために、タグをスナップショットに追加します VM に元々存在していたタグをリストアされた VM に追加します。	Microsoft.Resources/subscriptions/tagNames/tagValues/write Microsoft.Resources/subscriptions/tagNames/write
スナップショット	ディスクスナップショットを誤って削除しないように保護します。	Microsoft.Authorization/locks/*
リストアポイントの一覧表示	リストア用にスナップショット (リストアポイント) を一覧表示します。	Microsoft.Compute/restorePointCollections/read
スナップショットの一覧表示	VM のリストアポイントを一覧表示およびマッピングします。	Microsoft.Compute/restorePointCollections/restorePoints/read

機能	タスク/操作	必要な権限:
ディスクスナップショットの一覧表示	アプリケーションの一貫性を確保するために、ディスクのリストアポイントを一覧表示します。	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/read
スナップショットの書き込み	リストアポイントとしての増分スナップショット (アプリケーション整合)。	Microsoft.Compute/restorePointCollections/restorePoints/write
スナップショットのクリーンアップ	リストアエラーが発生した場合のクリーンアップ。	Microsoft.Compute/restorePointCollections/restorePoints/delete
リストアポイントコレクションの作成	VM に対してスナップショットがトリガされた場合に備えて VM ごとに 1 つの RPC を作成します。	Microsoft.Compute/restorePointCollections/write

機能	タスク/操作	必要な権限:
VM のリストア	リストアで VM を作成します。	Microsoft.Compute/virtualMachines/write
	保護計画で説明されているように、リストアされた VM の電源をオンにします。	Microsoft.Compute/virtualMachines/start/action
	インストールされている場合に ADE 拡張機能の詳細を取得します。	Microsoft.Compute/virtualMachines/extensions/read
	リストア時に ADE 拡張機能をインストールします。	Microsoft.Compute/virtualMachines/extensions/write
	VM の状態を変更します。ロールバックリストアのために VM を停止します。	Microsoft.Compute/virtualMachines/powerOff/action
	元のリソースと同じネットワーク、またはユーザーが選択したネットワークにリストアするために、ネットワークを一覧表示します。	Microsoft.Network/*/read
	カスタマ管理キーを一覧表示します。	Microsoft.KeyVault/vaults/keys/read
	リストアをロールバックします。ワークフローでエラーが発生した場合にクリーンアップします。	Microsoft.Network/networkInterfaces/delete
	リストアされた VM にネットワークインターフェースカードを接続します。	Microsoft.Network/networkInterfaces/join/action
	VM リストア用のネットワークインターフェースカードを作成します。	Microsoft.Network/networkInterfaces/write
	リストア時にネットワークセキュリティグループを VM に接続します。	Microsoft.Network/networkSecurityGroups/join/action
		Microsoft.Network/networkSecurityGroups/write

機能	タスク/操作	必要な権限:
	VM リストア用のネットワークセキュリティグループを作成します (元の VM にネットワークセキュリティグループが存在する場合)。	
	元の VM にパブリック IP がある場合にリストアでパブリック IP を接続します。	Microsoft.Network/publicIPAddresses/join/action
	元の VM にパブリック IP がある場合にリストアでパブリック IP を作成します。	Microsoft.Network/publicIPAddresses/write
	サブネット内に VM を作成します。つまり、サブネットを結合します。	Microsoft.Network/virtualNetworks/subnets/join/action
Kubernetes クラスタベース		
クラスタ情報の取得	クラスタ情報を取得します。	Microsoft.ContainerService/managedClusters/agentPools/read
スケールイン/スケールアウト	クラスタの機能を取得します。	Microsoft.ContainerService/managedClusters/read
スケールイン	VM スケールセットの状態を維持します。	Microsoft.Compute/virtualMachineScaleSets/delete/action
スケールアウト	VM スケールセットの状態を維持します。	Microsoft.Compute/virtualMachineScaleSets/write
マーケットプレイス配備		
高可用性	Snapshot Manager データディスクを VM スケールセットインスタンスに接続します。	Microsoft.Compute/virtualMachineScaleSets/write
	(スケールイン) VM スケールセットの状態を維持します。	Microsoft.Compute/virtualMachineScaleSets/delete/action

サポートされる PaaS データベースの検出、作成、削除、データベース認証および指定した時点へのリストア (Azure SQL と管理対象インスタンスデータベースのみに該当) に管理対象 ID を使用するには、次の権限セットが必要です。

```
actions": [
   "Microsoft.Authorization/*/read",
   "Microsoft.Subscription/*/read",
   "Microsoft.Resources/*/read",
   "Microsoft.ManagedIdentity/*/read",
   "Microsoft.Sql/*/read",
   "Microsoft.Sql/servers/databases/write",
   "Microsoft.Sql/servers/databases/delete",
   "Microsoft.Sql/managedInstances/databases/write",
   "Microsoft.Sql/managedInstances/databases/delete",
   "Microsoft.DBforMySQL/servers/read",
   "Microsoft.DBforMySQL/servers/databases/read",
   "Microsoft.DBforMySQL/flexibleServers/read",
   "Microsoft.DBforMySQL/flexibleServers/databases/read",
   "Microsoft.DBforMySQL/servers/databases/write",
   "Microsoft.DBforMySQL/flexibleServers/databases/write",
   "Microsoft.DBforMySQL/servers/databases/delete",
   "Microsoft.DBforMySQL/flexibleServers/databases/delete",
   "Microsoft.DBforPostgreSQL/servers/databases/delete",
   "Microsoft.DBforPostgreSQL/flexibleServers/databases/delete",
   "Microsoft.DBforPostgreSQL/servers/databases/write",
   "Microsoft.DBforPostgreSQL/flexibleServers/databases/write",
   "Microsoft.DBforPostgreSQL/servers/read",
   "Microsoft.DBforPostgreSQL/servers/databases/read",
   "Microsoft.DBforPostgreSQL/flexibleServers/read",
   "Microsoft.Compute/virtualMachines/read",
   "Microsoft.DBforPostgreSQL/flexibleServers/databases/read"
          ],
```

PaaS の作業負荷に必要な追加の権限

```
"Microsoft.DBforMySQL/servers/read",
"Microsoft.DBforMySQL/servers/databases/read",
"Microsoft.DBforMySQL/flexibleServers/read",
"Microsoft.DBforMySQL/flexibleServers/databases/read",
"Microsoft.DBforPostgreSQL/servers/read",
"Microsoft.DBforPostgreSQL/servers/databases/read",
"Microsoft.DBforPostgreSQL/flexibleServers/read",
"Microsoft.DBforMariaDB/servers/read",
"Microsoft.DBforMariaDB/servers/databases/read",
```

```
"Microsoft.DBforPostgreSQL/flexibleServers/databases/read",
"Microsoft.Sql/*/write",
"Microsoft.Sql/*/delete"
```

PaaS Azure SQL と管理対象インスタンスにシステム管理対象 ID を使用する場合は、メディアサーバーと Snapshot Manager に同じ権限またはルールのセットを適用します。ユーザー管理 ID を使用する場合は、同じユーザー管理 ID をメディアサーバーと Snapshot Manager に関連付けます。

NoSQL 用 Azure Cosmos DB に必要な権限

```
"Microsoft.DocumentDB/databaseAccounts/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/throughputSettings
/read"
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/throughputSettings
/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/storedProcedures
/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/storedProcedures
/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/triggers/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/triggers/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/userDefinedFunctions
/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/containers/userDefinedFunctions
/write",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/throughputSettings/read",
"Microsoft.DocumentDB/databaseAccounts/sqlDatabases/throughputSettings/write"
```

MongoDB 用 Azure Cosmos DB に必要な権限

```
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/write",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections
/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections
/write",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/delete",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/throughputSettings
/read",
"Microsoft.DocumentDB/databaseAccounts/mongodbDatabases/collections/throughputSettings
```

```
/write",
"Microsoft.DocumentDB/databaseAccounts/listKeys/action"
```

クラウドオブジェクトストアに必要な権限

Microsoft Azure Object Store の検出、バックアップ、リストア、認証に必要な権限のセットを次に示します。

```
{
 "properties": {
     "roleName": "cosp_minimal",
    "description": "minimal permission required for cos protection.",

     "assignableScopes": [
         "/subscriptions/<Subsfription_ID>"
     ],
     "permissions": [
         {
           "actions": [
             "Microsoft.Storage/storageAccounts/blobServices/read",
             "Microsoft.Storage/storageAccounts/
blobServices/containers/read",
             "Microsoft.Storage/storageAccounts/
blobServices/containers/write",
             "Microsoft.ApiManagement/service/*",
             "Microsoft.Authorization/*/read",
            "Microsoft.Resources/subscriptions/resourceGroups/read",

             "Microsoft.Storage/storageAccounts/read"

           ],
           "notActions": [],
           "dataActions": [
             "Microsoft.Storage/storageAccounts/
blobServices/containers/blobs/write",
             "Microsoft.Storage/storageAccounts/
blobServices/containers/blobs/filter/action",
             "Microsoft.Storage/storageAccounts/
blobServices/containers/blobs/tags/write",
             "Microsoft.Storage/storageAccounts/
blobServices/containers/blob/read",
           ],
           "notDataActions": []
         }
```

```
        ]
    }
}
```

Powershell を使用してカスタム役割を作成するには、Azure マニュアルの手順に従ってください。

次に例を示します。

```
New-AzureRmRoleDefinition -InputFile
"C:¥CustomRoles¥ReaderSupportRole.json"
```

Azure CLI を使用してカスタム役割を作成するには、Azure マニュアルの手順に従ってください。

次に例を示します。

```
az role definition create --role-definition "~/CustomRoles/
ReaderSupportRole.json"
```

メモ: 役割を作成する前に、以前に指定された役割定義 (JSON 形式のテキスト) を .json ファイルにコピーし、そのファイルを入力ファイルとして使用する必要があります。前述のサンプルコマンドでは、役割定義テキストを含む入力ファイルとして `ReaderSupportRole.json` を使用しています。

この役割を使用するには、次の手順を実行します。

- Azure 環境で動作しているアプリケーションに役割を割り当てます。
- NetBackup Snapshot Manager で、アプリケーションのクレデンシャルを使用して Azure オフホストプラグインを構成します。

p.171 の「Microsoft Azure プラグインの構成に関する注意事項」を参照してください。

Azure のスナップショットについて

NetBackup は Azure での増分スナップショットをサポートします。NetBackup は、前回のスナップショット以降に新たに変更が加えられたディスクの増分スナップショットを作成します。スナップショットはそれぞれ独立しています。たとえば、1 つのスナップショットを削除しても、それ以降に NetBackup が作成するスナップショットには影響しません。増分スナップショットは、必要なディスク容量を削減し、ストレージとして Premium HDD ではなく Azure Standard HDD を使用してバックアップのコストを大幅に削減します。

Microsoft Azure Stack Hub プラグインの構成に関する注意事項

Microsoft Azure Stack Hub プラグインでは、仮想マシンレベルと管理対象ディスクレベルでスナップショットを作成、削除、リストアできます。AAD または ADFS 認証方法を使用して、Azure Stack Hub プラグインを構成できます。

Azure Stack Hub プラグインを構成する前に、次の準備手順を完了します。

- Azure Stack Hub プラグインの ID プロバイダとして AAD (Azure Active Directory) を使用する場合、AAD にアプリケーションを作成するには、Microsoft Azure Stack ポータルを使用します。
  ID プロバイダのオプションについて詳しくは、Azure Stack のマニュアルを参照してください。
- リソースにアクセス可能な役割にサービスプリンシパルを割り当てます。

詳しくは、Azure Stack のマニュアルに記載されている手順に従ってください。

表 5-9 AAD を使用した Azure Stack Hub プラグインの構成パラメータ

NetBackup Snapshot Manager の構成パラメータ	Microsoft 製品の同等の用語と説明
Azure Stack Hub Resource Manager エンドポイントの URL (Azure Stack Hub Resource Manager endpoint URL)	NetBackup Snapshot Manager を Azure リソースに接続できるようにする、次の形式のエンドポイント URL。 `https://management.<location>.<FQDN>`
テナント ID (Tenant ID)	アプリケーションを作成した AAD ディレクトリの ID。
Client ID	アプリケーション ID。
シークレットキー (Secret Key)	アプリケーションのシークレットキー。
認証リソースの URL (省略可能) (Authentication Resource URL (optional))	認証トークンの送信先の URL。

表 5-10 AD FS を使用した Azure Stack Hub プラグインの構成パラメータ

NetBackup Snapshot Manager の構成パラメータ	Microsoft 製品の同等の用語と説明
Azure Stack Hub Resource Manager エンドポイントの URL (Azure Stack Hub Resource Manager endpoint URL)	NetBackup Snapshot Manager を Azure リソースに接続できるようにする、次の形式のエンドポイント URL。 `https://management.<location>.<FQDN>`

NetBackup Snapshot Manager の構成パラメータ	Microsoft 製品の同等の用語と説明
テナント ID (Tenant ID) (オプション)	アプリケーションを作成した AD FS ディレクトリの ID。
クライアント ID (Client ID)	アプリケーション ID。
シークレットキー (Secret Key)	アプリケーションのシークレットキー。
認証リソースの URL (省略可能) (Authentication Resource URL (optional))	認証トークンの送信先の URL。

Azure Stack Hub プラグインの制限事項

- プラグインの現在のリリースでは、BLOB のスナップショットはサポートされていません。
- NetBackup Snapshot Manager では現在、Azure Stack 管理対象ディスクと、管理対象ディスクによってバックアップされた仮想マシンのスナップショットの作成とリストアのみをサポートしています。
- NetBackup Snapshot Manager では現在、Azure Stack 管理対象ディスクと、Azure Stack Resource Manager 配備モデルを使用して配備された仮想マシンのスナップショットの作成とリストアのみをサポートしています。
- Azure Stack VM では OS ディスクのスワップをサポートしていないため、ロールバックリストア操作はサポートされません。
- Azure Stack Hub 2008 ではディスクの暗号化をサポートしていないため、NetBackup Snapshot Manager Azure Stack Hub プラグインではディスクの暗号化を実行できません。
- NetBackup Snapshot Manager では、ストレージプールから作成された仮想ディスクまたはストレージ領域にデータを格納するアプリケーションに対して、ディスクベースの保護をサポートしません。そのようなアプリケーションのスナップショットを作成するときには、ディスクベースのオプションは利用できません。
- NetBackup Snapshot Manager では、Azure Stack 環境での Ultra SSD ディスク形式のスナップショット操作をサポートしていません。

Azure Stack Hub プラグインの考慮事項

- 同じプラグインに対して複数の構成を作成する場合は、それらが異なるテナント ID の資産を管理していることを確認します。2 つ以上のプラグイン構成で、クラウド資産の同じセットを同時に管理しないようにする必要があります。
- スナップショットを作成するときに、Azure Stack Hub プラグインは各スナップショットに Azure Stack 固有のロックオブジェクトを作成します。スナップショットは、Azure コ

ンソールから、または Azure CLI または API 呼び出しからの予期しない削除を防ぐためにロックされます。ロックオブジェクトは、スナップショットと同じ名前になります。また、ロックオブジェクトには、スナップショットが属する、対応する VM または資産の ID が含まれる「notes」という名前のフィールドも含まれています。

スナップショットロックオブジェクトの「notes」フィールドが変更または削除されていないことを確認する必要があります。変更または削除されていると、対応する元の資産からスナップショットの関連付けが解除されます。

Azure Stack Hub プラグインは、ロックオブジェクトの「notes」フィールドの ID を使用して、たとえば「元の場所」へのリストア操作の一環として、ソースディスクを置換または削除するインスタンスにスナップショットを関連付けます。

Microsoft Azure Stack Hub でのアクセス権の設定

NetBackup Snapshot Manager で Microsoft Azure Stack 資産を保護できるようにするには、事前に Microsoft Azure Stack 資産へのアクセス権が必要です。NetBackup Snapshot Manager ユーザーが Azure Stack 資産と連携するために使用できるカスタム役割を関連付ける必要があります。

次のことを NetBackup Snapshot Manager に可能にするカスタム役割の定義を、以下に JSON 形式で示します。

- Azure Stack Hub プラグインを構成し、資産を検出します。
- ホストとディスクのスナップショットを作成します。
- 元の場所または新しい場所にスナップショットをリストアします。
- スナップショットを削除します。

表 5-11 NetBackup Snapshot Manager の機能と Microsoft Azure Stack Hub クラウドプロバイダの権限

機能	タスク/操作	必要な権限:
VM ベース		

機能	タスク/操作	必要な権限:
スナップショットからのバックアップ	スナップショットからのバックアップ用に共有アクセスシグネチャ URI を作成します。	Microsoft.Storage/*/read
	スナップショットからのバックアップ用に共有アクセスシグネチャ URI を生成します。	Microsoft.Compute/restorePointCollections/restorePoints/retrieveSasUris/action
	アクセス権を取得して、スナップショットからのバックアップでバックアップコピーを作成するために、ディスクリストアポイントから読み取ります。	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/beginGetAccess/action
	スナップショットからのバックアップが正常に完了した後に、リストアポイントへのアクセス終了を取得します。	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/endGetAccess/action
スナップショットからのバックアップ作成	スナップショットデータへのアクセス権を取得します。	Microsoft.Compute/snapshots/beginGetAccess/action
	スナップショットのデータがバックアップにコピーされた後に URI を終了します。	Microsoft.Compute/snapshots/endGetAccess/action
スナップショットからのバックアップからのリストア	管理対象ディスクの共有アクセスシグネチャ URI を作成します。	Microsoft.Compute/disks/beginGetAccess/action
	スナップショットからのバックアップの後、共有アクセスシグネチャ URI を削除します。	Microsoft.Compute/disks/endGetAccess/action
仮想マシンの保護	VM、VM スケールセット、接続されたディスクを一覧表示します。	Microsoft.Compute/*/read

機能	タスク/操作	必要な権限:
SQL データベースの保護	保護対象の Azure SQL データベースを一覧表示します。	`Microsoft.Sql/*/read`
スナップショットまたはリストアポイントからのディスクのリストア	リストア用のディスクを作成します。	`Microsoft.Compute/disks/write`
ロールバックリストア/リストアのクリーンアップ	ロールバックリストアで VM をリストアします。 または リストアワークフローでエラーが発生した場合にクリーンアップします。	`Microsoft.Compute/virtualMachines/delete`
ディスクのリストア	ディスクまたはファイルをリストアするために利用可能なディスクの接続ポイントを識別します。	`Microsoft.Compute/virtualMachines/vmSizes/read`
クリーンアップ	リストアワークフローのクリーンアップでエラーが発生した場合に、パブリック IP を削除します。元の VM にパブリック IP があり、代替の場所へのリストアが失敗した場合。	`Microsoft.Network/publicIPAddresses/delete`
	スナップショットの作成ワークフローが失敗したためにロールバックした場合に、RPC を削除します。	`Microsoft.Compute/restorePointCollections/delete`
リソースの一覧表示 (検出)	リソースグループと場所の情報を取得します。	`Microsoft.Resources/*/read`
検出	保護対象の資産を一覧表示するために使用できるサブスクリプションを一覧表示します。	`Microsoft.Subscription/*/read`

機能	タスク/操作	必要な権限:
スナップショットとリストア	タグが Snapshot Manager で作成されていることを示すために、タグをスナップショットに追加します VM に元々存在していたタグをリストアされた VM に追加します。	Microsoft.Resources/subscriptions/tagNames/tagValues/write Microsoft.Resources/subscriptions/tagNames/write
スナップショット	ディスクスナップショットを誤って削除しないように保護します。	Microsoft.Authorization/locks/*
リストアポイントの一覧表示	リストア用にスナップショット (リストアポイント) を一覧表示します。	Microsoft.Compute/restorePointCollections/read
スナップショットの一覧表示	VM のリストアポイントを一覧表示およびマッピングします。	Microsoft.Compute/restorePointCollections/restorePoints/read
ディスクスナップショットの一覧表示	アプリケーションの一貫性を確保するために、ディスクのリストアポイントを一覧表示します。	Microsoft.Compute/restorePointCollections/restorePoints/diskRestorePoints/read
スナップショットの書き込み	リストアポイントとしての増分スナップショット (アプリケーション整合)。	Microsoft.Compute/restorePointCollections/restorePoints/write
スナップショットのクリーンアップ	リストアエラーが発生した場合のクリーンアップ。	Microsoft.Compute/restorePointCollections/restorePoints/delete
リストアポイントコレクションの作成	VM に対してスナップショットがトリガされた場合に備えて VM ごとに 1 つの RPC を作成します。	Microsoft.Compute/restorePointCollections/write

機能	タスク/操作	必要な権限:
VM のリストア	リストアで VM を作成します。	Microsoft.Compute/virtualMachines/write
	保護計画で説明されているように、リストアされた VM の電源をオンにします。	Microsoft.Compute/virtualMachines/start/action
	VM の状態を変更します。ロールバックリストアのために VM を停止します。	Microsoft.Compute/virtualMachines/powerOff/action
	元のリソースと同じネットワーク、またはユーザーが選択したネットワークにリストアするために、ネットワークを一覧表示します。	Microsoft.Network/*/read
	リストアをロールバックします。ワークフローでエラーが発生した場合にクリーンアップします。	Microsoft.Network/networkInterfaces/delete
	リストアされた VM にネットワークインターフェースカードを接続します。	Microsoft.Network/networkInterfaces/join/action
	VM リストア用のネットワークインターフェースカードを作成します。	Microsoft.Network/networkInterfaces/write
	リストア時にネットワークセキュリティグループを VM に接続します。	Microsoft.Network/networkSecurityGroups/join/action
	VM リストア用のネットワークセキュリティグループを作成します (元の VM にネットワークセキュリティグループが存在する場合)。	Microsoft.Network/networkSecurityGroups/write
	元の VM にパブリック IP がある場合にリストアでパブリック IP を接続します。	Microsoft.Network/publicIPAddresses/join/action

機能	タスク/操作	必要な権限:
	元の VM にパブリック IP がある場合にリストアでパブリック IP を作成します。	Microsoft.Network/publicIPAddresses/write
	サブネット内に VM を作成します。つまり、サブネットを結合します。	Microsoft.Network/virtualNetworks/subnets/join/action
Kubernetes クラスタベース		
クラスタ情報の取得	クラスタ情報を取得します。	Microsoft.ContainerService/managedClusters/agentPools/read
スケールイン/スケールアウト	クラスタの機能を取得します。	Microsoft.ContainerService/managedClusters/read
スケールイン	VM スケールセットの状態を維持します。	Microsoft.Compute/virtualMachineScaleSets/delete/action
スケールアウト	VM スケールセットの状態を維持します。	Microsoft.Compute/virtualMachineScaleSets/write
マーケットプレイス配備		
高可用性	Snapshot Manager データディスクを VM スケールセットインスタンスに接続します。	Microsoft.Compute/virtualMachineScaleSets/write
	(スケールイン) VM スケールセットの状態を維持します。	Microsoft.Compute/virtualMachineScaleSets/delete/action

Powershell を使用してカスタム役割を作成するには、Azure Satck マニュアルの手順に従ってください。

次に例を示します。

- New-AzRoleDefinition

```
New-AzRoleDefinition -InputFile
"C:¥CustomRoles¥registrationrole.json"
```

- New-AzureRmRoleDefinition

```
New-AzureRmRoleDefinition -InputFile C:¥tools¥customRoleDef.json
```

Azure CLI を使用してカスタム役割を作成するには、Azure マニュアルの手順に従ってください。

次に例を示します。

```
az role definition create --role-definition "~/CustomRoles/
registrationrole.json"
```

メモ: 役割を作成する前に、役割定義 (JSON 形式のテキスト) を .json ファイルにコピーし、そのファイルを入力ファイルとして使用する必要があります。前述のサンプルコマンドでは、役割定義のテキストを含む入力ファイルとして registrationrole.json を使用しています。

この役割を使用するには、次の手順を実行します。

- Azure Stack 環境で動作しているアプリケーションに役割を割り当てます。
- NetBackup Snapshot Manager で、アプリケーションのクレデンシャルを使用して Azure Stack オフホストプラグインを構成します。

p.190 の「Microsoft Azure Stack Hub プラグインの構成に関する注意事項」を参照してください。

バックアップからリストアするための Azure Stack Hub VM のステージング場所の構成

Azure Stack Hub では、ストレージアカウント内にコンテナを作成し、バックアップイメージからリストアする際にステージング場所として使用する必要があります。ステージング場所は、リストア時にコンテナ内の管理対象外ディスクのステージングに使用されます。データがディスクに書き込まれると、ディスクは管理対象ディスクに変換されます。これは Azure Stack Hub プラットフォームの要件です。NetBackup で Azure Stack Hub を使用するための必須の構成です。

azurestack.conf ファイルには、VM がリストアされるサブスクリプション ID のステージング場所の詳細を含める必要があります。ソースサブスクリプション ID 以外の任意のターゲットサブスクリプション ID にリストアする場合は、ターゲットサブスクリプション ID の詳細が azurestack.conf ファイルに存在する必要があります。

リストアにスナップショットイメージを使用する場合、このステージング場所を作成する必要はありません。

メモ: ステージング場所はサブスクリプション ID に固有で、VM のリストアに使用しているサブスクリプションごとに 1 つのステージング場所を作成する必要があります。

サブスクリプション ID に対するステージング場所を構成するには

1 NetBackup Snapshot Manager で、

/cloudpoint/azurestack.conf に移動し、テキストエディタでこのファイルを開きます。このファイルは、NetBackup のクラウドサービスプロバイダとして Azure Stack Hub を追加した後にのみ作成されます。

2 ファイルに次の詳細を追加します。

[subscription/<subscription ID>]

storage_container = <ストレージコンテナの名前>

storage_account = /resourceGroup/<ストレージアカウントが存在するリソースグループの名前>/storageaccount/<ストレージアカウントの名前>

例: /resourceGroup/Harsha_RG/storageaccount/harshastorageacc

3 使用しているサブスクリプション ID ごとに、手順 2 を繰り返します。ファイルを保存して閉じます。

Azure Stack Hub スナップショットについて

NetBackup は Azure Stack Hub での増分スナップショットをサポートします。NetBackup は、Azure Stack Hub が提供する増分スナップショット機能を利用して、スナップショット間で変更されたブロックのみを格納します。スナップショットはそれぞれ独立しています。たとえば、1 つのスナップショットを削除しても、それ以降に NetBackup が作成するスナップショットには影響しません。増分スナップショットは、必要なディスク容量を削減し、ストレージとして Azure Standard HDD および Premium HDD を使用してバックアップのコストを大幅に削減します。

メモ: プレミアムディスク (SSD) と標準ディスク (HDD) は、Azure Stack Hub の同じストレージインフラでバッキングされます。提供されるパフォーマンスは同じです。

OCI プラグインの構成に関する注意事項

OCI プラグインを使用すると、OCI の VM と Oracle アプリケーションのスナップショットとバックアップを作成、リストア、削除できます。VM スナップショットからボリュームをリストアすることもできます。

OCI プラグインを構成する前に、保護するリージョンが有効になっていることと、NetBackup Snapshot Manager で OCI 資産を管理できるようにするために適切なアクセス権が構成されていることを確認します。

Oracle Private Cloud Appliance (PCA) では、リージョンは必須ではありません。

次に、NetBackup でサポートされる OCI のリージョンのリストを示します。

表 5-12 NetBackup Snapshot Manager でサポートされる OCI 商業リージョン

OCI 商業リージョン
af-johannesburg-1,
ap-chiyoda-1, ap-chuncheon-1, ap-dcc-canberra-1, ap-dcc-gazipur-1, ap-hyderabad-1, ap-ibaraki-1, ap-melbourne-1, ap-mumbai-1, ap-osaka-1, ap-seoul-1, ap-singapore-1, ap-singapore-2, ap-sydney-1, ap-tokyo-1, ap-chuncheon-2, ap-seoul-2, ap-suwon-1,
ca-montreal-1, ca-toronto-1,
eu-amsterdam-1, eu-dcc-milan-1, eu-dcc-milan-2, eu-dcc-dublin-1, eu-dcc-dublin-2, eu-dcc-rating-1, eu-dcc-rating-2, eu-dcc-zurich-1, eu-frankfurt-1, eu-frankfurt-2, eu-jovanovac-1, eu-madrid-1, eu-madrid-2, eu-marseille-1, eu-milan-1, eu-paris-1, eu-stockholm-1, eu-zurich-1,
il-jerusalem-1,
me-abudhabi-1, me-abudhabi-2, me-abudhabi-3, me-dcc-doha-1, me-dcc-muscat-1, me-dubai-1, me-jeddah-1, me-alain-1,
mx-monterrey-1, mx-queretaro-1,
sa-bogota-1, sa-santiago-1, sa-saopaulo-1, sa-valparaiso-1, sa-vinhedo-1,
uk-cardiff-1, uk-london-1,
us-ashburn-1, us-chicago-1, us-phoenix-1, us-saltlake-2, us-sanjose-1,

NetBackup OCI サポートの制限事項

- レプリケーションはサポートされません。
- Govt. クラウドリージョンはサポートされません。
- OCI CSP 構成は共有 VCN をサポートしません。
- AIR コピーからの VM のリストアはサポートされませんが、AIR コピーからのファイルとフォルダのリストアはサポートされます。
- スナップショットからのバックアップを機能させるには、Snapshot Manager と作業負荷 VM が同じリージョンにある必要があります。
- アプリケーションの整合性スナップショットは Windows インスタンスではサポートされません。
- ISCSI ボリュームの添付ファイルの種類は、ベンダーの制限により、Oracle PCA ではサポートされません。

OCI プラグイン構成の前提条件

OCI クラウドに NetBackup Snapshot Manager プラグインを配備する前に、次の手順を実行します。

- 動的グループを作成し、NetBackup Snapshot Manager をその動的グループの一部として含めます。動的グループの作成について詳しくは、OCI のマニュアルの「動的グループの管理」セクションを参照してください。
- 必要な権限でポリシーを作成します。p.202 の「NetBackup Snapshot Manager に必要な OCI 権限」を参照してください。
- スナップショット、シングルファイルリストア、インデックスからのバックアップの場合、ブロックボリューム管理プラグインを NetBackup Snapshot Manager ホストで有効にする必要があります。

OCI の構成パラメータ

NetBackup Snapshot Manager が OCI クラウドに配備されている場合、これは必須パラメータです。

表 5-13 OCI 配備のための OCI プラグイン構成パラメータ

NetBackup Snapshot Manager の構成パラメータ	説明
ソースアカウントの構成	
リージョン (Regions)	OCI ソースアカウントに関連付けられた、クラウド資産を検出する 1 つ以上の OCI リージョン。
endpointurl	これは Oracle PCA の必須パラメータです。

NetBackup Snapshot Manager が OCI クラウドに配備されていない場合、これらは必須パラメータです。

表 5-14 非 OCI 配備のための OCI プラグイン構成パラメータ

NetBackup Snapshot Manager の構成パラメータ	説明
ソースアカウントの構成	
ユーザー OCID (User OCID)	クレデンシャルを生成するユーザーの OCID。
テナンシー (Tenancy)	OCI アカウントのテナント ID。

NetBackup Snapshot Manager の構成パラメータ	説明
指紋 (Fingerprint)	クレデンシャルの生成中に取得した指紋。
秘密鍵 (Private Key)	クレデンシャルの生成中に取得した秘密鍵。
リージョン (Regions)	OCI ソースアカウントに関連付けられた、クラウド資産を検出する 1 つ以上の OCI リージョン。
endpointurl	これは Oracle PCA の必須パラメータです。

OCI のホストサポートの構成

OCI は OEL (Oracle Enterprise Linux) ホストと非 OEL ホストの両方をサポートします。

- OEL ホストでは、準仮想化と iSCSI の両方のタイプのボリューム添付がサポートされます。
- 非 OEL ホストは、iSCSI タイプのボリューム添付のみをサポートします。

非 OEL ホストで次の手順を実行して、準仮想化された添付をサポートします。ブロックボリュームを接続して、準仮想化された種類の添付を使用できます。

一貫性のあるスナップショットと個別リストアを実行するには、すべてのホストに Oracle Cloud Agent をインストールする必要があります。

1. 添付の種類を iSCSI に変更します。
2. プラグインレベルの検出または詳細検出を実行します。
3. その後、このホストに対してアプリケーションの整合性スナップショットが作成されます。

NetBackup Snapshot Manager に必要な OCI 権限

次の表に必要な権限を一覧表示します。

表 5-15 OCI 権限

権限	説明
`BOOT_VOLUME_BACKUP_CREATE`	ブートボリュームのスナップショットを作成します。
`BOOT_VOLUME_BACKUP_DELETE`	ポリシーに従ってブートボリュームのスナップショットを削除します。
`BOOT_VOLUME_BACKUP_INSPECT`	検出のブートボリュームバックアップのリストを取得します。

権限	説明
BOOT_VOLUME_BACKUP_READ	バックアップからブートボリュームを作成します。
COMPARTMENT_INSPECT	可用性ドメインを一覧表示し、テナント内のすべてのコンパートメントを取得します。
INSTANCE_ATTACH_VOLUME	リストア時にインスタンスにボリュームを接続します。
INSTANCE_CREATE	インスタンスをリストアします。
INSTANCE_DELETE	バックアップコピーからのブートボリュームのリストア用に作成されたインスタンスを作成および削除します。
INSTANCE_DETACH_VOLUME	バックアップおよびリストア操作後にボリュームを切断します。
INSTANCE_IMAGE_INSPECT	インスタンスの OS の詳細をフェッチします。
INSTANCE_INSPECT	VNIC やボリュームなどの各種の添付ファイルを一覧表示します。
INSTANCE_POWER_ACTIONS	パラメータ化されたリストア中にインスタンスを停止または起動します。
INSTANCE_READ	検出したインスタンスを一覧表示し、インスタンスの詳細を取得します。
INSTANCE_UPDATE	インスタンスに添付されているタグを更新します。
KEY_ASSOCIATE	パラメータ化されたリストアに CMK を関連付けます。
KEY_DISASSOCIATE	パラメータ化されたリストアの CMK の関連付けを解除します。
KEY_INSPECT	Vault のキーを一覧表示します。
KEY_READ	キーの詳細を取得します。
NETWORK_SECURITY_GROUP_READ	パラメータ化されたリストア用のネットワークセキュリティグループを一覧表示します。
NETWORK_SECURITY_GROUP_UPDATE_MEMBERS	ネットワークセキュリティグループをインスタンスに接続します。
SUBNET_ATTACH	特定のサブネットでインスタンスを起動します。
SUBNET_DETACH	特定のサブネットでインスタンスを終了します。

権限	説明
SUBNET_READ	パラメータ化されたリストアでサブネットを一覧表示します。
TAG_NAMESPACE_CREATE	NetBackup Snapshot Manager のタグ名前空間を作成します。
TAG_NAMESPACE_INSPECT	NetBackup Snapshot Manager のタグ名前空間が存在するかどうかを確認します。
TAG_NAMESPACE_USE	NetBackup Snapshot Manager のタグ名前空間のタグを作成します。
TENANCY_INSPECT	テナントの詳細を取得します。
VAULT_INSPECT	Vault を一覧表示し、キーを取得します。
VCN_READ	インスタンスに関連付けられている VCN の詳細を取得します。
VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP	インスタンスの起動時にネットワークセキュリティグループを関連付けます。
VNIC_ATTACH	インスタンスを起動します。
VNIC_ATTACHMENT_READ	VNIC の添付ファイルを一覧表示します。
VNIC_CREATE	インスタンスの起動時にインスタンスに VNIC を関連付けます。
VNIC_DELETE	関連付けられた VNIC を削除してインスタンスを削除します。
VNIC_READ	インスタンスに関連付けられている VNIC 情報をフェッチします。
VOLUME_ATTACHMENT_CREATE	リストア後にボリュームを接続します。
VOLUME_ATTACHMENT_DELETE	リストア後にボリュームを接続します。
VOLUME_ATTACHMENT_INSPECT	バックアップおよびリストア後にボリュームを切断します。
VOLUME_BACKUP_CREATE	ボリュームのスナップショットを作成します。
VOLUME_BACKUP_DELETE	ポリシーに従ってボリュームのスナップショットを削除します。
VOLUME_BACKUP_INSPECT	検出中にボリュームバックアップのリストを取得します。

権限	説明
VOLUME_BACKUP_READ	検出中にボリュームバックアップを一覧表示します。
VOLUME_CREATE	リストア中にボリュームを作成します。
VOLUME_DELETE	可用性ドメインが変更された場合に、パラメータ化されたリストア中にボリュームを削除します。
VOLUME_INSPECT	検出中にボリュームを一覧表示します。
VOLUME_UPDATE	ボリュームのタグとさまざまな属性を更新します。
VOLUME_WRITE	スナップショットからボリュームを作成します。

作成するポリシーに権限を割り当てる例を次に示します。ここで、*nbsm-iam-role* は動的グループの名前であり、NetBackup Snapshot Manager はその動的グループに含まれます。

```
Allow dynamic-group nbsm-iam-role to inspect compartments in tenancy
Allow dynamic-group nbsm-iam-role to inspect instance-images in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vnic-attachments in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vaults in tenancy
Allow dynamic-group nbsm-iam-role to read vcns in tenancy
Allow dynamic-group nbsm-iam-role to use keys in tenancy
Allow dynamic-group nbsm-iam-role to use subnets in tenancy where
any { request.permission='SUBNET_DETACH',
request.permission='SUBNET_ATTACH', request.permission='SUBNET_READ'
 }
Allow dynamic-group nbsm-iam-role to manage boot-volumes in tenancy
 where any { request.permission='BOOT_VOLUME_CREATE',
request.permission='BOOT_VOLUME_DELETE',
request.permission='BOOT_VOLUME_INSPECT',
request.permission='BOOT_VOLUME_WRITE' }
Allow dynamic-group nbsm-iam-role to manage boot-volume-backups in
tenancy where any { request.permission='BOOT_VOLUME_BACKUP_CREATE',
 request.permission='BOOT_VOLUME_BACKUP_DELETE',
request.permission='BOOT_VOLUME_BACKUP_INSPECT',
request.permission='BOOT_VOLUME_BACKUP_READ' ,
request.permission='BOOT_VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage instances in tenancy
where any { request.permission='INSTANCE_ATTACH_VOLUME',
```

```
request.permission='INSTANCE_CREATE',
request.permission='INSTANCE_DELETE',
request.permission='INSTANCE_DETACH_VOLUME',
request.permission='INSTANCE_INSPECT',
request.permission='INSTANCE_READ',
request.permission='INSTANCE_POWER_ACTIONS',
request.permission='INSTANCE_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage network-security-groups
 in tenancy where any {
request.permission='NETWORK_SECURITY_GROUP_READ',
request.permission='NETWORK_SECURITY_GROUP_UPDATE_MEMBERS' }
Allow dynamic-group nbsm-iam-role to manage tag-namespaces in tenancy
 where any { request.permission='TAG_NAMESPACE_CREATE',
request.permission='TAG_NAMESPACE_USE',
request.permission='TAG_NAMESPACE_INSPECT' }
Allow dynamic-group nbsm-iam-role to manage volumes in tenancy where
 any { request.permission='VOLUME_CREATE',
request.permission='VOLUME_DELETE',
request.permission='VOLUME_INSPECT',
request.permission='VOLUME_WRITE', request.permission='VOLUME_UPDATE'
 }
Allow dynamic-group nbsm-iam-role to manage volume-attachments in
tenancy where any { request.permission='VOLUME_ATTACHMENT_CREATE',
request.permission='VOLUME_ATTACHMENT_DELETE',
request.permission='VOLUME_ATTACHMENT_INSPECT' }
Allow dynamic-group nbsm-iam-role to manage volume-backups in tenancy
 where any { request.permission='VOLUME_BACKUP_CREATE',
request.permission='VOLUME_BACKUP_DELETE',
request.permission='VOLUME_BACKUP_INSPECT'request.permission='VOLUME_BACKUP_READ',
 request.permission='VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage vnics in tenancy where
any { request.permission='VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP',
request.permission='VNIC_ATTACH', request.permission='VNIC_CREATE',
 request.permission='VNIC_DELETE', request.permission='VNIC_READ' }
Allow dynamic-group nbsm-iam-role to use key-delegate in tenancy
```

NetBackup Snapshot Manager に必要な Oracle PCA 権限

次の表に必要な権限を一覧表示します。

表 5-16 Oracle PCA 権限

権限	説明
BOOT_VOLUME_BACKUP_CREATE	ブートボリュームのスナップショットを作成します。
BOOT_VOLUME_BACKUP_DELETE	ポリシーに従ってブートボリュームのスナップショットを削除します。
BOOT_VOLUME_BACKUP_INSPECT	検出のブートボリュームバックアップのリストを取得します。
BOOT_VOLUME_BACKUP_READ	バックアップからブートボリュームを作成します。
COMPARTMENT_INSPECT	可用性ドメインを一覧表示し、テナント内のすべてのコンパートメントを取得します。
INSTANCE_ATTACH_VOLUME	リストア時にインスタンスにボリュームを接続します。
INSTANCE_CREATE	インスタンスをリストアします。
INSTANCE_DELETE	バックアップコピーからのブートボリュームのリストア用に作成されたインスタンスを作成および削除します。
INSTANCE_DETACH_VOLUME	バックアップおよびリストア操作後にボリュームを切断します。
INSTANCE_IMAGE_INSPECT	インスタンスの OS の詳細をフェッチします。
INSTANCE_INSPECT	VNIC やボリュームなどの各種の添付ファイルを一覧表示します。
INSTANCE_POWER_ACTIONS	パラメータ化されたリストア中にインスタンスを停止または起動します。
INSTANCE_READ	検出したインスタンスを一覧表示し、インスタンスの詳細を取得します。
INSTANCE_UPDATE	インスタンスに添付されているタグを更新します。
NETWORK_SECURITY_GROUP_READ	パラメータ化されたリストア用のネットワークセキュリティグループを一覧表示します。
NETWORK_SECURITY_GROUP_UPDATE_MEMBERS	ネットワークセキュリティグループをインスタンスに接続します。
SUBNET_ATTACH	特定のサブネットでインスタンスを起動します。
SUBNET_DETACH	特定のサブネットでインスタンスを終了します。

権限	説明
SUBNET_READ	パラメータ化されたリストアでサブネットを一覧表示します。
TAG_NAMESPACE_CREATE	NetBackup Snapshot Manager のタグ名前空間を作成します。
TAG_NAMESPACE_INSPECT	NetBackup Snapshot Manager のタグ名前空間が存在するかどうかを確認します。
TAG_NAMESPACE_USE	NetBackup Snapshot Manager のタグ名前空間のタグを作成します。
TENANCY_INSPECT	テナントの詳細を取得します。
VAULT_INSPECT	Vault を一覧表示し、キーを取得します。
VCN_READ	インスタンスに関連付けられている VCN の詳細を取得します。
VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP	インスタンスの起動時にネットワークセキュリティグループを関連付けます。
VNIC_ATTACH	インスタンスを起動します。
VNIC_ATTACHMENT_READ	VNIC の添付ファイルを一覧表示します。
VNIC_CREATE	インスタンスの起動時にインスタンスに VNIC を関連付けます。
VNIC_DELETE	関連付けられた VNIC を削除してインスタンスを削除します。
VNIC_READ	インスタンスに関連付けられている VNIC 情報をフェッチします。
VOLUME_ATTACHMENT_CREATE	リストア後にボリュームを接続します。
VOLUME_ATTACHMENT_DELETE	リストア後にボリュームを接続します。
VOLUME_ATTACHMENT_INSPECT	バックアップおよびリストア後にボリュームを切断します。
VOLUME_BACKUP_CREATE	ボリュームのスナップショットを作成します。
VOLUME_BACKUP_DELETE	ポリシーに従ってボリュームのスナップショットを削除します。
VOLUME_BACKUP_INSPECT	検出中にボリュームバックアップのリストを取得します。

権限	説明
VOLUME_BACKUP_READ	検出中にボリュームバックアップを一覧表示します。
VOLUME_CREATE	リストア中にボリュームを作成します。
VOLUME_DELETE	可用性ドメインが変更された場合に、パラメータ化されたリストア中にボリュームを削除します。
VOLUME_INSPECT	検出中にボリュームを一覧表示します。
VOLUME_UPDATE	ボリュームのタグとさまざまな属性を更新します。
VOLUME_WRITE	スナップショットからボリュームを作成します。

作成するポリシーに権限を割り当てる例を次に示します。ここで、*nbsm-iam-role* は動的グループの名前であり、NetBackup Snapshot Manager はその動的グループに含まれます。

```
Allow dynamic-group nbsm-iam-role to inspect compartments in tenancy
Allow dynamic-group nbsm-iam-role to inspect instance-images in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vnic-attachments in
tenancy
Allow dynamic-group nbsm-iam-role to inspect vaults in tenancy
Allow dynamic-group nbsm-iam-role to read vcns in tenancy
Allow dynamic-group nbsm-iam-role to use keys in tenancy
Allow dynamic-group nbsm-iam-role to use subnets in tenancy where
any { request.permission='SUBNET_DETACH',
request.permission='SUBNET_ATTACH', request.permission='SUBNET_READ'
 }
Allow dynamic-group nbsm-iam-role to manage boot-volumes in tenancy
 where any { request.permission='BOOT_VOLUME_CREATE',
request.permission='BOOT_VOLUME_DELETE',
request.permission='BOOT_VOLUME_INSPECT',
request.permission='BOOT_VOLUME_WRITE' }
Allow dynamic-group nbsm-iam-role to manage boot-volume-backups in
tenancy where any { request.permission='BOOT_VOLUME_BACKUP_CREATE',
 request.permission='BOOT_VOLUME_BACKUP_DELETE',
request.permission='BOOT_VOLUME_BACKUP_INSPECT',
request.permission='BOOT_VOLUME_BACKUP_READ' ,
request.permission='BOOT_VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage instances in tenancy
where any { request.permission='INSTANCE_ATTACH_VOLUME',
```

```
request.permission='INSTANCE_CREATE',
request.permission='INSTANCE_DELETE',
request.permission='INSTANCE_DETACH_VOLUME',
request.permission='INSTANCE_INSPECT',
request.permission='INSTANCE_READ',
request.permission='INSTANCE_POWER_ACTIONS',
request.permission='INSTANCE_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage network-security-groups
 in tenancy where any {
request.permission='NETWORK_SECURITY_GROUP_READ',
request.permission='NETWORK_SECURITY_GROUP_UPDATE_MEMBERS' }
Allow dynamic-group nbsm-iam-role to manage tag-namespaces in tenancy
 where any { request.permission='TAG_NAMESPACE_CREATE',
request.permission='TAG_NAMESPACE_USE',
request.permission='TAG_NAMESPACE_INSPECT' }
Allow dynamic-group nbsm-iam-role to manage volumes in tenancy where
 any { request.permission='VOLUME_CREATE',
request.permission='VOLUME_DELETE',
request.permission='VOLUME_INSPECT',
request.permission='VOLUME_WRITE', request.permission='VOLUME_UPDATE'
 }
Allow dynamic-group nbsm-iam-role to manage volume-attachments in
tenancy where any { request.permission='VOLUME_ATTACHMENT_CREATE',
request.permission='VOLUME_ATTACHMENT_DELETE',
request.permission='VOLUME_ATTACHMENT_INSPECT' }
Allow dynamic-group nbsm-iam-role to manage volume-backups in tenancy
 where any { request.permission='VOLUME_BACKUP_CREATE',
request.permission='VOLUME_BACKUP_DELETE',
request.permission='VOLUME_BACKUP_INSPECT'request.permission='VOLUME_BACKUP_READ',
 request.permission='VOLUME_BACKUP_UPDATE' }
Allow dynamic-group nbsm-iam-role to manage vnics in tenancy where
any { request.permission='VNIC_ASSOCIATE_NETWORK_SECURITY_GROUP',
request.permission='VNIC_ATTACH', request.permission='VNIC_CREATE',
 request.permission='VNIC_DELETE', request.permission='VNIC_READ' }
Allow dynamic-group nbsm-iam-role to use key-delegate in tenancy
```

DBPaaS のクラウドサービスプロバイダのエンドポイント

次の表に、DBPaaS の Azure、AWS、GCP クラウドプロバイダのエンドポイントを示します。

メモ: DBPaaS では、OCI クラウドプロバイダはサポートされません。

表 5-17

クラウドサービスプロバイダ	サポート対象データベース	エンドポイント	説明/要件
Azure	管理、メタデータ、共通の API ストレージ	■ *.management.azure.com ■ *.login.microsoftonline.com ■ *.storage.azure.net	
	SQL データベース	*.management.azure.com	サーバーの URL
		*.login.microsoftonline.com	AMI トークンを取得するための URL
	■ 管理対象インスタンス ■ PostgreSQL ■ CosmosDB ■ MongoDB	*.management.azure.com	サーバーの一覧表示
	■ MySQL ■ MariaDB	*.management.azure.com https://ossrdbms-aad.database.windows.net	MySQL の場合 ■ サーバーの一覧表示 ■ データベースの一覧表示 MariaDB の場合 ■ サーバーの URL AMI トークンを取得するための URL
	CosmosDB NoSQL	*.documents.azure.com:443	

クラウドサービスプロバイダ	サポート対象データベース	エンドポイント	説明/要件
AWS	DynamoDB	dynamodb.<region>.amazonaws.com 例: dynamodb.us-east-2.amazonaws.com	デフォルト: DynamoDB はポート 8000 を使用 Amazon DynamoDB エンドポイントとクォータ
	Redshift	redshift.REGION.amazonaws.com redshift-data.REGION.amazonaws.com	■ クラスタとデータベースの一覧表示 ■ データベースに対する問い合わせの実行 Amazon Redshift エンドポイントとクォータ
	■ RDS MySQL ■ RDS Aurora MySQL ■ RDS MariaDB ■ RDS SQL	<REGION>.rds.amazonaws.com RDS SQL の場合: <dudename>s3<REGION>amazonaws.com	
	Custom for Oracle	<NAME>.<REGION>. rds.amazonaws.com	デフォルトポート: 1521
	Custom for SQL	<NAME>.<REGION>rdsamazonaws.com	デフォルトポート: 1433
	DocumentDB	<NAME><REGION>docdbamazonaws.com	デフォルトポート: 27017 Amazon DocumentDB エンドポイントとクォータ
	Neptune	<NAME><REGION>neptuneamazonaws.com	デフォルトポート: 8182 Amazon Neptune エンドポイントとクォータ

クラウドサービスプロバイダ	サポート対象データベース	エンドポイント	説明/要件
GCP	管理、メタデータ、共通の API ストレージ	https://oauth2.googleapis.com/token	OAuth2 トークン交換の場合
	■ MySQL ■ PostgreSQL ■ SQL Server	https://sqladmin.googleapis.com	SQL Server の場合: Access クラウドストレージ

6

クラウドホストまたは VM の資産を保護するための構成

この章では以下の項目について説明しています。

資産の保護に使用する NetBackup Snapshot Manager の機能 (オンホストエージェントまたはエージェントレス) の決定

単一ファイルのリストアまたはファイルシステムまたはアプリケーションの一貫性のために、NetBackup でホスト上の資産を検出して保護するには、プロバイダによって管理される一貫性を通じてスナップショットがファイルシステムまたはアプリケーションで一貫性がある場合でも、ホストにエージェントをインストールします。

(*保護対象のクラウドホストまたは VM の場合*) デフォルトでは、ファイルシステムの整合性スナップショットは、クラウドサービスプロバイダがサポートするプロバイダ管理の整合性によってのみ試行されます。これは、そのような資産のアプリケーションが「接続」状態にあるかどうかとは無関係です。オンホストエージェント接続またはエージェントレス接続は、クラウドホストまたは VM 上のアプリケーションがすべて構成されている場合にのみ必要です。

(*Microsoft Azure クラウドプロバイダ用*) スナップショットがアプリケーション整合になるように Azure リカバリポイントを使用するには、次の表を参照して Azure クラウドで VM に接続して構成します。

(OCI の場合) インスタンスの作成中に作成された、または接続されたブロックボリュームは、オンホスト接続またはエージェントレス接続を使用した整合性スナップショットではサポートされません。

Oracle PCA では、エージェントのインストールと整合性スナップショットはサポートされていません。

Windows の場合	Linux の場合
VM に接続して構成する必要はありません。	■ Linux の場合: デフォルトでは、スナップショットは Azure でファイルシステム整合性を持ちます。 ■ Linux 上の Oracle の場合: ■ VM が接続状態である必要があります。 または ■ アプリケーションの整合性を保つための事前スクリプトまたはポストスクリプトは、「Azure Linux VM のアプリケーション整合性バックアップ」の説明に記載されているとおりに Linux VM 用に構成する必要があります。

エージェントは、ホストの資産を保護するために必要な操作を実行するために必要なプラグインをインストールします。

次のいずれかの方法を使用して、保護する必要があるホストにエージェントをインストールできます。

- オンホストエージェント
  p.216 の「NetBackup Snapshot Manager のオンホストエージェント機能を使用した資産の保護」を参照してください。
- エージェントレス
  p.238 の「NetBackup Snapshot Manager のエージェントレス機能を使用した資産の保護」を参照してください。

上記のどちらの方法でも、操作を実行するために同じプラグインがホストにインストールされます。ただし、上記の 2 つの方法には次の違いがあります。

オンホストエージェント	エージェントレス
ユーザーは手動でエージェントをホストにインストールして、Snapshot Manager ホストに登録する必要があります。	VM に接続または構成することで、NetBackup Web UI を使用してホストにエージェントをインストールできます。
ホストクレデンシャルは、ユーザーがホストに手動でインストールするため、Snapshot Manager に共有しないでください。	ホストまたは VM のクレデンシャルは、Snapshot Manager がホストに接続してエージェントと必要なプラグインをインストールできるように、NetBackup クレデンシャルマネージャに格納する必要があります。

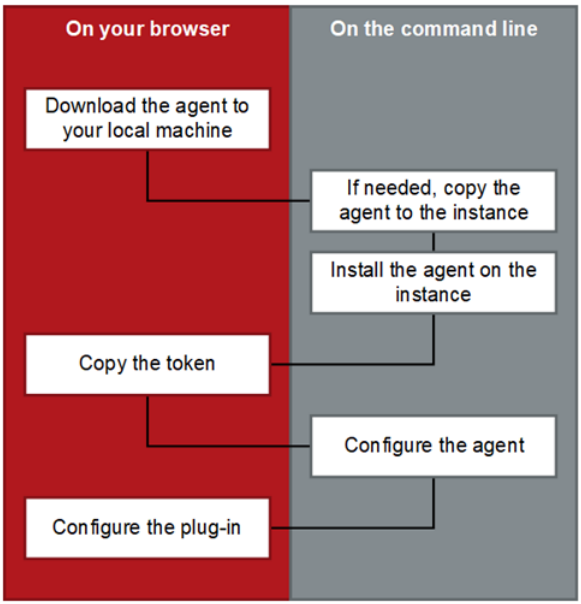
オンホストエージェント	エージェントレス
接続は、データを収集して送信するために、Snapshot Manager からホスト VM に RabbitMQ ポート 5671 を介して永続的に設定されます。	次のようにホストでの操作の実行が必要になるたびに、Snapshot Manager は、Linux および Windows の SSH ポートを使用して VM に一時的に接続し、エージェントをインストールします。 ■ 一貫性を保つためのファイルシステムまたはアプリケーションの静止 ■ シングルファイルリストア これにより、必要な操作とアンインストール自体を実行するように、プラグインがプッシュされます。ただし、データは転送されます。
一度手動でインストールされたエージェントは、アンインストールされないかぎり常にホストに残り、オンホストエージェント機能の名前も同様です。	エージェントが常にホスト上に存在するわけではないため、エージェントレス機能の名前も同様です。
接続は 1 回確立され、エージェントが登録解除されてアンインストールされるまで残ります。この方法は、ホストでの操作を実行しているエージェントレス機能に比べて高速です。	ホストで操作を実行するたびに接続を確立する必要があり、各接続用にエージェントまたはプラグインをインストールする必要があります。この方法では、オンホストエージェント機能に比べて時間がかかります。
NetBackup Snapshot Manager をアップグレードする場合は、オンホストエージェントでアップグレードを手動で実行する必要があります。	NetBackup Snapshot Manager がアップグレードされると、アップグレードは NetBackup Snapshot Manager からホストに自動的にプッシュされます。

メモ: 単一ファイルのリストアまたはファイルシステムまたはアプリケーションの一貫性のために、NetBackup でホスト上の資産を検出して保護するには、プロバイダによって管理される一貫性を通じてスナップショットがファイルシステムまたはアプリケーションで一貫性がある場合でも、ホストにエージェントをインストールします。

NetBackup Snapshot Manager のオンホストエージェント機能を使用した資産の保護

NetBackup Snapshot Manager エージェントおよびプラグインをインストールして構成するには、ブラウザの NetBackup ユーザーインターフェースと、ローカルコンピュータまたはアプリケーションホストのコマンドラインインターフェースを使用します。

図 6-1 NetBackup Snapshot Manager エージェントのインストールと構成の処理



p.217 の「NetBackup Snapshot Manager エージェントのダウンロードとインストール」を参照してください。

p.224 の「Windows ベースエージェントのインストールの準備」を参照してください。

p.220 の「Linux ベースエージェントのインストールの準備」を参照してください。

NetBackup Snapshot Manager エージェントのインストールおよび構成

このセクションでは、NetBackup Snapshot Manager エージェントのダウンロード、インストール、および構成の手順を説明します。

NetBackup Snapshot Manager エージェントのダウンロードとインストール

保護するアプリケーションに応じて、適切な NetBackup Snapshot Manager エージェントをダウンロードしてインストールします。Linux ベースのエージェントと Windows ベースのエージェントのどちらをインストールするかにかかわらず、これらの手順は類似しています。

このセクションで説明されている手順を実行する前に、次の操作を行います。

- エージェントをインストールするアプリケーションホストの管理者権限を持っていることを確認してください。
  管理者以外のユーザーがインストールを試みると、インストーラは Windows UAC のプロンプトを表示し、ユーザーは管理者ユーザーのクレデンシャルを指定する必要があります。
- 準備手順を完了し、それぞれのエージェントのすべての依存関係をインストールします。
  p.220 の「Linux ベースエージェントのインストールの準備」を参照してください。
  p.224 の「Windows ベースエージェントのインストールの準備」を参照してください。

エージェントをダウンロードしてインストールするには

1. NetBackup Web UI にサインインします。
2. 左側のナビゲーションペインで、[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択し、次に[NetBackup Snapshot Manager]タブを選択します。
   このペインには、プライマリサーバーに登録されているすべての NetBackup Snapshot Manager サーバーが表示されます。
3. 目的の NetBackup Snapshot Manager サーバーの行で、右側の処理アイコンをクリックし、次に[エージェントの追加 (Add agent)]を選択します。
4. [エージェントの追加 (Add agent)]ダイアログボックスで、[ダウンロード (Download)]リンクをクリックします。
   これにより、新しいブラウザウィンドウが開きます。
   NetBackup Web UI の既存の[エージェントの追加 (Add agent)]ダイアログボックスは、まだ閉じないでください。エージェントを構成するときは、このダイアログボックスに戻って認証トークンを取得できます。
5. 新しい Web ページブラウザウィンドウに切り替えて、[エージェントの追加 (Add Agent)]セクションから、目的の NetBackup Snapshot Manager エージェントインストールパッケージをダウンロードするためのダウンロードリンクをクリックします。
   Web ページには、Linux エージェントおよび Windows エージェントをダウンロードするための個別のリンクがあります。
6. 必要に応じて、エージェントをインストールするアプリケーションホストに、ダウンロードしたエージェントパッケージをコピーします。
7. エージェントをインストールします。
   - Linux/SUSE Linux ベースのエージェントの場合は、Linux/SUSE Linux ホスト上で次のコマンドを入力します。
     ```
     # sudo yum -y install <snapshotmanager_agent_rpm_name>
     ```
     ここで、*<snapshotmanager_agent_rpm_name>* は、以前にダウンロードしたエージェント rpm パッケージの名前です。
     次に例を示します。

```
# sudo yum -y install
VRTSflexsnap-agent-11.1.x.x-xxxx-RHEL.x86_64.rpm
```

- Windows ベースのエージェントの場合、エージェントパッケージファイルを実行し、インストールウィザードのワークフローに従って、Windows アプリケーションホストでエージェントをインストールします。Oracle Cloud Infrastructure は、ホストエージェントで Windows をサポートしていません。

メモ: インストールを許可するには、管理者ユーザーは Windows UAC プロンプトで[はい (Yes)]をクリックする必要があります。管理者以外のユーザーは、UAC プロンプトで管理者ユーザーのクレデンシャルを指定する必要があります。

インストーラは、デフォルトでは `C:¥Program Files¥Veritas¥CloudPoint` にエージェントをインストールします。このパスは変更できません。
または、Windows ホストで次のコマンドを実行して、サイレントモードで Windows ベースのエージェントをインストールすることもできます。

`msiexec /i <installpackagefilepath> /qn`

ここで、<installpackagefilepath> はインストールパッケージの絶対パスです。たとえば、インストーラが `C:¥temp` に保存されている場合、コマンド構文は次のようになります。

`msiexe /i C:¥temp¥VRTSflexsnap-core-<ver>-Windows.x64.msi /qn`

このモードでは、インストールパッケージは UI を表示せず、ユーザー操作も必要としません。エージェントは、デフォルトでは `C:¥Program Files¥Veritas¥CloudPoint` にインストールされ、このパスは変更できません。サードパーティの配備ツールを使用してエージェントのインストールを自動化する場合、サイレントモードのインストールは有効です。

メモ: エージェントバイナリのバージョンは、バイナリ名で 11.1.x.x-xxxx と示されていても 11.1.x.x.xxxx のままです。

---

8 これでエージェントのインストールは完了です。ここから、エージェントの登録に進めます。

p.220 の「Linux ベースのエージェントの登録」を参照してください。

p.224 の「Windows ベースのエージェントの登録」を参照してください。

Linux ベースのエージェント

このセクションでは、次を準備および登録する手順について説明します。

- Linux ベースのエージェント

- SUSE Linux ベースのエージェント
- Oracle Enterprise Linux ベースのエージェント

Linux ベースエージェントのインストールの準備

Oracle アプリケーションを検出するために Linux ベースのエージェントをアプリケーションホストにインストールする場合は、Oracle データベースファイルとメタデータファイルを最適化したことを確認します。

p.236 の「Oracle データベースのデータとメタデータファイルの最適化」を参照してください。

p.216 の「NetBackup Snapshot Manager のオンホストエージェント機能を使用した資産の保護」を参照してください。

Linux ベースのエージェントの登録

Linux ベースのエージェントを登録する前に、次のことを確認します。

- エージェントをアプリケーションホストにダウンロードしてインストールしたことを確認します。
  p.217 の「NetBackup Snapshot Manager エージェントのダウンロードとインストール」を参照してください。
- Linux インスタンスの root 権限を持っていることを確認します。
- NetBackup Snapshot Manager Linux ベースエージェントがすでにホストで構成されていて、同じ NetBackup Snapshot Manager インスタンスでエージェントを再登録する場合は、Linux ホストで次の手順を実行します。
  - Linux ホストから `/opt/keys` ディレクトリを削除します。
    エージェントが実行されているホストで次のコマンドを入力します。
    ```
    # sudo rm -rf /opt/keys
    ```
- NetBackup Snapshot Manager Linux ベースエージェントがすでにホストで登録されていて、別の NetBackup Snapshot Manager インスタンスでエージェントを登録する場合は、Linux ホストで次の手順を実行します。
  - Linux ホストからエージェントをアンインストールします。
    p.306 の「NetBackup Snapshot Manager エージェントの削除」を参照してください。
  - Linux ホストから `/opt/keys` ディレクトリを削除します。
    次のコマンドを入力します。
    ```
    # sudo rm -rf /opt/keys
    ```
  - Linux ホストから `/etc/flexsnap.conf` 構成ファイルを削除します。
    次のコマンドを入力します。
    ```
    sudo rm -rf /etc/flexsnap.conf
    ```

- Linux ホストのエージェントを再インストールします。
  p.217 の「NetBackup Snapshot Manager エージェントのダウンロードとインストール」を参照してください。

これらの手順を実行しないと、オンホストエージェント登録が失敗し、次のエラーが表示されることがあります。

```
On-host registration has failed. The agent is already registered
with Snapshot Manager instance <instance>.
```

- ホストが FIPS に対応していて、NetBackup Snapshot Manager は対応していない場合、またはその逆の場合、オンホストエージェントの登録が失敗することがあります。

Linux ベースのエージェントを登録するには

1. NetBackup Web UI に戻り、[エージェントの追加 (Add agent)]ダイアログボックスで、[トークンの作成 (Create Token)]をクリックします。

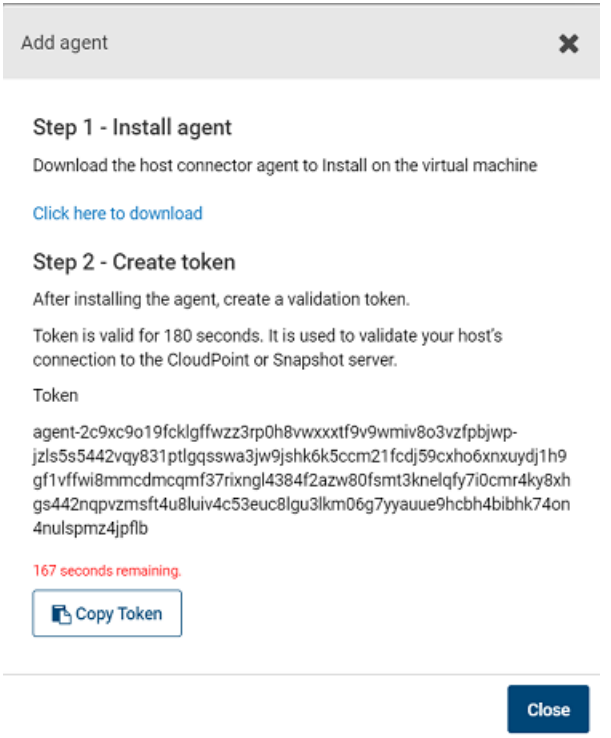
   このダイアログボックスを閉じている場合は、NetBackup Web UI に再びサインインして、次の操作を行います。

   - 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
   - [Snapshot Manager]タブをクリックします。
   - 目的の NetBackup Snapshot Manager サーバー行で、右側の処理ボタンをクリックし、次に[エージェントの追加 (Add agent)]を選択します。

- ［エージェントの追加 (Add agent)］ダイアログボックスで、［トークンの作成 (Create Token)］をクリックします。

2 ［トークンをコピー (Copy Token)］をクリックして、表示された NetBackup Snapshot Manager 検証トークンをコピーします。

トークンは英数字の一意のシーケンスであり、NetBackup Snapshot Manager との間のホスト接続を承認するための認証トークンとして使用されます。



メモ: トークンは 180 秒間のみ有効です。その時間枠内にトークンをコピーしない場合は、新しいトークンを再び生成します。

3 Linux ホストに接続し、次のコマンドを使用してエージェントを登録します。

```
# sudo flexsnap-agent --ip <snapshotmanager_host_FQDN_or_IP>
--token <authtoken>
```

ここで、*<snapshotmanager_host_FQDN_or_IP>* は、NetBackup Snapshot Manager 構成中に指定された NetBackup Snapshot Manager サーバーの FQDN (完全修飾ドメイン名) または IP アドレスです。

<authtoken> は、前の手順でコピーした認証トークンです。

メモ: `flexsnap-agent --help` を使用して、コマンドのヘルプを参照できます。

このコマンドを実行すると、NetBackup Snapshot Manager は次の処理を行います。

メモ: エラーが発生した場合は、`flexsnap-agent` のログを確認し、問題をトラブルシューティングします。

---

4 NetBackup Web UI に戻り、[エージェントの追加 (Add agent)]ダイアログボックスを閉じ、NetBackup Snapshot Manager サーバーの行で右側の処理ボタンをクリックして[検出 (Discover)]をクリックします。

これにより、NetBackup Snapshot Manager サーバーに登録されているすべての資産の手動検出がトリガされます。

5 [仮想マシン (Virtual machines)]タブをクリックします。

エージェントをインストールした Linux ホストが、検出された資産のリストに表示されます。

Linux ホストをクリックして選択します。ホストの状態が[VM 接続済み (VM Connected)]と表示されていて、[アプリケーションの構成 (Configure Application)]ボタンが表示されている場合は、エージェント登録の成功が確認されます。

6 これでエージェントの登録は完了です。これで、アプリケーションプラグインの構成に進めます。

p.227 の「アプリケーションプラグインの構成」を参照してください。

Windows ベースのエージェント

このセクションでは、Windows ベースのエージェントを準備および登録する手順について説明します。

Windows ベースエージェントのインストールの準備

Windows ベースのエージェントをインストールする前に、Windows アプリケーションホストで次の操作を実行します。

- 必要なポートが NetBackup Snapshot Manager ホストで有効になっていることを確認します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。
- リモートデスクトップを介してホストに接続できることを確認します。
- NetBackup Snapshot Manager を使用して保護するドライブまたはボリュームに、`pagefile.sys` が存在していないことを確認します。そのようなドライブにファイルが存在する場合は、そのファイルを代替の場所に移動します。
  `pagefile.sys` が、操作を実行しているのと同じドライブまたはボリューム上に存在する場合、スナップショットのリストアはシャドウコピーを戻すのに失敗します。

Windows ベースのエージェントの登録

Windows ベースのエージェントを登録する前に、次のことを確認します。

- エージェントを Windows アプリケーションホストにダウンロードしてインストールしたことを確認します。
  p.217 の「NetBackup Snapshot Manager エージェントのダウンロードとインストール」を参照してください。
- Windows ホストの管理者権限を持っていることを確認します。

Windows ベースのエージェントを登録するには

1. NetBackup Web UI に戻り、[エージェントの追加 (Add agent)]ダイアログボックスで、[トークンの作成 (Create Token)]をクリックします。

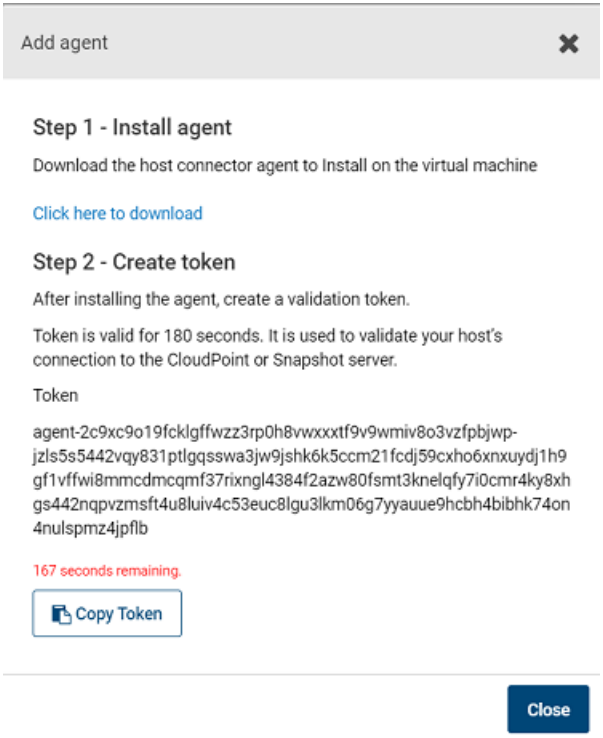
   このダイアログボックスを閉じている場合は、NetBackup Web UI に再びサインインして、次の操作を行います。

   - 左側で[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択します。
     [Snapshot Manager]タブをクリックします。
     目的の NetBackup Snapshot Manager サーバー行で、右側の処理ボタンをクリックし、次に[エージェントの追加 (Add agent)]を選択します。

- ［エージェントの追加 (Add agent)］ダイアログボックスで、［トークンの作成 (Create Token)］をクリックします。

2 ［トークンをコピー (Copy Token)］をクリックして、表示された NetBackup Snapshot Manager 検証トークンをコピーします。

トークンは英数字の一意のシーケンスであり、NetBackup Snapshot Manager との間のホスト接続を承認するための認証トークンとして使用されます。



メモ: トークンは 180 秒間のみ有効です。その時間枠内にトークンをコピーしない場合は、新しいトークンを再び生成します。

3 Windows インスタンスに接続し、エージェントを登録します。

コマンドプロンプトで、エージェントのインストールディレクトリに移動し、次のコマンドを入力します。

```
flexsnap-agent.exe --ip <snapshotmanager_host_FQDN_or_IP> --token <authtoken>
```

デフォルトのパスは <**システムドライブ**>¥Program Files¥Veritas¥CloudPoint¥ です。

ここで、*<snapshotmanager_host_FQDN_or_IP>* は、NetBackup の初期構成中に指定された NetBackup ホストの FQDN (完全修飾ドメイン名) または IP アドレスです。

<authtoken> は、前の手順でコピーした認証トークンです。

メモ: flexsnap-agent.exe --help を使用して、コマンドのヘルプを参照できます。

このコマンドを実行すると、NetBackup は次の処理を行います。

- Windows ベースのエージェントの登録
- Windows インスタンスでの <**システムドライブ**>¥ProgramData¥Veritas¥CloudPoint¥etc¥flexsnap.conf 構成ファイルの作成と、NetBackup ホスト情報を使用したファイルの更新
- Windows ホストでのエージェントサービスの有効化と起動

メモ: スクリプトまたはサードパーティの配備ツールを使用してエージェント登録処理を自動化する場合は、次の点を考慮してください。

エージェントが正常に登録された場合でも、Windows エージェントの登録コマンドが、エラーコード 0 ではなくエラーコード 1 (通常失敗を示す) を返すことがあります。

不正な戻りコードによって、登録が失敗したことを自動化ツールが誤って示すことがあります。このような場合、flexsnap-agent-onhost ログまたは NetBackup Web UI のいずれかでエージェントの登録状態を確認する必要があります。

ユーザーに次の警告が表示される場合がありますが、無視できます。

```
InsecureRequestWarning: Unverified HTTPS request is being made
to host '10.244.176.175'. Adding certificate verification is
strongly advised. See:
https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
```

しばらくしてからエージェントが登録されます。

4 NetBackup Web UI に戻り、[エージェントの追加 (Add agent)]ダイアログボックスを閉じ、NetBackup Snapshot Manager サーバーの行で右側の処理ボタンをクリックして[検出 (Discover)]をクリックします。

これにより、NetBackup Snapshot Manager サーバーに登録されているすべての資産の手動検出がトリガされます。

5 [仮想マシン (Virtual machines)]タブをクリックします。

エージェントをインストールした Windows ホストが、検出された資産のリストに表示されます。

Windows ホストをクリックして選択します。ホストの状態が[VM 接続済み (VM Connected)]と表示されていて、[アプリケーションの構成 (Configure Application)]ボタンが表示されている場合は、エージェント登録の成功が確認されます。

6 これでエージェントの登録は完了です。これで、アプリケーションプラグインの構成に進めます。

p.227 の「アプリケーションプラグインの構成」を参照してください。

NetBackup Snapshot Manager アプリケーションプラグインの構成

NetBackup Snapshot Manager エージェントをアプリケーションホストにインストールして登録した後、次の手順ではホストでアプリケーションプラグインを構成します。

メモ: Microsoft SQL Server は Oracle Cloud Infrastructure (OCI) ではサポートされません。Oracle プライベートクラウドアプライアンス (PCA) は、アプリケーションプラグインをサポートしません。

先に進む前に、以下のことを確認します。

- ホストにエージェントを構成したことを確認します。
  p.220 の「Linux ベースのエージェントの登録」を参照してください。
  p.224 の「Windows ベースのエージェントの登録」を参照してください。
- 構成するプラグインの構成要件を確認します。
  p.235 の「Oracle プラグインの構成に関する要件」を参照してください。
  p.228 の「Microsoft SQL プラグインの構成に関する要件」を参照してください。

アプリケーションプラグインの構成

アプリケーションプラグインを構成するには

1 NetBackup Web UI にサインインし、左側のナビゲーションペインで、[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択してから[仮想マシン (Virtual machines)]タブを選択します。

2 資産のリストから、NetBackup Snapshot Manager エージェントをインストールして登録したアプリケーションホストを検索します。

アプリケーションホストをクリックして選択し、上部のバーに[アプリケーションの構成 (Configure application)]ボタンが表示されることを確認します。

3 [アプリケーションの構成 (Configure application)]をクリックして、ドロップダウンリストから、構成するアプリケーションプラグインを選択し、[構成 (Configure)]をクリックします。

たとえば、Microsoft SQL 用の NetBackup Snapshot Manager プラグインを構成する場合は、[Microsoft SQL Server]を選択します。

4 プラグインが構成された後、資産の検出サイクルをトリガします。

[Snapshot Manager]タブをクリックして、目的の NetBackup Snapshot Manager サーバーの行の右側にある処理ボタンをクリックし、次に[検出 (Discover)]をクリックします。

5 検出が完了したら、[仮想マシン (Virtual machines)]タブをクリックして、アプリケーションホストの状態を確認します。資産のペインの[アプリケーション (Application)]列に値[構成済み (Configured)]が表示されたら、プラグインの構成が成功したことが確認されます。

6 [アプリケーション (Applications)]タブをクリックして、アプリケーション資産が資産リストに表示されていることを確認します。

たとえば、Microsoft SQL プラグインを構成した場合、[アプリケーション (Applications)]タブには、プラグインを構成したホスト上で実行されている SQL Server インスタンス、データベース、SQL AG (可用性グループ) データベースが表示されます。

これらの資産を選択し、保護計画を使用して保護を開始できるようになりました。

Microsoft SQL プラグイン

Microsoft SQL 用 NetBackup Snapshot Manager プラグインを構成して、SQL アプリケーションのインスタンスとデータベースを検出し、ディスクレベルのスナップショットを使用してそれらを保護できます。プラグインを構成した後、NetBackup Snapshot Manager は、SQL Server ホストで構成されているすべてのファイルシステム資産、SQL インスタンスおよびデータベースを自動的に検出します。検出された SQL 資産は、NetBackup UI (ユーザーインターフェース) に表示され、ここから、保護計画にサブスクライブして、または手動でスナップショットを取得して資産を保護できます。

Microsoft SQL プラグインの構成に関する要件

プラグインを構成する前に、環境が次の要件を満たしていることを確認します。

- このプラグインは、Microsoft Azure、Google Cloud Platform、および Amazon AWS 環境でサポートされます。
- サポート対象バージョンの Microsoft SQL Server が Windows インスタンスにインストールされています。
  p.19 の「 システム要件への準拠」を参照してください。

- 保護する SQL Server インスタンスがシステムドライブ以外のドライブで実行されている必要があります。
  NetBackup Snapshot Manager は、マウントポイントにインストールされている SQL Server インスタンスもサポートしません。
- NetBackup Snapshot Manager は、Microsoft VSS (ボリュームシャドウコピーサービス) を使用します。
  シャドウコピーをデータベースが存在するドライブと同じドライブ (元のドライブ) に保存するように VSS を構成していることを確認します。
  p.250 の「元のドライブのシャドウコピーを格納するための VSS の構成」を参照してください。

Microsoft SQL Server のリストアの要件および制限事項

SQL Server スナップショットをリストアする前に、次の点を考慮してください。

- SQL Server スナップショットをリストアする前に、SQL Management Studio を閉じていることを確認します。
  これは、現在の資産を置き換えてスナップショットをリストアする場合 (既存のものを上書きするオプション)、または元の資産と同じ場所にスナップショットをリストアする場合 (元の場所のオプション) にのみ該当します。
- ターゲットホストが接続または構成されている場合、SQL インスタンスのディスクレベルの新しい場所へのリストアは失敗します。
  このような場合に SQL Server スナップショットの新しい場所へのリストアを正常に完了するには、次の順序でリストアを実行する必要があります。
  - まず、SQL Server のディスクレベルのスナップショットリストアを実行します。
    SQL Server によって使用されているすべてのディスクのディスクスナップショットをリストアしていることを確認します。これらは、SQL Server データが格納されているディスクです。
    p.230 の「SQL AG データベースをリストアする前に必要な手順」を参照してください。
  - その後、ディスクレベルのリストアが成功したら、追加の手動の手順を実行します。
    p.231 の「SQL Server インスタンススナップショットのリストア後に必要な追加手順」を参照してください。
- NetBackup Snapshot Manager では、先頭または末尾に空白または印字不可能な文字を含む SQL データベースの検出、スナップショット、およびリストア操作はサポートされません。これは、VSS ライターがそのようなデータベースに対してエラー状態になるためです。
  詳しくは次を参照してください。
  Microsoft SQL Server データベースのマニュアル
- SQL AG (可用性グループ) データベースをリストアする前に、次のリストア前の手順を手動で実行します。

p.230 の「SQL AG データベースをリストアする前に必要な手順」を参照してください。

- システムデータベースの新しい場所のリストアはサポートされていません。
- 宛先インスタンスに AG が構成されている場合、リストアはサポートされません。
- データベースが新しい場所の宛先に存在し、既存のデータの上書きオプションが選択されていない場合、リストアジョブは失敗します。
- AG の一部であるデータベースに対して既存の上書きオプションが選択されている場合、リストアジョブは失敗します。
- システムデータベースのリストアの場合、SQL Server のバージョンは同じである必要があります。ユーザーデータベースの場合、上位の SQL バージョンから下位バージョンにはリストアできません。
- デフォルトの 6 時間のタイムアウトでは、大きいデータベース (サイズが 300 GB を超える) のリストアは許可されません。より大きいデータベースをリストアできるように、構成可能なタイムアウトパラメータ値を設定できます。
  p.315 の「NetBackup Snapshot Manager のトラブルシューティング」を参照してください。

SQL AG データベースをリストアする前に必要な手順

SQL AG (可用性グループ) データベースをリストアする前に、次の手順を実行する必要があります。

メモ: AG データベースを複数のレプリカにリストアする場合は、最初にプライマリレプリカでリストア処理全体を実行してから、各セカンダリレプリカに対して手順を繰り返します。

---

1. リストアするデータベースで、レプリカからのデータの移動を中断します。

   SQL Server Management Studio で、データベースを右クリックして[データの移動を一時停止 (Suspend Data Movement)]を選択します。

2. レプリカの AG からデータベースを削除します。

   SQL Server Management Studio で、データベースを右クリックして[可用性グループからデータベースを削除 (Remove Database from Availability Group)]を選択します。

   データベースが AG の一部ではなくなったことを確認します。プライマリレプリカのデータベースが同期モードではなくなり、セカンダリレプリカの対応するデータベースの状態が[(リストア中...) ((Restoring...))]と表示されることを確認します。

3. レプリカからデータベースを削除します。

   SQL Server Management Studio で、データベースを右クリックして[削除 (Delete)]を選択します。

SQL AG データベースをリストアした後に必要な追加手順

SQL AG (可用性グループ) データベースをリストアした後に、次の手順を実行する必要があります。

メモ: AG データベースを複数のレプリカにリストアする場合は、最初にプライマリレプリカでリストア処理全体を実行してから、各セカンダリレプリカに対して手順を繰り返します。

- リストアされたデータベースをプライマリレプリカの AG に追加します。
  SQL Server Management Studio で、AG エントリを右クリックして[データベースの追加 (Add Database)]を選択します。ウィザードのワークフローで、データベースを選択し、[初期データ同期 (Initial Data Synchronisation)]ページで、[最初のデータの同期をスキップ (Skip Initial Data Synchronization)]オプションを選択します。必要条件に応じて、その他のオプションを選択できます。

同じデータベースをセカンダリレプリカにリストアする場合は、次の手順を実行します。

1. 「リカバリされていない」状態のセカンダリ SQL インスタンスにデータベースをリストアします。リカバリなしのリストアが正常に実行されます。
2. セカンダリレプリカの AG にデータベースを結合します。

   SQL Server Management Studio で、セカンダリレプリカノードに接続して、データベースを右クリックして[可用性グループに結合 (Join Availability Group)]を選択します。

   セカンダリレプリカのデータベースの状態が、[**リストア中...** (Restoring...)]から[**同期済み** (Synchronized)]に変更されたことを確認します。これは、AG データベースのスナップショットのリストアが成功したことを示します。

AG データベースをリストアする各レプリカに対して、これらの手順を繰り返す必要があります。

SQL Server インスタンススナップショットのリストア後に必要な追加手順

NetBackup UI (ユーザーインターフェース) から SQL Server インスタンススナップショットをリストアした後、次の手順が必要になります。リストア操作が正常に実行された場合でも、これらの手順は、通常の用途でアプリケーションデータベースを再び利用できるようにするために必要です。

SQL Server のホストレベルのリストア後に必要な手順

NetBackup UI からホストレベルの SQL Server スナップショットをリストアした後に、これらの手順を実行します。これらの手順は、スナップショットを元の場所にリストアするか、新しい場所にリストアするかに関係なく必要になります。

続行する前に、次のことを確認します。

- シャドウコピーを戻す予定の Windows ホスト上の SQL Server ユーザーアカウントに、リストアデータへのフルアクセス権があることを確認します。
- スナップショットの作成またはスナップショットのリストア用に選択したドライブに、`pagefile.sys` が存在しないことを確認します。
  ファイルが選択したドライブに存在する場合、スナップショットの作成とスナップショットのリストア操作は失敗します。

シャドウコピーを戻すために実行する手順

1. SQL Server インスタンスが実行されている Windows ホストに接続します。
   ホストで管理者権限を持つアカウントを使用していることを確認します。
2. Windows ホストで SQL Server サービスを停止します。
3. コマンドプロンプトウィンドウを開きます。Windows UAC がホストで有効になっている場合は、管理者として実行モードでコマンドプロンプトを開きます。
4. `%programdata%¥Veritas¥CloudPoint¥tmp¥tools¥windows¥tools¥` ディレクトリに移動し、そこから次のコマンドを実行します。

   ```
   vss_snapshot.exe  --revertSnapshot
   ```

   このコマンドは、状態が 0 の json 出力を表示します。これで、操作が成功したことを確認します。

   このコマンドは、システムドライブを除くすべてのドライブのシャドウコピーを元に戻します。SQL Server サービスは、スナップショットが戻される前に停止し、復帰操作が成功した後に自動的に起動されます。
5. Windows ホストで SQL Server サービスを開始します。

SQL Server インスタンスのディスクレベルのスナップショットを新しい場所にリストアした後に必要な手順

NetBackup UI からディスクレベルの SQL Server インスタンススナップショットをリストアした後に、これらの手順を実行します。これらの手順は、スナップショットが新しい場所にリストアされる場合にのみ必要です。新しい場所とは、SQL インスタンスが実行されているホストとは異なる新しいホストを指します。

メモ: これらの手順は、SQL Server インスタンスのスナップショットが新しい場所にリストアされる場合にのみ適用できます。これらは SQL Server データベースのスナップショットのリストアには適用されません。

ホストに接続されている新しいディスクの読み取り専用モードを解除します。

実行する手順

1. SQL Server インスタンスが実行されている新しい Windows ホストに接続します。

   ホストで管理者権限を持つアカウントを使用していることを確認します。

2. コマンドプロンプトウィンドウを開きます。Windows UAC がホストで有効になっている場合は、管理者として実行のモードでコマンドプロンプトを開きます。

3. 次のコマンドを使用して、diskpart ユーティリティを起動します。

   ```
   diskpart
   ```

4. 次のコマンドを使用して、新しいホストのディスクのリストを表示します。

   ```
   list disk
   ```

   スナップショットのリストア操作によって接続された新しいディスクを識別し、ディスク番号を書き留めます。これは、次の手順で使用します。

5. 次のコマンドを使用して、目的のディスクを選択します。

   ```
   select disk <disknumber>
   ```

   ここで、<disknumber> は、前の手順でメモしたディスクを表します。

6. 次のコマンドを使用して、選択したディスクの属性を表示します。

   ```
   attributes disk
   ```

   出力には、ディスクの属性のリストが表示されます。属性の 1 つは `read-only` で、次の手順で変更します。

7. 次のコマンドを使用して、選択したディスクの読み取り専用属性を変更します。

   ```
   attributes disk clear readonly
   ```

   このコマンドを実行すると、ディスクが読み書きモードに変更されます。

8. ディスクをオンラインにします。

   Windows Server マネージャコンソールから、[ファイルとストレージデバイス (Files and Storage Devices)]、[ディスク (Disks)]の順に移動し、新しく接続したディスクを右クリックして[オンラインにする (Bring online)]を選択します。

9. 前の手順でオンラインにしたディスク上のボリュームにドライブ文字を割り当てます。ドライブ文字は、ディスクの各ボリュームに関連付けられているシャドウコピーを表示するために必要です。

   コマンドプロンプトウィンドウに戻って、次の手順を実行します。

   - 次のコマンドを使用して、新しいホストのボリュームのリストを表示します。

     ```
     list volume
     ```

表示されたボリュームのリストから、ドライブ文字を割り当て、変更、または削除するボリュームを識別します。

- 次のコマンドを使用して、目的のボリュームを選択します。

  ```
  select volume <volnumber>
  ```

  ここで、<volnumber> は、前の手順でメモしたボリュームを表します。

- 次のコマンドを使用して、選択したボリュームにドライブ文字を割り当てます。

  ```
  assign letter=<driveletter>
  ```

  ここで、<driveletter> は、ボリュームに割り当てるドライブ文字です。指定したドライブ文字が、すでに別のボリュームによって使用されていないことを確認します。

- ディスク上のすべての SQL Server ボリュームにドライブ文字を割り当てるには、これらの手順を繰り返します。

10 次のコマンドを使用して、diskpart ユーティリティを終了します。

```
exit
```

コマンドプロンプトをまだ閉じないでおきます。同じウィンドウを使用して、次のセクションで説明されている残りの手順を実行できます。

Microsoft DiskShadow ユーティリティを使用してシャドウコピーを戻す

実行する手順

1 以前使用していたものと同じコマンドウィンドウから、次のコマンドを使用して、対話モードで diskshadow コマンドインタプリタを起動します。

```
diskshadow
```

2 新しいホストに存在するすべてのシャドウコピーのリストを表示します。次のコマンドを入力します。

```
list shadows all
```

復帰操作に使用するシャドウコピーを特定し、シャドウコピー ID を書き留めます。シャドウ ID は、次の手順で使用します。

3 次のコマンドを使用して、目的のシャドウコピーにボリュームを戻します。

```
revert <shadowcopyID>
```

ここで、<shadowcopyID> は、前の手順でメモしたシャドウコピー ID を示します。

4 次のコマンドを使用して、DiskShadow ユーティリティを終了します。

```
exit
```

インスタンスデータベースへの .mdf および .ldf ファイルの接続

次の手順を実行します。

1. ディスクレベルのスナップショットリストア操作が正常に完了し、新しいディスクが作成され、アプリケーションホストにマウントされていることを確認します。
2. データベース管理者として Microsoft SQL Server Management Studio にログオンします。
3. オブジェクトエクスプローラから、SQL Server データベースエンジンのインスタンスに接続し、クリックしてインスタンスのビューを展開します。
4. 展開したインスタンスビューで、[データベース (Databases)]を右クリックし、[接続 (Attach)]をクリックします。
5. [データベースの接続 (Attach Databases)]ダイアログボックスで、[追加 (Add)]をクリックし、次に[データベースファイルの検索 (Locate Database Files)]ダイアログボックスで、データベースを含むディスクドライブを選択し、そのデータベースに関連付けられているすべての .mdf ファイルと .ldf ファイルを見つけて選択します。次に[OK]をクリックします。

   選択したディスクドライブは、ディスクレベルのスナップショットのリストア操作によって新しく作成されたドライブです。
6. 要求された操作が完了するまで待機してから、データベースが利用可能で、NetBackup で正常に検出されたことを確認します。

Oracle プラグイン

Oracle データベースアプリケーションを検出して、ディスクレベルのスナップショットで保護するように Oracle プラグインを構成できます。

Oracle プラグインの構成に関する要件

Oracle プラグインを構成する前に、環境が次の要件を満たしていることを確認します。

- サポート対象バージョンの Oracle が、サポート対象の RHEL (Red Hat Enterprise Linux) または OEL (Oracle Enterprise Linux) ホスト環境にインストールされています。
  p.19 の「 システム要件への準拠」を参照してください。
- Oracle スタンドアロンインスタンスを検出できます。
- Oracle バイナリと Oracle データは、別のボリュームに存在する必要があります。
- ログのアーカイブが有効です。
- `db_recovery_file_dest_size` パラメータのサイズは、Oracle の推奨事項に従って設定されています。

詳しくは、Oracle 社のバックアップとリカバリの基本に関するドキュメントを参照してください。

- データベースが実行中で、マウントされており、開いています。
- NetBackup Snapshot Manager は、バックアップモードのデータベースでの検出とスナップショット操作をサポートします。スナップショットを取得した後、データベースの状態はそのまま保持されます。NetBackup Snapshot Manager は、このようなデータベースの状態は変更しません。ただし、そのようなデータベースのインプレースリストアはサポートされません。

Oracle データベースのデータとメタデータファイルの最適化

Cohesity では、ブートディスクまたはルートディスク上に Oracle 構成ファイルを保存しないことをお勧めします。これらのファイルを移動して Oracle インストールを最適化する方法について詳しくは、次の情報を参照してください。

Cohesity は、ディスクのスナップショットを取得します。より優れたバックアップとリカバリのために、Oracle データベースのデータとメタデータファイルを最適化する必要があります。

各 Oracle データベースインスタンスには、制御ファイルがあります。制御ファイルには、各トランザクションのデータベースの管理についての情報が含まれています。高速かつ効率的なバックアップとリカバリのために、Oracle は、データベースの REDO ログファイルと同じファイルシステムに制御ファイルを配置することを推奨しています。データベース制御ファイルがブートディスクまたはルートディスクの上に作成されたファイルシステムに存在する場合は、データベース管理者に連絡して、制御ファイルを適切な場所に移動してください。

制御ファイルとその移動方法について詳しくは、データベース管理者に問い合わせるか、Oracle のマニュアルを参照してください。

アプリケーションをリストアするためにスナップショットを使用した後は、操作を実行しないでください。Oracle が新しいデータを読み込み、データベースを起動するためにしばらく時間がかかります。データベースが起動しない場合は、データベース管理者に連絡して、問題の原因を判断してください。

Oracle のリストアの要件および制限事項

Oracle スナップショットをリストアする前に次の点を考慮します。

- スナップショットをリストアする宛先ホストには、ソースと同じバージョンの Oracle がインストールされている必要があります。
- 新しい場所にスナップショットをリストアする場合は、次のことを確認します。
  - ターゲットホストで同じインスタンス名のデータベースが実行されていないことを確認します。

- アプリケーションファイルをマウントするために必要なディレクトリが、ターゲットホストですでに使用されていないことを確認します。

- ターゲットホストで Oracle 向けの NetBackup プラグインが構成されていない場合、ディスクレベルの新しい場所へのリストアは失敗します。
  このような場合に Oracle スナップショットの新しい場所へのリストアを正常に完了するには、次の順序でリストアを実行する必要があります。
  - まず、Oracle のディスクレベルのスナップショットリストアを実行します。
    Oracle によって使用されているすべてのディスクのディスクスナップショットをリストアしていることを確認します。これらは、Oracle データが格納されているディスクです。
  - その後、ディスクレベルのリストアが成功したら、追加の手動の手順を実行します。
    p.237 の「Oracle スナップショットのリストア後に必要な追加手順」を参照してください。

- Azure 環境では、ホストレベルのリストア操作の実行後にデバイスマッピングが変更されることがあります。その結果、リストア後に、新しいインスタンスで Oracle アプリケーションがオンラインになることができなくなる場合があります。
  リストア後のこの問題を解決するには、ファイルシステムを手動でマウント解除してから、元のホストのマッピングに従って再びマウントする必要があります。
  `/etc/fstab` ファイルを使用してファイルシステム、マウントポイント、マウント設定を格納している場合、Cohesityでは、デバイスマッピングの代わりにディスク UUID を使用することをお勧めします。ディスク UUID を使用すると、それぞれのマウントポイントにファイルシステムが正しくマウントされるようになります。

- LVM タイプのパーティションの一部であるファイルシステムに存在するアプリケーションデータのスナップショットはサポートされません。このようなファイルシステムのスナップショットを作成しようとすると、次のエラーが表示されます。
  `*flexsnap.GenericError: 資産を保護できません* (*flexsnap.GenericError: Unable to protect asset *)`

Oracle スナップショットのリストア後に必要な追加手順

Oracle スナップショットをリストアした後、次の手順を実行する必要があります。リストア操作自体が正常に実行された場合でも、これらの手順は、通常の用途でアプリケーションデータベースを再び利用できるようにするために必要です。

これらの手動の手順は、次のシナリオでディスクレベルのリストアを行う場合には必要ありません。

- 元の場所または代替の場所へのディスクレベルのリストアを実行している
- ターゲットホストが NetBackup Snapshot Manager ホストに接続されている
- NetBackup Snapshot Manager Oracle プラグインがターゲットホストに構成されている

次の手順を実行します。

1. スナップショットリストア操作が正常に完了し、新しいディスクが作成され、アプリケーションホストにマウントされていること (ディスクレベルのリストアの場合)、またはアプリケーションホストが起動し実行されていること (ホストレベルのリストアの場合) を確認します。
2. 仮想マシンに接続してから、データベース管理者 (sysdba) として Oracle データベースにログオンします。
3. 次のコマンドを使用して、マウントモードで Oracle データベースを起動します。

   ```
   # STARTUP MOUNT
   ```

   データベースが正常にマウントされたことを確認します。
4. 次のコマンドを使用して、Oracle データベースのバックアップモードを解除します。

   ```
   # ALTER DATABASE END BACKUP
   ```
5. 次のコマンドを使用して、通常の使用のために Oracle データベースを開きます。

   ```
   # ALTER DATABASE OPEN
   ```
6. 新しく作成されたデータベースのエントリを Oracle `listerner.ora` および `tnsnames.ora` ファイルに追加します。
7. 次のコマンドを使用して、Oracle リスナーを再起動します。

   ```
   # lsnrctl start
   ```

NetBackup Snapshot Manager のエージェントレス機能を使用した資産の保護

NetBackup でホスト上の資産を検出して保護する場合に、ホストのベンダーソフトウェアの占有域を最小限にするときは、NetBackup Snapshot Manager のエージェントレス機能を検討します。通常、エージェントを使用すると、ソフトウェアは常にホストに残ります。一方、エージェントレス機能は次のように動作します。

- NetBackup Snapshot Manager ソフトウェアは、Linux と Windows で SSH を介してホストにアクセスします。
- NetBackup Snapshot Manager は、スナップショットの作成など、指定したタスクを実行します。
- タスクが完了すると、NetBackup Snapshot Manager ソフトウェアによってプロセスが停止されます。

現在、NetBackup Snapshot Manager エージェントレス機能は Windows または Linux ファイルシステム資産、Oracle Database、および Microsoft SQL データベース資産を検出して操作します。

NetBackup Snapshot Manager エージェントレス機能は、FIPS 対応の NetBackup Snapshot Manager 配備でサポートされるようになりました。

NetBackup Snapshot Manager エージェントレス機能は、Oracle PCA ではサポートされていません。

p.239 の「エージェントレス構成の前提条件」を参照してください。

p.241 の「エージェントレス機能の構成」を参照してください。

エージェントレス構成の前提条件

Linux でエージェントレス機能を使用する場合の前提条件

- 次の情報を確認します。
  - ホストユーザー名
  - ホストパスワードまたは SSH 鍵

  NetBackup Snapshot Manager では、ホストへのアクセス権を取得し、要求された操作を実行するために、これらの詳細が必要です。
- この機能を構成するホストで、NetBackup Snapshot Manager に提供するホストユーザーアカウントにパスワードなしの sudo アクセス権を付与します。

メモ: SSH を介してリモートでログインするには、ユーザーはシステムアカウントまたはサービスアカウントではなく、通常のユーザーアカウントである必要があります。

ホストユーザーアカウントへのパスワードなしの sudo アクセス権の付与

NetBackup Snapshot Manager では、ホストのユーザーアカウントに、ホストに接続して操作を実行することを要求します。NetBackup Snapshot Manager に提供するユーザーアカウントには、パスワードなしの sudo アクセス権を付与する必要があります。これは、エージェントレス機能を構成するすべてのホストに必要です。

メモ: 次の手順は一般的なガイドラインとして提供されています。パスワードなしの sudo アクセス権をユーザーアカウントに付与する方法について詳しくは、オペレーティングシステムまたは配布に固有のマニュアルを参照してください。

---

1. エージェントレス機能を構成するホストで次の手順を実行します。
2. NetBackup Snapshot Manager に指定するホストのユーザー名が、`wheel` グループに含まれることを確認します。

   root ユーザーとしてログオンし、次のコマンドを実行します。

```
# usermod -aG wheel hostuserID
```

ここで、*hostuserID* は、NetBackup Snapshot Manager に提供するホストのユーザー名です。

3. 変更を有効にするには、ログアウトして再度ログオンします。
4. visudo コマンドを使用して、/etc/sudoers ファイルを編集します。

```
# sudo visudo
```

5. /etc/sudoers ファイルに次のエントリを追加します。

```
hostuserID ALL=(ALL) NOPASSWD: ALL
```

6. /etc/sudoers ファイルで、次のように wheel グループのエントリを編集します。
   - 次の行エントリをコメントアウト (行の先頭に # 文字を追加) します。
     #% wheel ALL = (all) ALL
   - 次の行エントリのコメントアウトを解除 (行の先頭の # 文字を削除) します。
     % wheel ALL = (ALL) NOPASSWD: ALL

   変更は次のように表示されます。

```
## Allows people in group wheel to run all commands
# %wheel ALL=(ALL) ALL

## Same thing without a password
%wheel ALL=(ALL) NOPASSWD: ALL
```

7. 変更を /etc/sudoers ファイルに保存します。
8. NetBackup Snapshot Manager に指定したユーザーアカウントを使用して、ログアウトしてホストに再度ログオンします。
9. 次のコマンドを実行して、変更が有効であることを確認します。

```
# sudo su
```

パスワードの入力を求めるメッセージが表示されない場合は、ユーザーアカウントにパスワードなしの sudo アクセス権が付与されています。

これで、NetBackup Snapshot Manager エージェントレス機能の構成に進めます。

Windows でエージェントレス機能を使用する場合の前提条件

- Windows VM に OpenSSH サーバーをインストールして有効にします。
  Windows に OpenSSH サーバーをインストールしてサービスを起動する手順について詳しくは、Microsoft 社のマニュアルを参照してください。
- Windows VM のセキュリティグループとファイアウォールからポート 22 を有効にします。

前述の手順で OpenSSH サーバーをインストールして有効にすると、ポート 22 はデフォルトで有効になります。

- Powershell バージョン 5.1 以降がインストールされている必要があります。
- (オプション) ユーザーが WMI/SMB ポートを有効にしていて、他のどのアプリケーションでも使用されていない場合は、NetBackup Snapshot Manager バージョン 10.4 以降にアップグレードした後、セキュリティグループとファイアウォールルールからこれらのポートを無効にすることができます。

メモ: エージェントレス機能は Microsoft Windows バージョン 2019 以降でサポートされます。

制限事項

- Windows OS を搭載したホストは、エージェントレスとホストエージェントの OCI ではサポートされません。

エージェントレス機能の構成

NetBackup Snapshot Manager エージェントレス機能を構成する前に、すべての前提条件を確認します。

p.239 の「エージェントレス構成の前提条件」を参照してください。

エージェントレス機能を構成するには

1. NetBackup Web UI にサインインし、左側のナビゲーションペインで、[作業負荷 (Workloads)]、[クラウド (Cloud)]の順に選択してから[仮想マシン (Virtual machines)]タブを選択します。
2. 資産のリストから、エージェントレス機能を使用するホストを検索します。

   メモ: 現在、NetBackup Snapshot Manager エージェントレス機能は Windows または Linux ファイルシステム資産、Oracle Database、および MS SQL データベース資産を検出して操作します。

3. ホストをクリックして選択し、上部のバーで[接続 (Connect)]をクリックします。

メモ: VM にクレデンシャルを割り当てていない場合は、VM に接続する前にクレデンシャルを割り当てるようプロンプトが表示されます。『Web UI 管理者ガイド』の「クレデンシャルの管理」セクションを参照してください。

NetBackup Snapshot Manager のアップグレード後のエージェントレス機能の構成

ユーザーは OpenSSH サーバーをインストールして有効にし、セキュリティグループとファイアウォールからポート 22 を有効にする必要があります。

すでに接続状態だったクラウド資産は、アップグレード後も引き続き動作します。すでに接続状態にある Linux エージェントレスインスタンスの資産のクレデンシャルを変更する場合は、クレデンシャル管理から資産のクレデンシャルを関連付け、更新する必要があります。

7

Snapshot Manager for Cloud カタログのバックアップとリカバリ

この章では以下の項目について説明しています。

スクリプトの使用について

`/cloudpoint` フォルダが破損している、または NetBackup Snapshot Manager VM が破棄された場合は、`flexsnap_configure backup/recover` コマンドを使用して NetBackup Snapshot Manager をリカバリできます。

コマンドの使用方法:

- 次のコマンドを実行して、NetBackup Snapshot Manager メタデータのバックアップを作成します。

  ```
  # flexsnap_configure backup
  ```

- 次のコマンドを実行して、Snapshot Manager の新規インストール後に NetBackup Snapshot Manager のメタデータをリカバリします。

  ```
  # flexsnap_configure recover --backup-file <path_of_backup_file>
  ```

NetBackup Snapshot Manager データのバックアップ

スクリプトを使用した NetBackup Snapshot Manager データのバックアップ

1. `flexsnap_configure backup` コマンドを実行するための root 権限をユーザーに付与します。
2. コマンドの実行後、tar ファイルが作成されます。
3. 作成した tar ファイルを NetBackup Snapshot Manager VM 以外の場所に保存します。これはリカバリ中に必要です。
4. クラウドプロバイダの追加後にコマンドを実行します。

メモ: バックアップ後に新しいストレージアレイ構成が追加された場合、NetBackup Web UI でのリカバリ後にプラグインは無効になります。

NetBackup Snapshot Manager データのリカバリ

スクリプトを使用した NetBackup Snapshot Manager データのリカバリ

1. tar ファイルを使用して NetBackup Snapshot Manager メタデータをリカバリしている間に、NetBackup Snapshot Manager を再インストールして、recover オプションを使用して tar ファイルを使用します。

   例: `flexsnap_configure recover --backup-file <tar file>`
2. ディザスタリカバリ後の NetBackup Snapshot Manager の再インストール時に、同じホスト名 (FQDN) を使用していることを確認します。
3. 再インストール中に、NetBackup Web UI からホストに対して生成した再発行トークンを指定して、以前に使用したポート番号と同じポート番号を使用していることを確認します。
4. すべての構成手順 (`/cloudpoint/openv/etc/hosts` にホストエントリを追加するなど) は、新しい NetBackup Snapshot Manager VM で再度実行する必要があります。
5. (NetBackup プライマリサーバーのバージョンが 10.4 以降でない場合にのみ必要) NetBackup Snapshot Manager を、NetBackup で再発行トークンを使用して再登録する必要があります。
6. オンホストとエージェントレスホストの両方の既存のエージェントをリカバリして接続するには、次の手順を実行します。

- オンホストエージェントの場合、エージェントを更新するには、次のコマンドを実行します。

  Linux の場合

  ```
  /opt/VRTScloudpoint/bin/flexsnap-agent --renew --token
  <auth_token>
  ```

  Windows の場合

  ```
  "c:¥ProgramFiles¥Veritas¥CloudPoint¥flexsnap-agent.exe" --renew
  --token <auth_token>
  ```

  この手順は、エージェントレス接続では必要ありません。

- Linux オンホストエージェントを再起動し、次のコマンドを実行します。

  ```
  sudo systemctl restart flexsnap-agent.service
  ```

  この手順は、エージェントレス接続では必要ありません。

- Web UI から NetBackup Snapshot Manager のプラグインレベルの検出を実行して、エージェントレスおよびオンホストのエージェント資産を検出します。
- Web UI から NetBackup Snapshot Manager の検出を実行して、エージェントレスおよびオンホストのエージェント資産を取得して表示します。
- (オプション) バックアップが失敗した場合は、NetBackup Snapshot Manager を再起動して、次のコマンドを実行します。

  ```
  flexsnap-configure restart
  ```

リカバリ手順に従うと、NetBackup Snapshot Manager は正常に動作します。以前のスナップショットまたはバックアップコピーを使用して資産をリカバリすることもできます。

8

NetBackup Snapshot Manager for Cloud 資産の保護

この章では以下の項目について説明しています。

NetBackup 保護計画

保護計画は、バックアップを実行するタイミング、バックアップの保持期間、使用するストレージ形式を定義します。保護計画を設定したら、その保護計画に資産をサブスクライブできます。

クラウド資産に対する NetBackup 保護計画の作成

保護計画の管理について詳しくは、『NetBackup Web UI バックアップ管理者ガイド』を参照してください。

NetBackup 保護計画へのクラウド資産のサブスクライブ

1 つの資産または資産のグループを、保護計画にサブスクライブできます。たとえば、週単位のスナップショットを作成し、ポリシーをすべてのデータベースアプリケーションに割り当てる計画を作成できます。また、1 つの資産に複数のポリシーを設定することもできます。たとえば、週次のスナップショットに加えて、月次のスナップショットを取得するために 2 番目のポリシーをデータベースアプリケーションに割り当てることができます。

NetBackup は、同種のクラウド資産のサブスクリプションをサポートします。保護計画に資産をサブスクライブする際、資産のクラウドプロバイダは、保護計画で定義されているクラウドプロバイダと同じである必要があります。

続行する前に、NetBackup Web UI から保護計画に資産を割り当てるための十分な権限を持っていることを確認します。

保護計画にクラウド資産をサブスクライブするには

1. NetBackup Web UI にサインインします。
2. 左側のナビゲーションペインで、[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックし、次に[アプリケーション (Applications)]タブを選択します。

   [アプリケーション (Application)]タブには、保護できる資産のリストが表示されます。
3. [アプリケーション (Application)]タブで、保護する資産を検索して選択し、[保護の追加 (Add Protection)]をクリックします。

   たとえば、Microsoft SQL を保護するために、SQL インスタンス、スタンドアロンデータベース、AG (可用性グループ) データベースを選択できます。

   メモ: インスタンスレベルの SQL Server バックアップを選択した場合、オンラインのデータベースのみがスナップショットに含められます。スナップショットには、オフラインの、またはエラーがある状態のデータベースは含まれません。

   ---
4. [保護計画の選択 (Choose a protection plan)]パネルで、適切な保護計画を検索して選択し、[保護する (Protect)]をクリックします。

   [アプリケーション (Applications)]タブで、選択した資産の[次によって保護: (Protected by)]列に、割り当てた保護計画が表示されることを確認します。これは、構成された保護計画によって資産が現在保護されていることを示します。

   バックアップジョブは、計画で定義されたスケジュールに従って自動的にトリガされます。[アクティビティモニター (Activity monitor)]ペインからバックアップジョブを監視できます。

   (EKS にのみ適用可能) EKS でバックアップジョブの完了にかかる時間は、通信に追加の遅延を発生させるネットワークモジュレーターやスヌーパーが原因でさらに長くなります。

PaaS 資産をサブスクライブする前に、データベースにクレデンシャルを関連付ける必要があります。詳しくは、『NetBackup Web UI クラウド管理者ガイド』を参照してください。

保護計画に資産をサブスクライブする方法について詳しくは、『NetBackup Web UI バックアップ管理者ガイド』を参照してください。

スナップショットとリストアポイントコレクションのタグの割り当て

スナップショットへのタグの割り当て

ホスト (インスタンス) またはディスク (ボリューム) のスナップショットが NetBackup Snapshot Manager で開始されると、ソースのタグは、作成されたスナップショットに次のように適用されます。

- ホストのスナップショットが作成されると、ホストまたは VM で割り当てられたタグ (AWS と Azure) またはラベル (GCP) がスナップショットに適用されます。
- ディスクのスナップショットが作成されると、ディスクで割り当てられたタグ (AWS と Azure) またはラベル (GCP) がスナップショットに適用されます。
- スナップショットの作成中に、NetBackup Snapshot Manager は、スナップショットにいくつかのラベルまたはタグも適用します。
- NetBackup Snapshot Manager で必要なタグとソースタグの数が、タグの許容される最大制限より多い場合、これらの余分なタグはソース (ホスト/VM) からコピーされず、これらのスキップされたタグのキーは警告として NetBackup Snapshot Manager のログに記録されます。

Azure の場合	Azure Stack の場合	AWS の場合	GCP の場合	OCI の場合
タグの最大制限: 48 Azure Stack のリソースに割り当てることができるタグの最大数: 15	タグの最大制限: 15 インスタンスまたはディスクで許可されるタグの最大数: 13	タグの最大制限: 50 インスタンスまたはボリュームで許可されるタグの最大数: 40。 残りの 10 個のタグは、スナップショットを作成するために NetBackup Snapshot Manager 用に予約されます。	ラベルの最大制限: 62	タグの最大制限: 61

Azure の場合	Azure Stack の場合	AWS の場合	GCP の場合	OCI の場合
Azure で使用されるキー:	Azure Stack で使用されるキー:	AWS で使用されるキー:	GCP で使用されるキー:	OCI で使用されるキー:
cp:data、createdby	cp:data、createdby	cp:data、src-volume、src-vol-region、cloudpoint-replicated、src-inst-region、createdby、cp:host-snapshot-name、cloudpoint-description、cloudpoint-src-region、cloudpoint-src-account	instance_id、createdby	createdby、cp:data、cp:host-snapshot-name

NetBackup Snapshot Manager がスナップショットに割り当てるタグまたはラベルがいくつかあります。これらのタグは、インスタンス (ホスト) やディスク (ボリューム) などのリソースには割り当てないことをお勧めします。スナップショットの作成中に、資産に NetBackup Snapshot Manager タグのいずれかが見つかった場合、これらのタグはスキップされ、対応するスナップショットに割り当てられない可能性があります。

(Azure にのみ該当) リストアポイントコレクションへのタグの割り当て

- リストアポイントコレクションが存在しない場合は、インスタンスタグと NetBackup Snapshot Manager タグを使用して、新しいリストアポイントコレクションが作成されます。
- リストアポイントコレクションが存在し、タグが存在しない場合は、インスタンスタグと NetBackup Snapshot Manager タグが既存のリストアポイントコレクションに適用されます。
- リストアポイントコレクションが存在し `createdby: cloudpoint` タグがない場合は、リストアポイントコレクションの既存のタグを保持し、インスタンスの新しいタグと、NetBackup Snapshot Manager で必要なタグを追加します。
- リストアポイントコレクションが存在し `createdby: cloudpoint` タグがある場合は、リストアポイントコレクションの既存のタグを保持し、インスタンスの新しいタグと、NetBackup Snapshot Manager で必要なタグを追加します。

元のドライブのシャドウコピーを格納するための VSS の構成

Windows ファイルシステムまたは Microsoft SQL アプリケーションのディスクレベルのアプリケーションとの整合性を確保したスナップショットを取得する場合は、Microsoft VSS (ボリュームシャドウコピーサービス) を構成する必要があります。VSS を使用すると、アプリケーションでボリュームへの書き込みを続行しながらボリュームのスナップショットを取得できます。

VSS を構成するときは、次の点に注意してください。

- NetBackup Snapshot Manager には、現在、元のドライブと同じドライブまたはボリュームにシャドウコピーの作成場所を手動で構成する必要があるという制限があります。この方法により、アプリケーションとの整合性を確保したスナップショットが作成されます。
- 別のドライブまたは専用ドライブにシャドウストレージがすでに存在する場合は、そのストレージを無効にして、次の手順で構成内で置き換える必要があります。
- NetBackup Snapshot Manager では、先頭または末尾に空白または印字不可能な文字を含む SQL データベースの検出、スナップショット、およびリストア操作はサポートされません。これは、VSS ライターがそのようなデータベースに対してエラー状態になるためです。
  詳しくは、Microsoft 社のマニュアルを参照してください。

元のドライブのシャドウコピーを格納するための VSS を構成するには

1. Windows ホスト上で、コマンドプロンプトを開きます。サーバーで UAC (ユーザーアカウント制御) 設定が有効になっている場合は、管理者として実行のモードでコマンドプロンプトを起動します。
2. NetBackup Snapshot Manager を使用してディスクレベルのアプリケーションとの整合性を確保したスナップショットを作成する各ドライブ文字について、次のようなコマンドを入力します。

   ```
   vssadmin add shadowstorage /for=<drive being backed up> ^
   /on=<drive to store the shadow copy> ^
   /maxsize=<percentage of disk space allowed to be used>
   ```

   ここで、maxsize は、シャドウストレージドライブで許可される空き領域の最大使用状況を示します。コマンドのキャレット文字 (^) は、Windows のコマンドラインの継続文字を表します。

   たとえば、D: ドライブの VSS シャドウコピーを D: ドライブに格納し、D: の空きディスク容量の最大 80% を使用できるようにした場合、コマンド構文は次のようになります。

```
vssadmin add shadowstorage /for=d: /on=d: /maxsize=80%
```

コマンドプロンプトには、次のようなメッセージが表示されます。

```
Successfully added the shadow copy storage association
```

3. 次のコマンドを使用して、変更を確認します。

```
vssadmin list shadowstorage
```

9

NetBackup Snapshot Manager for Cloud でのボリュームの暗号化

この章では以下の項目について説明しています。

NetBackup Snapshot Manager でのボリュームの暗号化のサポートについて

NetBackup Snapshot Manager は、AWS、Azure、OCI、および Google Cloud Platform のディスクボリュームの暗号化をサポートします。ボリュームの暗号化は、クラウドプロバイダの KMS (Key Management Service) のカスタマキーまたはシステムキーを使用して行います。

クロスアカウントレプリケーションについて詳しくは、『NetBackup™ Web UI クラウド管理者ガイド』の「アカウントのレプリケーションのサポートマトリックス」セクションを参照してください。

Azure でのボリュームの暗号化

Azure では、次の方法でディスクを暗号化できます。

- デフォルトの暗号化 (PMK (Platform Managed Key) を使用)
- Azure Key Vault を使用した CMK (Customer Managed Key)
- 保存時の二重暗号化

Azure の暗号化について詳しくは、Microsoft Azure のマニュアルのデータ暗号化モデルに関するセクションを参照してください。

表 9-1 スナップショットの作成時の暗号化

ディスクの暗号化	スナップショットの暗号化
PMK (Platform Managed Key)	ソースディスクと同じ PMK を使用します。
CMK (Customer Managed Key)	ソースディスクと同じ CMK を使用します。
二重暗号化 (PMK_CMK)	ソースディスクと同じ CMK を使用します。

表 9-2 スナップショットのリストア時の暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	スナップショットと同じ PMK を使用します。
CMK	スナップショットと同じ CMK を使用します。
PMK_CMK	スナップショットと同じ CMK を使用します。

表 9-3 バックアップからのリストアのための暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	ソースディスクと同じ PMK を使用します。
CMK	ソースディスクと同じ CMK を使用します。
PMK_CMK	ソースディスクと同じ CMK を使用します。それ以外の場合は、PMK を使用します。

表 9-4 スナップショットまたはバックアップからの VM リストア中の暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。

スナップショットの暗号化	リストアディスクの暗号化
CMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。
PMK_CMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK、CMK または PMK_CMK にできます。

暗号化に使用する Key Vault への権限の割り当て

CMK 暗号化ディスクを使用した VM のスナップショットまたはバックアップからのリストアを有効にするには、暗号化に使用する Key Vault に次の権限を割り当てます。

1. 目的の Key Vault の新しいアクセスポリシーを作成します。

   Key Vault のアクセスポリシーについて詳しくは、Microsoft Azure のマニュアルの Key Vault アクセスポリシーの割り当てに関するセクションを参照してください。

2. [Key Permissions]の各セクションの[Permissions]タブで次の権限を追加します。

セクション	権限
キー管理操作	取得
暗号化操作	キーのラップ
	キーのラップ解除

3. [Principal]タブで、プロバイダの構成で使用されるサービスプリンシパルのオブジェクト ID を選択します。
4. アクセスポリシーを確認して作成します。
5. 手順 1 から手順 4 に従って、ディスク暗号化セットのサービスプリンシパルの ObjectID に同じ権限を割り当てます。

Key Vault: Azure の役割ベースのアクセス制御の権限

Azure の役割ベースのアクセス制御の権限モデルを使用して Key Vault が作成される場合:

1. Key Vault Reader の権限を持つ役割を追加し、アプリケーションサービスプリンシパルを割り当てます。
2. 同様に、Key Vault Secrets Officer の権限を追加し、アプリケーションサービスプリンシパルを割り当てます。

   詳しくは、Microsoft Azure のマニュアルの Azure の役割ベースのアクセス制御による Key Vault のキー、証明書、Secret へのアクセス権の付与に関するセクションを参照してください。

システム管理 ID: 有効

システムの管理対象 ID が NetBackup Snapshot Manager で有効になっている場合は、管理対象 ID に次の役割を割り当てます。

役割	管理対象 ID
Key Vault Reader	仮想マシンスケールセット
Key Vault Secrets Officer	仮想マシンスケールセット
Key Vault Crypto Service Encryption User	アプリ (ディスク暗号化セット)

ユーザー管理 ID: 有効

ユーザー管理 ID が NetBackup Snapshot Manager で有効になっている場合は、Key Vault Crypto Service Encryption User ロールを Key Vault のユーザー管理 ID に割り当てます。

GCP でのボリュームの暗号化

GCP では、次の方法でディスクを暗号化できます。

- デフォルトの暗号化 (PMK または Google Managed Key)
- Google Cloud KMS を使用した CMEK (Customer Managed Encryption Key)

GCP での暗号化について詳しくは、Google Cloud のマニュアルで暗号化に関するセクションを参照してください。

表 9-5 スナップショットの作成時の暗号化

ディスクの暗号化	スナップショットの暗号化
PMK (Platform Managed Key)	ソースディスクと同じ PMK を使用します。
CMK/CMEK	ソースディスクと同じ CMEK を使用します。

表 9-6 スナップショットのリストア時の暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	スナップショットと同じ PMK を使用します。
CMK/CMEK	リストア先がキーのスコープ内に含まれる場合、スナップショット同じ CMEK を使用します。

表 9-7 バックアップからのリストアのための暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	ソースディスクと同じ PMK を使用します。
CMK/CMEK	ソースディスクと同じ CMEK を使用します。

メモ: リストアを正常に実行するには、リストア時にリストア先をキーのスコープ内に配置する必要があります。Google Cloud ナレッジベースの記事で、必要な権限について次の記事を参照してください。

「KMS キーを使用した Google Compute Engine ディスクの暗号化が権限エラーにより失敗する」

表 9-8 スナップショットまたはバックアップからの VM リストア中の暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。
CMK/CMEK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。

AWS でのボリュームの暗号化

AWS では、次の方法でディスクを暗号化できます。

- デフォルトの暗号化 (PMK (Platform Managed Key) を使用)
- AWS KMS を使用した CMEK (Customer Managed Encryption Key)

AWS の暗号化について詳しくは、『Amazon Elastic Compute Cloud Linux インスタンス用ユーザーガイド』の Amazon EBS の暗号化に関するセクションを参照してください。

表 9-9 スナップショットの作成時の暗号化

ディスクの暗号化	スナップショットの暗号化
PMK (Platform Managed Key)	ソースディスクと同じ PMK を使用します。
CMEK	ソースディスクと同じ CMEK を使用します。

表 9-10 スナップショットのリストア時の暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	スナップショットと同じ PMK を使用します。
CMEK	スナップショットと同じ CMEK を使用します。

表 9-11 バックアップからのリストアのための暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	ソースディスクと同じ PMK を使用します。
CMK	ソースディスクと同じ CMK を使用します。

表 9-12 スナップショットまたはバックアップからの VM リストア中の暗号化

スナップショットの暗号化	リストアディスクの暗号化
なし	暗号化されていないディスクに適用されます。
PMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。
CMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。

OCI でのボリュームの暗号化

OCI では、次の方法でディスクを暗号化できます。

- デフォルトの暗号化 (PMK (Platform Managed Key) を使用)
- CMK (Customer Managed Encryption Key) (OCI マスター暗号化キーを使用)

OCI の暗号化について詳しくは、Oracle 社のマニュアルを参照してください。

表 9-13 スナップショットの作成時の暗号化

ディスクの暗号化	スナップショットの暗号化
PMK	ソースディスクと同じ PMK を使用します。
CMK	ソースディスクと同じ CMK を使用します。

表 9-14 スナップショットのリストア時の暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	スナップショットと同じ PMK を使用します。
CMK	スナップショットと同じ CMK を使用します。

表 9-15 バックアップからのリストアのための暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	ソースディスクと同じ PMK を使用します。
CMK	ソースディスクと同じ CMK を使用します。

表 9-16 スナップショットまたはバックアップからの VM リストア中の暗号化

スナップショットの暗号化	リストアディスクの暗号化
PMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。
CMK	ディスク上の暗号化は、リストア時のユーザーの選択に応じて PMK または CMK にできます。

10

NetBackup Snapshot Manager for Cloud のセキュリティ

この章では以下の項目について説明しています。

Azure Stack のセキュリティの構成

Azure Stack の作業負荷には 2 つの方法で接続できます。

- NetBackup Snapshot Manager は、プロバイダのプラグインを使用してクラウドの作業負荷に接続できます。
- NetBackup Snapshot Manager 上のデータムーバーコンテナは、クラウドコネクタのプラグインコンポーネントを介して作業負荷に接続できます。

Azure Stack の作業負荷の場合、これらのコンポーネントは HTTPS プロトコルを使用して接続します。デフォルトで、ピアとホストの検証は常に有効です。

p.27 の「プロキシサーバーの要件」を参照してください。

p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。

Azure Stack 用クラウドコネクタの構成

クラウドコネクタコンポーネントは、セキュアなメカニズムを介して作業負荷に接続します。次の構成を実行する必要があります。

SSL ピアとホストの検証

デフォルトで、ピアとホストの検証は有効です。ピアとホストの検証は、Azure Stack に対してのみ無効にできます。

ピアとホストの検証を無効にするには、NetBackup Snapshot Manager の `/cloudpoint/openv/netbackup/bp.conf` ファイルでパラメータ *VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED=NO* を設定します。ピアとホストの検証を無効にした後も、HTTPS プロトコルを使用する必要があります。

クラウド作業負荷の場合、パブリック root 証明書はコンテナイメージの一部です。NetBackup では、パブリッククラウドのルート証明書を含む `cacert.pem` ファイルを次の場所に保持します。

```
/usr/openv/var/global/wmc/cloud/cacert.pem
```

Azure Stack の場合は、NetBackup Snapshot Manager の `/cloudpoint/openv/netbackup/bp.conf` ファイルの *ECA_TRUST_STORE_PATH* パラメータを使用して、ルート証明書のファイルパスを指定する必要があります。*ECA_TRUST_STORE_PATH* の値が */cloudpoint/eca/trusted/cacerts.pem* ファイルに含まれている必要があります。

CRL の検証の構成

リリース 10.1 以降、NetBackup Snapshot Manager は NetBackup との通信中に NetBackup エンティティとして扱われます。NetBackup のエンティティ間の通信中は、証明書失効リスト (CRL) のチェックがデフォルトで有効です。

- ECA_CRL_CHECK: このフラグは、2 つの NetBackup エンティティ間の通信中に使用されます。デフォルトでは、CRL チェックは ECA_CRL_CHECK フラグで有効になっています。NetBackup Snapshot Manager マシン証明書が失効した場合、NetBackup と NetBackup Snapshot Manager との間の通信は次のエラーで失敗します。

  ```
  "The Snapshot Manager's certificate is not valid or doesn't
  exist.(9866)"
  ```

- VIRTUALIZATION_CRL_CHECK: 10.1 より前では、NetBackup Snapshot Manager は NetBackup との通信中に作業負荷と見なされていました。NetBackup と作業負荷間で通信が発生するたびに、VIRTUALIZATION_CRL_CHECK フラグの値が CRL チェックに使用されていました。デフォルトでは、CRL チェックは VIRTUALIZATION_CRL_CHECK フラグで無効になっています。

メモ: NetBackup をバージョン 9.1 から 10.4 以降にアップグレードした場合、ユーザーは、NetBackupと NetBackup Snapshot Manager との間の CRL チェック用に有効になっていた VIRTUALIZATION_CRL_CHECK フラグを削除できます。

Azure Stack の CA 構成

Azure Stack の作業負荷には、NetBackup とは異なる ECA で署名できます。NBCA モードで構成することもできます。次のように構成できます:

1. NetBackup Snapshot Manager と Azure Stack が同じ ECA で構成されている場合:
   - NetBackup への NetBackup Snapshot Manager の登録で、*ECA_TRUST_STORE_PATH* が `/cloudpoint/openv/netbackup/bp.conf` ファイルに追加されるため、手動による手順は不要です。
   - 必要な CA 証明書は `/cloudpoint/eca/trusted/cacerts.pem` ファイルにすでにあります。
2. NetBackup Snapshot Manager と Azure Stack が異なる ECA で構成されている場合:
   - 次のコマンドを使用して Snapshot Manager を更新します。
     ```
     # flexsnap_configure truststore --addtrust
     <azure_stack_root_ca>
     ```
   - 次のコマンドを使用して Snapshot Manager トラストストアを検証します。
     ```
     # flexsnap_configure truststore
     ```
   - 次のコマンドを使用して Snapshot Manager トラストストアから CA を削除します。
     ```
     flexsnap_configure truststore --rmtrust <azure_stack_root_ca>
     ```
3. 既知のパブリック CA を使用して Azure Stack を構成:

   NetBackup Snapshot Manager 側での手動による手順は必要ありません。

2

NetBackup Snapshot Manager for Cloud のメンテナンス

11

NetBackup Snapshot Manager for Cloud のログ記録

この章では以下の項目について説明しています。

NetBackup Snapshot Manager のログ記録のしくみについて

NetBackup Snapshot Manager は、ログデータの収集と統合に Fluentd ベースのログフレームワークを使用します。Fluentd は、構造化ログデータの収集と消費のための統合ログ層を提供するオープンソースデータコレクタです。

Fluentd について詳しくは、Fluentd の Web サイトを参照してください。

すべての NetBackup Snapshot Manager コンテナサービスが、構成されている Docker ログドライバにサービスログを生成し、公開します。ログドライバは、NetBackup Snapshot Manager ホスト上で独立した `flexsnap-fluentd` コンテナとして実行されている Fluentd フレームワークです。Fluentd フレームワークを使用すると、これらの個々のサービスログが構造化され、Fluentd データコレクタにルーティングされ、ここから構成された出力プラ

グインに送信されるようになります。flexsnap-fluentd コンテナのログは、デフォルトで構成されている出力プラグインです。

Fluentd ベースのログを使用すると、次のようなメリットがあります。

- すべての NetBackup Snapshot Manager サービスのログを格納する、永続的な構造化リポジトリ
- すべての NetBackup Snapshot Manager ログを 1 つのストリームで扱うことで (多種多様な個別のログファイルでなく)、特定のログを簡単に追跡および監視可能
- ログに関連付けられたメタデータにより、トラブルシューティングが迅速化する横断検索が可能
- NetBackup Snapshot Manager ログを分析および自動化のためにサードパーティ製ツールに統合してプッシュする機能

Fluentd ベースの NetBackup Snapshot Manager ログ記録のしくみ

NetBackup Snapshot Manager をインストールまたはアップグレードすると、NetBackup Snapshot Manager ホストで次の変更が発生します。

- `flexsnap-fluentd` という名前の新しいコンテナサービスが、NetBackup Snapshot Manager ホスト上で開始されます。このサービスは、他のすべての NetBackup Snapshot Manager コンテナサービスの前に開始されます。`flexsnap-fluentd` サービスは、ホスト上の `fluentd` デーモンとして機能します。
- すべての NetBackup Snapshot Manager コンテナサービスは、Docker ログドライバとして `fluentd` を使用して開始されます。
- `fluentd` 構成ファイルは `/cloudpoint/fluent/fluent.conf` で作成されます。このファイルには、NetBackup Snapshot Manager ログを消費するためのリダイレクト先の決定に使用される出力プラグインの定義が格納されます。

すべてのインフラコンポーネントの準備が完了すると、各 NetBackup Snapshot Manager サービスは、構成された Docker `fluentd` ログドライバにそれぞれのログメッセージを送信します。その後、`fluentd` デーモンは、`fluentd` 構成ファイルに設定された出力プラグインに、構造化ログをリダイレクトします。これらのログは、NetBackup Snapshot Manager ホスト上の `/cloudpoint/logs/flexsnap.log` ファイルに送信されます。

ファイルサイズが最大 100 MB に達すると、`flexsnap.log` ファイルがローテーションされることに注意してください。`flexsnap.log` ファイルの合計 30 世代 (ローテーション済みファイル) が保持されます。これらの条件は、`fluentd` コマンドで導入された、新しいログファイルのローテーション (`log-rotate-age`) とログサイズ (`log-rotate-size`) コマンドオプションによって適用されます。

ログファイルのローテーションとログサイズのコマンドオプションの構成手順

1 `/cloudpoint/flexsnap.conf` ファイルで、`log_rotate_age` と `log_rotate_size` の値をログセクションに入力し、`flexsnap-fluentd` コンテナを再起動して変更を有効にします。

`flexsnap.conf` ファイルの例:

```
[logging]
log_rotate_age = 7
log_rotate_size = 20000
```

- log_rotate_age: ローテーションされたログファイルを保持する世代 (ローテーション前に累積できるファイルの合計数) を指定します。デフォルト値は 30 です。
- log_rotate_size: 単一のログファイルをローテーションする上限のログファイルサイズを指定します (バイト単位)。デフォルト値は 100000000 バイトです。

2 `flexsnap.conf` ファイルを変更した後、`flexsnap-fluentd` コンテナを再起動します。

- Docker 環境の場合: `# sudo docker restart flexsnap-fluentd`
- Podman 環境の場合:

```
# sudo podman stop flexsnap-fluentd
# sudo podman start flexsnap-fluentd
```

NetBackup Snapshot Manager fluentd 構成ファイルについて

Fluentd は、ログメッセージのソース、ログの選択に使用するルールとフィルタのセット、ログメッセージを配信するためのターゲットの宛先を定義する構成ファイルを使用します。

NetBackup Snapshot Manager ホスト上で稼働する `fluentd` デーモンは、さまざまな宛先に NetBackup Snapshot Manager ログを送信する役割を担います。これらのターゲットは、入力データソースや必須の fluentd パラメータなど、その他の詳細とともに、プラグインの構成ファイル内に定義されます。NetBackup Snapshot Manager の場合、これらのプラグイン構成は、NetBackup Snapshot Manager ホスト上の `fluentd` 構成ファイル (`/cloudpoint/fluent/fluent.conf` 内) に格納されます。fluentd デーモンは、この構成ファイルから出力プラグインの定義を読み込み、NetBackup Snapshot Manager ログメッセージを送信する場所を決定します。

デフォルトでは、次の出力プラグイン定義が構成ファイルに追加されます。

`STDOUT`: これは、NetBackup Snapshot Manager ログメッセージを `/cloudpoint/logs/flexsnap.log` に送信するために使用されます。

このプラグインは次のように定義されます。

```
# Send to fluentd docker logs
<store>
@type stdout
</store>
```

さらに、NetBackup Snapshot Manager fluentd 構成ファイルには、次の宛先のプラグイン定義が含まれます。

- Splunk
- ElasticSearch

これらのプラグイン定義はテンプレートとして提供され、ファイル内でコメント化されます。実際の Splunk または ElasticSearch ターゲットを構成するには、これらの定義のコメントを解除し、必要に応じてパラメータ値を置換します。

fluentd 構成ファイルの変更

既存のプラグイン定義を変更する場合は、`fluent.conf` 構成ファイルを変更します。

fluent.conf ファイルを変更するには

1. NetBackup Snapshot Manager ホスト上で、任意のテキストエディタを使用して `/cloudpoint/fluent/fluent.conf` 構成ファイルを開き、内容を編集してプラグイン定義を追加または削除します。
2. ファイルに対するすべての変更を保存します。
3. `flexsnap-fluentd` コンテナサービスを次のコマンドを使用して再起動します。

   ```
   # sudo docker restart flexsnap-fluentd
   ```

変更がすぐに有効になり、変更後に生成される新しいログメッセージにのみ適用されることに注意してください。ファイルの変更は、構成ファイルが更新される前に生成された古いログには適用されません。

NetBackup Snapshot Manager ログ

NetBackup Snapshot Manager は、NetBackup Snapshot Manager アクティビティの監視と、問題があった場合のトラブルシューティングに使用できる次のログを保持します。ログは、NetBackup Snapshot Manager ホストの `<install_path>/cloudpoint/logs` に格納されます。

表 11-1 NetBackup Snapshot Manager ログファイル

ログ	説明
/cloudpoint/logs/flexsnap.log	このログファイルには、すべての製品ログが含まれています。
/cloudpoint/logs/flexsnap-cloudpoint.log	このログファイルには、すべての NetBackup Snapshot Manager インストールログと構成ログ (flexsnap_configure) が含まれています。
/cloudpoint/logs/flexsnap-ipv6config.log	このログファイルには、すべての IPv6 関連のログが含まれています。

スナップショットからのバックアップおよびバックアップジョブからのリストアのログ

/cloudpoint/openv/dm/datamover.<id> に移動します。

ここで、ログは logs、opt、netbackup の各ディレクトリにあります。

- nbpxyhelper と nbsubscriber のログは、logs ディレクトリ内にあります。
- VRTSpbx のログは、opt ディレクトリ内にあります。
- bpbkar、bpcd、bpclntcmd、nbcert、vnetd、vxms およびその他すべてのサービスのログは、netbackup ディレクトリ内にあります。

ログの詳細度を高めるため、NetBackup Snapshot Manager の /cloudpoint/openv/netbackup で、bp.conf ファイルと nblog.conf ファイルを更新できます。『NetBackup ログリファレンスガイド』を参照してください。

bp.conf ファイルと nblog.conf ファイルへの変更は、スナップショットからのバックアップまたはリストアジョブが次回実行されたときに有効になります。

ログの保持

データムーバーログのデフォルトの構成は次のとおりです。

- ログの最大保持期間は 30 日です。30 日以上経過したログは削除されます。
- データムーバーログの高水準点と低水準点のデフォルトの構成は、「/cloudpoint」マウントポイントのサイズの 70% と 30% です。たとえば、/cloudpoint フォルダの使用可能なサイズが 30 GB の場合、高水準点は 21 GB (70%)、低水準点は 9 GB (30%) です。ログのディレクトリ (/cloudpoint/openv/dm/) のサイズが高水準点に達した場合、クリーンアップされて実行されなくなったデータムーバーコンテナの古いログは削除対象と見なされます。このようなデータムーバーコンテナのログは、低水準点に達するか、クリーンアップされた、または実行されなくなったデータムーバーコンテナのログがなくなるまで削除されます。

デフォルト構成の修正

ログの保持のデフォルト構成は、プライマリ NetBackup Snapshot Manager の flexsnap.conf に次のようなセクションを追加することで修正できます。パス /cloudpoint/flexsnap.conf から flexsnap.conf ファイルを開き、次のセクションを追加します。

```
[datamover]
high_water_mark = 50
low_water_mark = 20
log_retention_in_days = 60
```

NetBackup Snapshot Manager 拡張機能の場合、プライマリ NetBackup Snapshot Manager の構成が使用されます。プライマリで構成を変更すると、1 時間以内に各 Snapshot Manager 拡張機能で構成が更新されます。プライマリ NetBackup Snapshot Manager や NetBackup Snapshot Manager 拡張機能に個別のカスタム構成は使用できません。また、構成はプライマリ NetBackup Snapshot Manager でのみ変更する必要があります。プライマリ NetBackup Snapshot Manager と NetBackup Snapshot Manager 拡張機能の構成は同じですが、ログサイズの高水準点と低水準点は、各プライマリ NetBackup Snapshot Manager または NetBackup Snapshot Manager 拡張機能にマウントされた /cloudpoint ディレクトリに基づいて計算されます。

NetBackup Snapshot Manager 拡張機能のログ

各 NetBackup Snapshot Manager 拡張機能は、独自の /cloudpoint/logs の場所でログを保持します。

- VM ベースの拡張機能ログ: 拡張機能 VM の /cloudpoint/logs ディレクトリ。
- 管理対象 Kubernetes のクラスタベースの拡張機能ログ: Kubernetes 拡張機能ポッドにアクセスしてそこで実行し、ファイル共有に属する /cloudpoint/logs ディレクトリを検索する必要があります。

エージェントレスログおよびオンホストエージェントログ

エージェントレスログ

クラウドインスタンスへのエージェントレス接続のログは、プラットフォームに基づいてクラウドインスタンスの次の場所に存在します。

- Linux の場合: /opt/VRTScloudpoint/.agent/
- Windows の場合: C:¥ProgramData¥Veritas¥CloudPoint¥logs¥

オンホストエージェントログ

クラウドインスタンスへのオンホストエージェント接続のログは、プラットフォームに基づいてクラウドインスタンスの次の場所に存在します。

- Linux の場合: `/var/log/flexsnap/`
- Windows の場合: `C:¥ProgramData¥Veritas¥CloudPoint¥logs¥`

NetBackup Snapshot Manager ログ記録のトラブルシューティング

`/cloudpoint/logs/flexsnap.log` ファイルから NetBackup Snapshot Manager サービスのログを取得するには、次のコマンドを実行します。

```
# sudo cat /cloudpoint/logs/flexsnap.log | grep <flexsnap-service name>
```

12

NetBackup Snapshot Manager for Cloud のアップグレード

この章では以下の項目について説明しています。

NetBackup Snapshot Manager for Cloud のアップグレードについて

2 つのバージョンの NetBackup Snapshot Manager を 2 つの異なるホストで使用して同じ資産を管理することがないようにします。

NetBackup Snapshot Manager のアップグレード時に、以前のバージョンのスナップショットデータと構成データはすべて外部の `/cloudpoint` データボリュームで維持されます。Cohesity では、同じホスト、または以前のバージョンの NetBackup Snapshot Manager データボリュームが接続されている別のホストで NetBackup Snapshot Manager をアップグレードすることをお勧めします。

サポート対象のアップグレードパス

表 12-1 NetBackup Snapshot Manager アップグレードパス

アップグレード前のバージョン	アップグレード後のバージョン
10.3/10.3.0.1/10.4/10.4.0.1/10.5/10.5.0.1/11.0/11.0.0.1	11.1
10.2 以下	10.3 にアップグレードされた 10.2.0.1

アップグレードのシナリオ

次の表に、NetBackup Snapshot Manager のアップグレードのシナリオを示します。

メモ: NetBackup バージョン 10.4 以降の場合、NetBackup (プライマリ、メディア) サーバーと NetBackup Snapshot Manager のバージョンは同じレベルである必要があります。アップグレード中に、最初に NetBackup Snapshot Manager をアップグレードしてから NetBackup サーバーをアップグレードします。

メモ: NetBackup Snapshot Manager が Azure Marketplace 経由でインストールされている場合は、NetBackup Snapshot Manager を Azure Marketplace 経由でアップグレードすることをお勧めします。詳しくは、『Azure クラウドでの NetBackup™ マーケットプレイス配備』ガイドの Snapshot Manager のアップグレードに関するセクションを参照してください。

表 12-2 アップグレードのシナリオ

シナリオ	説明	処理
NetBackup バージョン 10.5 以降へのアップグレード	NetBackup を 10.3 以降にアップグレードする場合 (すべての NetBackup Snapshot Manager サーバーのアップグレードを含む) p.271 の「サポート対象のアップグレードパス」を参照してください。	このアップグレードのプロセスは次のとおりです。 ■ メンテナンスのため、NetBackup Web UI で NetBackup Snapshot Manager サーバーを無効にします。 ■ NetBackup Snapshot Manager サーバーを NetBackup 9.1.x から NetBackup 10.x にアップグレードします。 ■ NetBackup Snapshot Manager サーバーを NetBackup 10.x から NetBackup 10.5 以降にアップグレードします。 ■ NetBackup Web UI で NetBackup Snapshot Manager サーバーを有効にします。 ■ NetBackup サーバーを 8.3.x から直接 10.5 にアップグレードします。 ■ ストレージユニットで構成されている場合は、メディアサーバーを 10.5 にアップグレードします。 **メモ:** 1 台以上の NetBackup Snapshot Manager サーバーをアップグレードしない場合は、NetBackup Web UI を使用してこれらのサーバーを無効にする必要があります。この場合、無効にした NetBackup Snapshot Manager サーバーに関連付けられている資産は NetBackup で保護できません。 **メモ:** Snapshot Manager をアップグレードした後も、Snapshot Manager に対して証明書が発行されていない場合は、次の手順を実行します。 `tpconfig -update -snapshot_manager <snapshot_manager_name> -snapshot_manager_user_id <username> -manage_workload <workload>`

シナリオ	説明	処理
NetBackup Snapshot Manager のみをバージョン 10.3 以降にアップグレード	NetBackup Snapshot Manager サーバーのみを 10.3 以降にアップグレードし、NetBackup は 10.3 以降にアップグレードしない場合。	NetBackup Snapshot Manager と NetBackup のバージョン間の非互換性をサポートする EEB (Emergency Engineering Binary) を入手するには、Veritas Technical Supportにお問い合わせください。 ■ NetBackup Snapshot Manager サーバーを無効にします。 ■ NetBackup プライマリサーバーと関連付けられているメディアサーバーに EEB パッチを適用します。 ■ NetBackup Snapshot Manager をアップグレードします。 ■ 次に、NetBackup Snapshot Manager サーバーを有効にします。 p.285 の「パッチまたは Hotfix を使用した NetBackup Snapshot Manager のアップグレード」を参照してください。 **メモ:** `flexsnap_configure` CLI を使用して Snapshot Manager をアップグレードした後も、Snapshot Manager に対して証明書が発行されていない場合は、次の手順を実行します。 `tpconfig -update -snapshot_manager <snapshot_manager_name> -snapshot_manager_user_id <username> -manage_workload <workload>`
	NetBackup Snapshot Manager のみをバージョン 10.3 以降にアップグレードする予定だったが、オンホストエージェントと NetBackup Snapshot Manager 拡張機能をアップグレードしなかった場合。	■ オンホストエージェントのバージョンを 10.3 以降に更新します。 ■ NetBackup Snapshot Manager 拡張機能をバージョン 10.3 以降に更新します。 NetBackup Snapshot Manager とオンホスト/NetBackup Snapshot Manager 拡張機能のバージョン間の非互換性をサポートする場合は、Veritas Technical Supportにお問い合わせください。 **メモ:** 上記の推奨処置は「 NetBackup Snapshot Manager における RabbitMQ の認証回避の脆弱性」のセキュリティアドバイザリに基づいています。
VM ベースの NetBackup Snapshot Manager の Kubernetes 配備への移行	VM ベースの NetBackup Snapshot Manager を管理対象 Kubernetes クラスタに移行する場合。	手順について詳しくは、『Kubernetes クラスタ向け Cohesity Cloud Scale Technology 手動配備ガイド』の「NetBackup Snapshot Manager の移行とアップグレード」セクションを参照してください。
RHEL での NetBackup Snapshot Manager の移行とアップグレード	RHEL 8.6 または 8.4 での NetBackup Snapshot Manager の移行とアップグレードを行う場合	p.288 の「NetBackup Snapshot Manager の移行とアップグレード」を参照してください。

NetBackup Snapshot Manager のアップグレードの準備

アップグレード前に以下の点に注意してください。

- NetBackup Snapshot Manager インスタンス、仮想マシン、または物理ホストが、アップグレード先の NetBackup Snapshot Manager バージョンの要件を満たしていることを確認します。
  p.19 の「 システム要件への準拠」を参照してください。
- NetBackup サーバーで必要なポートが、次の章の「必要なポート」セクションで説明されている要件を満たしていることを確認します。
  p.37 の「NetBackup Snapshot Manager でのスナップショットジョブからのバックアップの準備」を参照してください。
- NetBackup Snapshot Manager のアップグレード時に、以前のバージョンのスナップショットデータと構成データはすべて外部の `/cloudpoint` データボリュームで維持されます。この情報は NetBackup Snapshot Manager コンテナとイメージの外部にあり、アップグレード中保持されます。
  ただし、必要に応じて、アップグレードプロセス中にメッセージが表示されたら、または手動で `/cloudpoint` ボリューム内のすべてのデータのバックアップを作成できます。
  p.303 の「NetBackup Snapshot Manager のバックアップ」を参照してください。
- VPC エンドポイントを使用して AWS プラグインを構成する場合は、アップグレードする前に、次のセクションで説明する必要な手順を実行していることを確認します。
  p.126 の「VPC エンドポイントを使用した AWS プラグイン構成の前提条件」を参照してください。
- (PostgreSQL の場合) インストールディレクトリの権限は 755 以上である必要があります。PostgreSQL サーバーは root 以外のユーザーで実行されるため、インストールディレクトリにアクセスするユーザーは root 以外のユーザーである必要があります。
  Mongo データベースから PostgreSQL データベースにデータを移行する場合、必要な最小容量は 1 GB です。
- NetBackup Snapshot Manager で実行されているジョブがないことを確認します。
  - NetBackup コンソールから、Snapshot Manager に関連するポリシーと SLP を無効にします。
  - NetBackup アクティビティモニターで、Snapshot Manager に関連する実行中のジョブを取り消します。
  - Snapshot Manager インスタンスまたはサービスがアップグレードまたは移行の一環としてシャットダウンされた後も実行中のジョブがある場合は、Snapshot Manager をホストしている VM に接続されている追加のディスクを検索します。これらのディスクを特定して手動で削除します。

- NetBackup Snapshot Manager のアップグレード後に、必要に応じて NetBackup プライマリサーバーをアップグレードできます。また、NetBackup Web UI から NetBackup Snapshot Manager サーバーを有効にする必要があります。

NetBackup Snapshot Manager のアップグレード

次の手順では、NetBackup Snapshot Manager の配備をアップグレードする方法について説明します。アップグレード中に、現在のバージョンの NetBackup Snapshot Manager を実行しているコンテナを新しいコンテナに置き換えます。

Podman/Docker 環境で NetBackup Snapshot Manager サーバーをアップグレードするには

1. NetBackup Snapshot Manager アップグレードインストーラをダウンロードします。

   NetBackup Snapshot Manager のダウンロードページで、[今すぐダウンロード (Download Now)]をクリックして NetBackup Snapshot Manager インストーラをダウンロードします。

   NetBackup Snapshot Manager ソフトウェアコンポーネントはパッケージ形式で利用可能です。ファイル名の形式を次に示します。

   ```
   NetBackup_SnapshotManager_<version>.tar.gz
   ```

   メモ: 実際のファイル名は、リリースバージョンによって異なる場合があります。

2. NetBackup Snapshot Manager を配備するコンピュータに、ダウンロードした圧縮イメージファイルをコピーします。
3. イメージファイルの tar を解凍し、内容を一覧表示します。

   ```
   # ls
   NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
   netbackup-flexsnap-11.1.x.x-xxxx.tar.gz
   flexsnap_preinstall.sh
   ```

4 次のコマンドを実行して、NetBackup Snapshot Manager ホストのインストールを準備します。

```
# sudo ./flexsnap_preinstall.sh
```

出力は次のようになります。

Podman の場合

```
Checking for disk space                   ...  done
Checking for swap space                   ...  done
Validate host resources                   ...  done
Validate SELINUX                          ...  done
Check for podman installation             ...  done
Validate podman version support           ...  done
Check for podman socket file              ...  done
Checking for required packages            ...  done
Validate required services health         ...  done
Removing deprecated services              ...  done
Loading Snapshot Manager service images   ...  done
Creating nbsvcusr user and group          ...  done
Loading CIL policy for containers         ...  done
Copying flexsnap_configure script         ...  done
```

Docker の場合

```
Checking for disk space                   ...  done
Checking for swap space                   ...  done
Validate host resources                   ...  done
Check for docker installation             ...  done
Validate docker version support           ...  done
Check for docker socket file              ...  done
Checking for required packages            ...  done
Validate required services health         ...  done
Loading Snapshot Manager service images   ...  done
Copying flexsnap_configure script         ...  done
```

5 保護ポリシーのスナップショットまたは他の操作が進行中でないことを確認してから、次のコマンドを実行して NetBackup Snapshot Manager を停止します。

```
# flexsnap_configure stop
```

メモ: ベリタスでは、Snapshot Manager のインストールに flexsnap_configure CLI を使用することをお勧めします。Docker/Podman CLI を使用した Snapshot Manager のインストールは、RHEL 8/9 以外では非推奨となり、RHEL 8/9 では削除されています。

または

次の同等の Docker/Podman コマンドを使用して、NetBackup Snapshot Manager を停止します。

- *Podman の場合*

```
# sudo podman run -it --rm -u 0 -v
/cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<current_version> stop
```

- *Docker の場合*

```
# sudo docker run -it --rm -u 0 -v
/cloudpoint:/cloudpoint
-v /run/docker/docker.sock:/run/docker/docker.sock
veritas/flexsnap-deploy:<current_version> stop
```

ここで、*current_version* は、現在インストールされている NetBackup Snapshot Manager のバージョンを表します。

メモ: 改行なしでコマンドを入力していることを確認します。

NetBackup Snapshot Manager コンテナが 1 つずつ停止します。次のようなメッセージがコマンドラインに表示されます。

```
Stopping the services
Stopping services at time: Mon Jul 31 12:49:01 UTC 2023
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
```

```
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Mon Jul 31 12:49:21 UTC 2023
```

すべての NetBackup Snapshot Manager コンテナの停止を待機してから、次の手順に進みます。

6 次のコマンドを実行して、NetBackup Snapshot Manager をアップグレードします。

```
flexsnap_configure install
```

メモ: ベリタスでは、Snapshot Manager のインストールに flexsnap_configure CLI を使用することをお勧めします。Docker/Podman CLI を使用した Snapshot Manager のインストールは、RHEL 8/9 以外では非推奨となり、RHEL 8/9 では削除されています。

または

次の同等の Docker/Podman コマンドを使用して、NetBackup Snapshot Manager をアップグレードします。

- *Podman の場合*

```
            # podman run -it --rm -u 0 -v
/cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<new_version> install
```

無人インストールの場合は、次のコマンドを使用します。

```
            # podman run -it --rm -u 0 -v
/cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-deploy:<new_version> install -y
```

- *Docker の場合*

```
            # sudo docker run -it --rm -u 0 -v
/cloudpoint:/cloudpoint -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<new_version> install
```

無人インストールの場合は、次のコマンドを使用します。

```
            # sudo docker run -it --rm --privileged -u 0 -v
/cloudpoint:/cloudpoint -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-deploy:<new_version> install -y
```

ここで、*new_version* はアップグレード後の NetBackup Snapshot Manager のバージョン (たとえば 11.1.x.x-xxxx) を表します。

-y オプションを指定すると、以降のすべてのインストールプロンプトで承認され、インストーラを非対話モードで進められます。

メモ: 改行なしでコマンドを入力していることを確認します。

インストーラは最初に個々のサービスイメージをロードし、次にそれらをそれぞれのコンテナで起動します。

出力は次のようになります。次に、Podman 環境の出力例を示します。

```
Stopping the services
Stopping services at time: Wed Jan  3 06:12:52 UTC 2024
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
```

```
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Wed Jan  3 06:13:24 UTC 2024
Configuration started at time: Wed Jan  3 06:13:31 UTC 2024
Podman server version: 4.2.0
This is an upgrade to NetBackup Snapshot Manager 11.1.x.x-xxxx
Previous Snapshot Manager version: 10.4.x.x.xxxx
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-postgresql ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-fluentd ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-rabbitmq ...done
Deleting network : flexsnap-network ...done
Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.4.x.x.xxxx.tar.gz.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...Starting container: flexsnap-certauth ...done
Waiting for flexsnap-certauth container to move to healthy
state...Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
```

```
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Wed Jan  3 06:16:56 UTC 2024
```

例 2:

```
Stopping the services
Stopping services at time: Fri Aug  4 10:38:37 UTC 2023
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-mongodb ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Fri Aug  4 10:38:55 UTC 2023
Configuration started at time: Fri Aug  4 10:38:57 UTC 2023
Docker server version: 20.10.7

IPv6 configuration is temporarily disabled on system. Snapshot
Manager will be configured without IPv6 support.
For Snapshot Manager with IPv6 support, enable IPv6 configuration
 on the system.

This is an upgrade to NetBackup Snapshot Manager 11.1.x.x-xxxx
Previous Snapshot Manager version: 10.4.0.0.xxxx
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-rabbitmq ...done
```

```
Removing exited container flexsnap-mongodb ...done
Removing exited container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done

Taking backup of Snapshot Manager metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_10.4.0.0.xxxx.tar.gz.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...Starting container: flexsnap-mongodb ...done
Waiting for flexsnap-mongodb container to move to healthy
state...Data migration required from mongo database to postgresql
 database
Data migration is successful.
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...Starting container: flexsnap-certauth ...done
Waiting for flexsnap-certauth container to move to healthy
state...Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Deleteing mongo resources
flexsnap-mongodb
```

7 NetBackup Snapshot Manager の対話型および非対話型アップグレード:

- NetBackup Snapshot Manager の対話型アップグレード:

  ```
  # flexsnap_configure install -i
  ```

  出力は次のようになります。

  ```
  Do you want to take a backup of the Snapshot Manager metadata
   prior to upgrade? (y/n): n
  Stopping the services
  Stopping services at time: Wed Jan  3 06:12:52 UTC 2024
  Stopping container: flexsnap-workflow-system-0-min ...done
  ```

```
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
Stopping services completed at time: Wed Jan  3 06:13:24 UTC
2024
Configuration started at time: Wed Jan  3 06:13:31 UTC 2024
Podman server version: 4.2.0
This is an upgrade to NetBackup Snapshot Manager 11.1.x.x-xxxx
Previous Snapshot Manager version: 10.4.x.x.xxxx
Removing exited container flexsnap-nginx ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-listener ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-postgresql ...done
Removing exited container flexsnap-certauth ...done
Removing exited container flexsnap-fluentd ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-rabbitmq ...done
Deleting network : flexsnap-network ...done
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-postgresql ...done
Waiting for flexsnap-postgresql container to move to healthy
state...Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...Starting container: flexsnap-certauth ...done
Waiting for flexsnap-certauth container to move to healthy
state...Starting container: flexsnap-api-gateway ...done
```

```
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Wed Jan  3 06:16:56 UTC 2024
```

- NetBackup Snapshot Manager の非対話型アップグレード:

  ```
  # flexsnap_configure install
  ```

  出力は次のようになります。

  ```
  Configuration started at time: Thu Jul 13 09:23:27 UTC 2023
  Docker server version: 1.13.1
  This is an upgrade to NetBackup Snapshot Manager 11.1.x.x-xxxx
  Previous Snapshot Manager version: 10.4.0.0.1188
  Taking backup of Snapshot Manager metadata...done
  Backup completed successfully.
  Backup file located at
  /cloudpoint/backup/cloudpoint_10.2.0.0.1188.tar.gz.
  Removing exited container
  flexsnap-agent.837b51be82f5451e8eca27761d2f5b0c ...done
  Removing exited container flexsnap-nginx ...done
  Removing exited container flexsnap-notification ...done
  Removing exited container flexsnap-policy ...done
  Removing exited container flexsnap-scheduler ...done
  Removing exited container flexsnap-onhostagent ...done
  Removing exited container flexsnap-agent ...done
  Removing exited container flexsnap-listener ...done
  Removing exited container flexsnap-coordinator ...done
  Removing exited container flexsnap-api-gateway ...done
  Removing exited container flexsnap-certauth ...done
  Removing exited container flexsnap-rabbitmq ...done
  Removing exited container flexsnap-postgresql ...done
  Removing exited container flexsnap-fluentd ...done
  Deleting network : flexsnap-network ...done
  Creating network: flexsnap-network ...done
  Starting container: flexsnap-fluentd ...done
  Starting container: flexsnap-postgresql ...done
  Waiting for flexsnap-postgresql container to move to healthy
  state...
  ```

```
Starting container: flexsnap-rabbitmq ...done
Waiting for flexsnap-rabbitmq container to move to healthy
state...
Starting container: flexsnap-certauth ...done
Starting container: flexsnap-api-gateway ...done
Starting container: flexsnap-coordinator ...done
Starting container: flexsnap-listener ...done
Starting container: flexsnap-agent ...done
Starting container: flexsnap-onhostagent ...done
Starting container: flexsnap-scheduler ...done
Starting container: flexsnap-policy ...done
Starting container: flexsnap-notification ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Thu Jul 13 09:27:18 UTC 2023
```

8 NetBackup Snapshot Manager は、クラウド VM 作業負荷のプライマリサーバーまたはメディアサーバーをアップグレードせずに、より新しいバージョンにアップグレードできます。

9 (省略可能) 次のコマンドを実行して、以前のバージョンのイメージを削除します。

(*Podman* の場合) `# podman rmi -f <imagename>:<oldimage_tagid>`

(*Docker* の場合) `# docker rmi -f <imagename>:<oldimage_tagid>`

10 新しい NetBackup Snapshot Manager バージョンが正常にインストールされたことを確認するには:

p.63 の「NetBackup Snapshot Manager が正常にインストールされたことの確認」を参照してください。

11 これによりアップグレードプロセスは終了します。NetBackup Snapshot Manager 構成の設定と、データがそのまま維持されていることを確認します。

次の手順では、クレデンシャルを使用して NetBackup Snapshot Manager を NetBackup プライマリサーバー (10.2 以前) に登録します。

パッチまたは Hotfix を使用した NetBackup Snapshot Manager のアップグレード

パッチまたは Hotfix を使用しても現在の NetBackup Snapshot Manager サーバーをアップグレードできます。通常のアップグレードに適用される考慮事項および手順はすべて、パッチまたは Hotfix を使用するアップグレードにも適用されます。ただし、新しい NetBackup Snapshot Manager イメージをダウンロードする代わりにパッチまたは Hotfix バイナリをダウンロードします。

パッチまたは Hotfix の EEB (Emergency Engineering Binary) を入手については、Veritas Technical Support (https://www.veritas.com/content/support/en_US/contact-us) にお問い合わせください。

以下に、例を含めた簡単な手順を示します。アップグレード手順について詳しくは、

p.275 の「NetBackup Snapshot Manager のアップグレード」を参照してください。

現在インストールされているバージョンが NetBackup Snapshot Manager `10.4.x.x` で、Podman/Docker 環境の RHEL 8.6 システムで NetBackup Snapshot Manager パッチバージョン `11.1.x.x-xxxx` にアップグレードする場合を考えます。

パッチまたは Hotfix を使用して NetBackup Snapshot Manager をアップグレードするには

1. Veritas Technical Support から取得した NetBackup Snapshot Manager EEB をダウンロードします。

   例: `NetBackup_SnapshotManager_<version>.tar.gz`

2. イメージファイルの tar を解凍し、内容を一覧表示します。

   ```
   # ls
   NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
   netbackup-flexsnap-11.1.x.x-xxxx.tar.gz
   flexsnap_preinstall.sh
   ```

3. 次のコマンドを実行して、NetBackup Snapshot Manager ホストのインストールを準備します。

   ```
   # sudo ./flexsnap_preinstall.sh
   ```

4. 保護ポリシーのスナップショットまたは他の操作が進行中でないことを確認してから、次のコマンドを実行して NetBackup Snapshot Manager を停止します。

   Docker/Podman の場合: flexsnap_configure CLI を使用する場合:

   ```
   # flexsnap_configure stop
   ```

メモ: ベリタスでは、Snapshot Manager のインストールに flexsnap_configure CLI を使用することをお勧めします。Docker/Podman CLI を使用した Snapshot Manager のインストールは、RHEL 8/9 以外では非推奨となり、RHEL 8/9 では削除されています。

---

5 次のコマンドを実行して、NetBackup Snapshot Manager をアップグレードします。

Docker/Podman の場合: flexsnap_configure CLI を使用する場合:

```
# flexsnap_configure install
```

メモ: ベリタスでは、Snapshot Manager のインストールに flexsnap_configure CLI を使用することをお勧めします。Docker/Podman CLI を使用した Snapshot Manager のインストールは、RHEL 8/9 以外では非推奨となり、RHEL 8/9 では削除されています。

インストーラは最初に個々のサービスイメージをロードし、次にそれらをそれぞれのコンテナで起動します。

6 (省略可能) 次のコマンドを実行して、以前のバージョンのイメージを削除します。

(*Podman* の場合) `# sudo podman rmi -f <imagename>:<oldimage_tagid>`

(*Docker* の場合) `# sudo docker rmi -f <imagename>:<oldimage_tagid>`

7 新しい NetBackup Snapshot Manager バージョンが正常にインストールされたことを確認するには:

p.63 の「NetBackup Snapshot Manager が正常にインストールされたことの確認」を参照してください。

8 これで、パッチまたは Hotfix を使用した NetBackup Snapshot Manager のアップグレードプロセスが完了しました。NetBackup Snapshot Manager 構成の設定と、データがそのまま維持されていることを確認します。

NetBackup Snapshot Manager ホストへのオペレーティングシステムパッチの適用

NetBackup Snapshot Manager ホストにオペレーティングシステムパッチを適用するには、次の手順を実行します。

1. 次のコマンドを使用して、NetBackup Snapshot Manager を停止します。

```
# flexsnap_configure stop
```

2. オペレーティングシステムのパッチを適用するには、該当するオペレーティングシステムのマニュアルに記載されている手順を実行します。
3. オペレーティングシステムのパッチが適用されたら、次のコマンドを使用して NetBackup Snapshot Manager を開始します。

```
# flexsnap_configure start
```

NetBackup Snapshot Manager の移行とアップグレード

このセクションでは、RHEL で NetBackup Snapshot Manager を移行およびアップグレードする手順について説明します。

NetBackup Snapshot Manager の移行を開始する前に

NetBackup Snapshot Manager をインストールする前に次を完了していることを確認します。

- 環境がシステム要件を満たしていることを確認します。
  p.19 の「 システム要件への準拠」を参照してください。
- NetBackup Snapshot Manager をインストールするインスタンスを作成するか、物理ホストを準備します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。
  p.34 の「NetBackup Snapshot Manager をインストールするインスタンスの作成またはホストの準備」を参照してください。
- RHEL 8.x または 9.x ホストのインストールを準備します。既存の RHEL 7.x OS を RHEL 8.x/9.x OS にアップグレードするか、RHEL 8.x/9.x で新しいシステムを作成できます。
  - RHEL 7.x から RHEL 8.x または 9.x へのシステムのアップグレードについては、Red Hat 社のマニュアルに従ってください。
  - RHEL 8.x または 9.x で新しいシステムを作成する場合は、Podman コンテナプラットフォームを構成します
    p.34 の「コンテナプラットフォーム (Docker、Podman) のインストール」を参照してください。
    簡単な手順を以下に示します。
    - RHEL リポジトリを設定します。
      AWS クラウドの場合は追加のリポジトリを有効にします。
      ```
      # sudo yum-config-manager --enable
      rhui-REGION-rhel-server-extras
      ```
    - 必要に応じて Podman をインストールします。
      ```
      # sudo yum install -y podman
      ```
- 次のコマンドを実行して、必要なパッケージ (`podman-plugins`、`lvm2`、`systemd-udev`、`udica`、`policycoreutils-devel`) をホストにインストールします。
  ```
  #yum install -y lvm2-<version>
  #yum install -y lvm2-libs-<version>
  ```

```
#yum install -y systemd-udev-<version>
#yum install -y podman-plugins
#yum install -y udica policycoreutils-devel
```

- インスタンスまたは物理ホストで特定のポートが開いていることを確認します。
  p.37 の「インスタンスまたは物理ホストで特定のポートが開いていることの確認」を参照してください。

次に、RHEL 7.x ホストから新しく準備した RHEL 8.x/9.x ホストに NetBackup Snapshot Manager を移行します。

p.289 の「RHEL 8.x および 9.x での NetBackup Snapshot Manager の移行とアップグレード」を参照してください。

RHEL 8.x および 9.x での NetBackup Snapshot Manager の移行とアップグレード

RHEL 7.x ホストから新しい RHEL 8.x または 9.x ホストに NetBackup Snapshot Manager 10.0 または 10.0.0.1 を移行するには、次の手順を実行します。

Docker 環境で NetBackup Snapshot Manager をインストールまたはアップグレードするには

1. NetBackup Snapshot Manager アップグレードインストーラをダウンロードします。

   例: `NetBackup_SnapshotManager_<version>.tar.gz`

2. イメージファイルの tar を解凍し、内容を一覧表示します。

   ```
   # ls
   NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
   netbackup-flexsnap-11.1.x.x-xxxx.tar.gz
   flexsnap_preinstall.sh
   ```

3. 次のコマンドを実行して、NetBackup Snapshot Manager ホストのインストールを準備します。

   ```
   # sudo ./flexsnap_preinstall.sh
   ```

4. 次のコマンドを実行して、NetBackup Snapshot Manager をアップグレードします。

   ```
   # flexsnap_configure install
   ```

   インストーラは最初に個々のサービスイメージをロードし、次にそれらをそれぞれのコンテナで起動します。

5 (省略可能) 次のコマンドを実行して、以前のバージョンのイメージを削除します。

```
# docker rmi -f <imagename>:<oldimage_tagid>
```

6 新しい NetBackup Snapshot Manager バージョンが正常にインストールされたことを確認するには:

p.63 の「NetBackup Snapshot Manager が正常にインストールされたことの確認」を参照してください。

Podman 環境で NetBackup Snapshot Manager を移行するには

1 RHEL 7.x ホストで、保護ポリシーのスナップショットまたは他の操作が進行中でないことを確認してから、次のコマンドを実行して NetBackup Snapshot Manager を停止します。

```
# flexsnap_configure stop
```

NetBackup Snapshot Manager コンテナが 1 つずつ停止します。次のようなメッセージがコマンドラインに表示されます。

```
Stopping the services
Stopping container:
flexsnap-agent.8f9ee77e48964e278a0367e60defdf6e ...done
Stopping container: flexsnap-workflow-system-0-min ...done
Stopping container: flexsnap-workflow-general-0-min ...done
Stopping container: flexsnap-listener ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-onhostagent ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-certauth ...done
Stopping container: flexsnap-rabbitmq ...done
Stopping container: flexsnap-postgresql ...done
Stopping container: flexsnap-fluentd ...done
```

すべての NetBackup Snapshot Manager コンテナの停止を待機してから、次の手順に進みます。

2 RHEL 8.x および 9.x ホストに NetBackup Snapshot Manager 構成データを移行します。

- RHEL 8.x および 9.x で新しいシステムを作成した場合:

- 現在のホストから /cloudpoint をマウント解除するには、次のコマンドを実行します。

  ```
  # umount /cloudpoint
  ```

- /cloudpoint マウントポイントにマウントされていたデータディスクを接続解除します。

  メモ: データディスクの接続解除または接続について詳しくは、クラウドベンダーまたはストレージベンダーが提供するマニュアルに従ってください。

- RHEL 8.x および 9.x ホストで、次のコマンドを実行してディスクを作成してマウントします。

  ```
  # mkdir /cloudpoint
  # mount /dev/<diskname> /cloudpoint
  ```

  ベンダー固有の詳細について

  p.35 の「NetBackup Snapshot Manager データを格納するボリュームの作成とマウント」を参照してください。

- RHEL 7.x から RHEL 8.x および 9.x にアップグレードした場合は、RHEL 7.x システムから /cloudpoint マウントポイントデータをコピーし、それを RHEL 8.x および 9.x システムの /cloudpoint フォルダに移動します。

「「Docker 環境で NetBackup Snapshot Manager をインストールまたはアップグレードするには」」に記載されている手順に従って、以前のホストと異なるホスト(RHEL 8.x と 9.x) に同じバージョンの NetBackup Snapshot Manager をインストールします。

これにより、NetBackup Snapshot Manager の移行プロセスが完了します。

移行後、「「Docker 環境で NetBackup Snapshot Manager をインストールまたはアップグレードするには」」に記載されている手順に従って、新しいホストに new_version をインストールします。

3 移行プロセス中に、NetBackup Snapshot Manager が別のシステムに移行されたか、IP アドレスが変更された場合は、次のように証明書を再生成します。

flexsnap_configure CLI の使用

- 次のコマンドを使用して NetBackup Snapshot Manager サービスを停止します。

  ```
  # flexsnap_configure stop
  ```

- 次のコマンドを使用して証明書を再生成します。

  ```
  # flexsnap_configure renew --help
  ```

メモ: /cloudpoint/openv/netbackup/bp.conf ファイルの CLIENT_NAME の値が Snapshot Manager のホスト名と一致することを確認します。ホスト名を変更してから移行する場合は、証明書を再生成する前にこの値を手動で更新する必要があります。

p.59 の「NetBackup Snapshot Manager への接続のセキュリティ保護」を参照してください。

- 次のコマンドを使用して NetBackup Snapshot Manager サービスを起動します。

```
# flexsnap_configure start
```

4 NetBackup Snapshot Manager を RHEL 8.x および 9.x ホストに移行した後、次の手順を実行して NetBackup Snapshot Manager を 11.1.x.x.xxxx にアップグレードします。

p.275 の「NetBackup Snapshot Manager のアップグレード」を参照してください。

5 これにより NetBackup Snapshot Manager の移行とアップグレードのプロセスが完了します。NetBackup Snapshot Manager 構成の設定と、データがそのまま維持されていることを確認します。

ゾーンからリージョンへの移行のための GCP 構成

リリース 10.1 より前は、GCP プロバイダはゾーンを選択して構成されていました。このリリースでは、リージョンを選択するためのチェックリストが提供されます。プロバイダにリージョンを構成すると、構成済みのリージョンのすべてのゾーンの資産が検出されます。

Snapshot Manager が以前のリリースからアップグレードされた場合、すべてのゾーン構成はリージョンに移動されます。アップグレード後にゾーンからリージョンに移行するさまざまなシナリオの例を次に示します。

- 単一の GCP プロバイダを使用したアップグレード:
  アップグレード前に、*us-west1-a* と *us-east1-b* ゾーンを使用した単一のプロバイダ構成が存在する場合、アップグレード後に構成は *us-west1* と *us-east1* に変更されます。*us-west1-a* と *us-east1-b* ゾーンとともに、*us-west1* と *us-east1* リージョンに含まれる他のゾーンからの資産も保護できます。
- 複数の GCP プロバイダを使用したアップグレード:
  - 競合しないリージョン: アップグレード前に、次のように 2 つの GCP プロバイダが構成されている場合:
    GCP1 で構成されているゾーン: *us-east1-a*、*us-west1-a*
    GCP2 で構成されているゾーン: *us-central-a*
    アップグレード後に、上記の構成は次のようにリージョンに変更されます。
    GCP1: *us-east1* と *us-west1*

GCP2: *us-central*

メモ: ゾーンからリージョンに構成を更新した後、異なるプロバイダで重複するリージョンはありません。

- 競合するリージョン: アップグレード前に、次のように 2 つの GCP プロバイダが構成されている場合:
  GCP1 で構成されているゾーン: *us-east1-a*、*us-west1-a*
  GCP2 で構成されているゾーン: *us-central-a*、*us-east1-b*
  アップグレード後に、上記の構成は次のようにリージョンに変更されます。
  GCP1: *us-east1* と *us-west1*
  GCP2: *us-central* と *us-east1*

  メモ: ゾーンからリージョンに構成を更新した後、*us-east1* リージョンは GCP1 プロバイダと GCP2 プロバイダで重複しています。

アップグレード後のリージョンの競合の解決

アップグレード後に、次の場合にリージョンで競合が発生する可能性があります。

- 単一の Snapshot Manager サーバーに複数のプロバイダが追加された場合
  または
- 単一の NetBackup マスターサーバーに複数の Snapshot Manager サーバーが登録された場合

競合を解決する例を次に示します。

- 例 1:
  GCP1: *us-east1* と *us-west1*
  GCP2: *us-east1* と *us-central*
  ユーザーは、プロバイダのタブにある[編集 (Edit)]オプションを使用して、上記のいずれかの構成から *us-east1* を削除できます。
  複数の Snapshot Manager サーバー間で競合が発生した場合は、次の手順を実行します。
  - 競合していないリージョン用に、新しいプロバイダ構成 GCP3 を追加します。例: us-west1
  - GCP1 を削除して、2 つの Snapshot Manager サーバー間のリージョンの競合を削除します。

メモ: 複数の Snapshot Manager サーバーが 1 つの NetBackup に登録されている場合は、アップグレードについてベリタスのサポートチームにお問い合わせください。

- 例 2:
  GCP1: *us-east1* と *us-west1*
  GCP2: *us-east1*
  ユーザーは `tpconfig` コマンドから delete_plugin オプションを使用して、GCP2 から *us-east1* を削除できます。
- 例 3:
  GCP1: *us-east1*
  GCP2: *us-east1*
  ユーザーは、`tpconfig` コマンドから delete_plugin オプション使用して任意の 1 つのプロバイダ構成を削除できます。

アップグレード後のタスク

NetBackup Snapshot Manager サーバーが正常にアップグレードされた後、次のタスクの実行が必要になる場合があります。

アップグレード後のタスク

1. Linux および Windows アプリケーションホストの NetBackup Snapshot Manager エージェントをアップグレードします。

   メモ: NetBackup Snapshot Manager 8.3 から 9.0 または 9.1 にアップグレードする場合は、オンホストエージェントを手動でアップグレードする必要があります。
   NetBackup Snapshot Manager 9.0 から 9.1 にアップグレードする場合、オンホストエージェントのアップグレードは省略可能です。

   Linux ホストのエージェントをアップグレードするには、次の手順を実行します。

   - NetBackup UI にサインインして、新しいエージェントパッケージをダウンロードします。
     [クラウド (Cloud)]、[NetBackup Snapshot Manager]、[処理 (Actions)]、[エージェントの追加 (Add agent)]の順に移動します。
   - エージェントをアップグレードする Linux ホストの flexsnap エージェントサービスを停止します。
     Linux ホストで次のコマンドを実行します。

     ```
     # sudo systemctl stop flexsnap-core.service
     ```
   - Linux ホストのエージェントをアップグレードします。

Linux ホストで次のコマンドを実行します。

```
# sudo rpm -Uvh --force flexsnap_agent_rpm_name
```

ここで、*flexsnap_agent_rpm_name* は、以前にダウンロードしたエージェント rpm パッケージの名前です。

- プロンプトが表示されたら、デーモンを再ロードします。
  Linux ホストで次のコマンドを実行します。

  ```
  # sudo systemctl daemon-reload
  ```

- Linux ベースのエージェントをアップグレードするすべての Linux ホストで、これらの手順を繰り返します。

次の点に注意してください。

CloudPoint エージェントから Flexsnap エージェントにアップグレードする場合は、次の推奨アンインストールコマンドとインストールコマンドを使って、最初に CloudPoint エージェントをアンインストールしてから Flexsnap エージェントをインストールします。

- アンインストール: `sudo yum -y remove cloudpoint_agent_rpm_name`
- インストール: `sudo yum -y install flexnsap_agent_rpm_name`
- Linux ホストに接続し、次のコマンドを使用してエージェントを再登録します。

  ```
  sudo flexsnap-agent --ip <snapshotmanager_host_FQDN_or_IP>
  --token <authtoken>
  ```

- 検出タスクを実行します。

Windows ホストのエージェントをアップグレードするには、次の手順を実行します。

- NetBackup UI にサインインして、新しいエージェントパッケージをダウンロードします。
  [クラウド (Cloud)]、[NetBackup Snapshot Manager]、[処理 (Actions)]、[エージェントの追加 (Add agent)]の順に移動します。
- ホストで実行されている Cohesity NetBackup Snapshot Manager エージェントサービスを停止します。
- 新しいバージョンのエージェントパッケージファイルを実行し、インストールウィザードのワークフローに従って、Windows ホストでオンホストエージェントをアップグレードします。
  インストーラによって既存のインストールが検出され、新しいバージョンにパッケージが自動的にアップグレードされます。
- エージェントの構成のトークンを生成します。NetBackup Web UI で[クラウド (Cloud)]、[NetBackup Snapshot Manager]、[処理 (Actions)]、[エージェントの追加 (Add agent)]、[トークンの作成 (Create Token)]の順に移動します。

- Windows ベースのエージェントをアップグレードするすべての Windows ホストで、これらの手順を繰り返します。

NetBackup UI からエージェントインストールパッケージをダウンロードする方法について詳しくは、次を参照してください。

p.217 の「NetBackup Snapshot Manager エージェントのダウンロードとインストール」を参照してください。

2 次のいずれかの操作を実行します。

- NetBackup プライマリサーバーで次のコマンドを実行します。

```
./tpconfig -update -snapshot_manager <snapshot_manager_name>
-snapshot_manager_user_id <user_ID> -manage_workload
<manage_workload> [-requiredport <IP_port_number>]
[-security_token <token_value>]
```

メモ: クラウドの作業負荷を管理している NetBackup Snapshot Manager を更新するには、追加のオプション `-security_token` が必要です。トークンは標準ホストトークンである必要があります。これは、NetBackup Snapshot Manager で NetBackup 証明書を生成するために必要です。

UNIX システムでは、このコマンドへのディレクトリパスは `/usr/openv/volmgr/bin/` です。Windows システムでは、このコマンドへのディレクトリパスは `install_path¥Volmgr¥bin¥` です。詳しくは、『Cohesity NetBackup コマンドリファレンスガイド』を参照してください。
または

- 次の URL を使用して NetBackup プライマリサーバーへの PATCH API 呼び出しを行います。
  https://*primaryserver.domain*.com/netbackup/config/servers/snapshot-mgmt-servers/*cp-hostname*

または

Snapshot Manager が 10.3 より前の NetBackup バージョンに登録されている場合は、NetBackup UI で再発行トークンを使用して Snapshot Manager を編集します。

3 デフォルトでは、NetBackup Snapshot Manager のスナップショット作成操作では、スナップショットの代わりにリカバリポイントが作成されます。このため、アプリケーション整合になるようにスナップショットに対して Azure リカバリポイントを使用するには、Azure リストアポイントを有効にするように次の追加の権限が構成されていることを確認します。

```
actions": [
 "Microsoft.Compute/restorePointCollections/read",
 "Microsoft.Compute/restorePointCollections/write",
 "Microsoft.Compute/restorePointCollections/delete",
 "Microsoft.Compute/restorePointCollections/restorePoints/read",

 "Microsoft.Compute/restorePointCollections/restorePoints/write",

 "Microsoft.Compute/restorePointCollections/restorePoints/delete",

 "Microsoft.Compute/restorePointCollections/restorePoints/
  retrieveSasUris/action",
 "Microsoft.Compute/restorePointCollections/restorePoints/
  diskRestorePoints/read",
 "Microsoft.Compute/restorePointCollections/restorePoints/
  diskRestorePoints/beginGetAccess/action",
 "Microsoft.Compute/restorePointCollections/restorePoints/
  diskRestorePoints/endGetAccess/action"
            ],"
```

4 NetBackup Snapshot Manager をバージョン 11.1.x.x.xxxx にアップグレードした後、オンホストエージェントを再起動して、LVM ストレージの資産を検出して保護する必要があります。

`tpconfig` コマンドとそのオプションについて詳しくは、『Cohesity NetBackup コマンドリファレンスガイド』を参照してください。

メモ: アップグレードが完了したら、NetBackup コンソールから、Snapshot Manager に関連するポリシーと SLP を有効にします。

VPC エンドポイントを使用した AWS プラグイン構成のアップグレード後のタスク

NetBackup Snapshot Manager をバージョン 11.1.x.x.xxxx に正常にアップグレードした後、AWS プラグイン構成に VPC エンドポイントを使用するには、次を実行します。

1. AWS コンソールから AWS STS (セキュリティトークンサービス) のエンドポイントを作成します。

2. ［作業負荷 (Workloads)］、［クラウド (Cloud)］の順に移動し、NetBackup Snapshot Manager のタブを選択します。
3. アマゾンウェブサービスクラウドプロバイダで Snapshot Manager を選択して、［処理 (Actions)］メニューの［編集 (Edit)］オプションをクリックしてプラグインを編集します。
4. VPC エンドポイントで、ゾーンが指定されておらず、NetBackup Snapshot Manager リージョンが STS エンドポイントで作成されたリージョンと同じである必要がある AWS STS の最初の DNS 名を渡します。

NetBackup Snapshot Manager 拡張機能のアップグレード

NetBackup Snapshot Manager がアップグレードされると、すべての拡張機能が自動的に無効になります。必要な NetBackup Snapshot Manager バージョンの拡張機能をアップグレードし、NetBackup Web UI から手動で有効にする必要があります。

管理対象 Kubernetes クラスタ (AKS) での NetBackup Snapshot Manager 拡張機能のアップグレード

1 実行可能ファイルとしての実行をスクリプトに対して許可します。

```
# chmod +x cp_extension_start.sh
```

2 次のようにコマンドを実行します。

```
# ./cp_extension.sh install

NetBackup Snapshot Manager image repository path.
Format=<Login-server/image:tag>:
bfsscale.azurecr.io/veritas/flexsnap-deploy:11.1.x.x.xxxx
Snapshot Manager extension namespace: cloudpoint-system
Snapshot Manager extension token:
This is an upgrade of NetBackup Snapshot Manager Extension

Starting Snapshot Manager service deployment
customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 unchanged serviceaccount/cloudpoint-acc unchanged
clusterrole.rbac.authorization.k8s.io/cloudpoint-cloudpoint-system
 unchanged
clusterrolebinding.rbac.authorization.k8s.io/cloudpoint-rolebinding-cloudpoint-system
 unchanged deployment.apps/flexsnap-deploy unchanged
Snapshot Manager service deployment ...done

customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
 condition met
Generating Snapshot Manager Custom Resource Definition object
```

```
deployment "flexsnap-deploy" successfully rolled out
cloudpointrule.veritas.com/cloudpoint-config-rule configured
Snapshot Manager extension installation ...done
```

実行可能な方法

- 実行可能ファイルとしての実行をスクリプトに対して許可します。

  ```
  # chmod +x cp_extension_start.sh
  ```

- 次のようにインストールコマンドを実行します。

  ```
  # ./cp_extension_start.sh install -i <target_image:tag> -n
  <namespace> -t <workflow_token>
  ```

  例:

  ```
  # ./cp_extension_start.sh install -i
  mycontainer.azurecr.io/veritas/flexsnap-deploy:11.1.x.x-xxxx
  -n cloudpoint-system -t workflow
  3q3ou4jxiircp9tk0eer2g9jx7mwuypwz10k4i3sms2e7k4ee7-.....
  ```

Azure の管理対象 Kubernetes クラスタ (AKS) への NetBackup Snapshot Manager 拡張機能のアップグレード

NetBackup 10.4 以降のセキュリティを向上させるために、Data Mover コンテナのプロセスはサービス (非 root) ユーザーで起動するように構成されています。SMB プロトコルを使用してファイル共有が作成された場合、データ移動操作のために Data Mover を起動すると、スナップショットからのバックアップ、スナップショットからのインデックス操作などが失敗します。この問題を解決するには、次を実行します。

1. 古いファイル共有からログのバックアップを作成するか、古いファイル共有を保持します。
2. NetBackup Snapshot Manager 拡張機能をアンインストールします。永続ボリューム、ConfigMap、Secret を AKS 拡張機能から削除します。
3. NetBackup Snapshot Manager 拡張機能をインストールします。StorageClass を定義する際は、NFS プロトコルを使用した `Azure` **ファイル**に CSI プロビジョナを使用することを検討してください。

   p.74 の「Azure の管理対象 Kubernetes クラスタ (AKS) への NetBackup Snapshot Manager 拡張機能のインストール」を参照してください。

AWS の管理対象 Kubernetes クラスタ (EKS) での NetBackup Snapshot Manager 拡張機能のアップグレード

NetBackup 10.4 以降のセキュリティを向上させるために、Data Mover コンテナのプロセスはサービス (非 root) ユーザーで起動するように構成されています。SMB プロトコルを使用してファイル共有が作成された場合、データ移動操作のために Data Mover を起動すると、スナップショットからのバックアップ、スナップショットからのインデックス操作などが失敗します。この問題を解決するには、次を実行します。

1. 古いファイル共有からログのバックアップを作成するか、古いファイル共有を保持します。
2. NetBackup Snapshot Manager 拡張機能をアンインストールします。永続ボリューム、ConfigMap、Secret を EKS 拡張機能から削除します。
3. NetBackup Snapshot Manager 拡張機能をインストールします。StorageClass を定義するときに、`uid/gid` を root に設定することを検討します。

   p.83 の「AWS の管理対象 Kubernetes クラスタ (EKS) への NetBackup Snapshot Manager 拡張機能のインストール」を参照してください。

VM での NetBackup Snapshot Manager 拡張機能のアップグレード

1 イメージファイルの tar を解凍し、内容を一覧表示します。

```
# ls
NetBackup_SnapshotManager_11.1.x.x-xxxx.tar.gz
netbackup-flexsnap-11.1.x.x-xxxx.tar.gz
flexsnap_preinstall.sh
```

2 次のコマンドを実行して、Snapshot Manager ホストのインストールを準備します。

```
# ./flexsnap_preinstall.sh
```

3 VM 拡張機能をアップグレードするには、次の各コマンドを実行します。

- NetBackup Snapshot Manager 拡張機能の非対話型更新:

  ```
  # flexsnap_configure install --extension
  ```

- NetBackup Snapshot Manager 拡張機能の対話型更新:

  ```
  # flexsnap_configure install --extension -i
  ```

アップグレード後の制限事項

NetBackup Snapshot Manager バージョン 11.1.x.x.xxxx にアップグレードした後は、Linux プラットフォームの RPM、または Windows サーバーの MSI インストーラを使って、配備されたオンホストエージェントをアップグレードすることをお勧めします。

詳しくは次のトラブルシューティングに関する項を参照してください。

p.332 の「NetBackup Snapshot Manager バージョン 11.x へのアップグレード後に、接続済みまたは構成済みのクラウド VM のアプリケーション状態にエラーが表示される」を参照してください。 へのアップグレード後に、接続済みまたは構成済みのクラウド VM のアプリケーション状態にエラーが表示される

移行後のタスク

移行後に名前を NetBackup Snapshot Manager に変更した場合は、Linux と Windows のオンホストエージェント更新のために次の手順を実行し、プラグインレベルの検出を実行します。

Linux の場合:

- /etc/flexsnap.conf ファイルを編集し、対象のフィールドを NetBackup Snapshot Manager の新しい IP/ホストで更新します。
  例:

```
[root@testVM]# cat /etc/flexsnap.conf
[global]
target = nbuxqa-alphaqa-10-250-172-172.vxindia.veritas.com
hostid = azure-vm-b5c2b769-256a-4488-a71d-f809ce0fec5d

[agent]
id = agent.c2ec74c967e043aaae5818e50a939556
```

- 次のコマンドを使用して、Linux のオンホストエージェント更新を実行します。
  `/opt/VRTScloudpoint/bin/flexsnap-agent --renew --token <auth_token>`
- 次のコマンドを使用して、Linux のオンホストエージェントを再起動します。
  `sudo systemctl restart flexsnap-agent.service`

Windows の場合:

- ¥etc¥flexsnap.conf を編集し、対象のフィールドを NetBackup Snapshot Manager の新しい IP/ホストで更新します。
  例:

```
[global]
target = nbuxqa-alphaqa-10-250-172-172.vxindia.veritas.com
hostid = azure-vm-427a67a0-6f91-4a35-abb0-635e099fe9ad

[agent]
id = agent.3e2de0bf17d54ed0b54d4b33530594d8
```

- 次のコマンドを使用して、Windows のオンホストエージェント更新を実行します。
  `"c:¥ProgramFiles¥Veritas¥CloudPoint¥flexsnap-agent.exe" --renew --token <auth_token>`

13

NetBackup Snapshot Manager for Cloud のアンインストール

この章では以下の項目について説明しています。

NetBackup Snapshot Manager のアンインストールの準備

NetBackup Snapshot Manager をアンインストールする前に、以下の点に注意してください。

- アクティブな NetBackup Snapshot Manager 操作が進行中でないことを確認します。たとえば、稼働中のスナップショット、レプリケーション、リストアまたはインデックスのジョブが実行中の場合は、完了するまで待機します。

ポリシーを構成した場合は、スケジュール設定されたポリシーの実行を停止していることを確認します。これらのポリシーを削除することもできます。

- アプリケーションホストにインストールされている NetBackup Snapshot Manager エージェントを削除することを確認します。アプリケーションホストは、NetBackup Snapshot Manager によって保護されているアプリケーションが実行されているシステムです。
p.306 の「NetBackup Snapshot Manager エージェントの削除」を参照してください。
- NetBackup Snapshot Manager サーバーを NetBackup から無効にすることを確認します。NetBackup Web UI から NetBackup Snapshot Manager サーバーを無効にできます。
- 既存のインストールのすべてのスナップショットデータと構成データは、外部の `/cloudpoint` データボリュームで維持されます。この情報は NetBackup Snapshot Manager コンテナとイメージの外部にあり、アンインストール後は削除されます。
必要に応じて、`/cloudpoint` ボリューム内のすべてのデータのバックアップを作成できます。
p.303 の「NetBackup Snapshot Manager のバックアップ」を参照してください。

NetBackup Snapshot Manager のバックアップ

NetBackup Snapshot Manager がクラウドに配備されている場合

クラウドに配備されている NetBackup Snapshot Manager をバックアップするには

1. NetBackup Snapshot Manager サービスを停止します。

   (Docker/Podman の場合)

   ```
   flexsnap_configure stop
   ```

2. すべての NetBackup Snapshot Manager コンテナが停止していることを確認してください。NetBackup Snapshot Manager の一貫したバックアップを取得するために、NetBackup Snapshot Manager との間のすべてのアクティビティと接続を停止する必要があるため、この手順は重要です。

   次のように入力します。

   (*Docker の場合*) `# sudo docker ps | grep veritas`

   (*Podman の場合*) `# sudo podman ps | grep veritas`

   このコマンドでは、アクティブに実行されている NetBackup Snapshot Manager コンテナが返されることはありません。

3 (オプション) アクティブなコンテナが引き続き表示される場合は、手順 2 を繰り返します。この方法が機能しない場合は、アクティブになっている各コンテナで次のコマンドを実行します。

(*Docker の場合*) `# sudo docker kill container_name`

(*Podman の場合*) `# sudo podman kill container_name`

Docker 環境のコマンドの例を次に示します。

```
# sudo docker kill flexsnap-api
```

4 すべてのコンテナが停止した後、NetBackup Snapshot Manager をインストールしたボリュームのスナップショットを作成します。クラウドプロバイダのスナップショットツールを使用します。

5 スナップショットが完了したら、NetBackup Snapshot Manager サービスを再起動します。

次のコマンドを使用します。

(Docker/Podman の場合)

```
flexsnap_configure start
```

NetBackup Snapshot Manager プラグインの構成解除

NetBackup Snapshot Manager プラグインは、スナップショットを取得して資産を保護できるように、NetBackup Snapshot Manager でホストの資産を検出することを可能にします。必要に応じて、NetBackup UI を使用して NetBackup Snapshot Manager プラグインの構成を削除できます。

ホストからプラグイン構成を削除する前に、次の点を考慮します。

- 構成解除するプラグインに関連する資産のすべてのスナップショットを削除する必要があります。
  資産スナップショットが存在する場合、プラグインの構成解除は失敗します。
- プラグインの構成を解除すると、選択したホストからプラグインが削除されます。同じホスト上のプラグイン関連の資産を再度保護するには、ホストでそのプラグインを再構成する必要があります。
- プラグインの構成を解除すると、プラグインに関連するすべての資産が NetBackup Snapshot Manager の構成から削除され、それらの資産を保護できなくなります。

ホストからプラグインを構成解除するには

1 NetBackup UI にサインインします。

2 すべてのプラグイン関連の資産スナップショットを削除したことを確認します。

3 左側のメニューで[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックし、[仮想マシン (Virtual machines)]タブをクリックします。

4 [仮想マシン (Virtual machines)]タブで、エージェントの構成を解除するホストを選択し、上部に表示されるメニューバーから[構成解除 (Unconfigure)]をクリックします。

NetBackup Snapshot Manager は、ホストからプラグインを構成解除します。[構成解除 (Unconfigure)]ボタンが[構成 (Configure)]に変わることを確認します。これは、プラグインの構成解除がホストで成功したことを示します。

NetBackup Snapshot Manager エージェントの構成解除

リモートホストの資産の保護を NetBackup Snapshot Manager で有効にするには、まず NetBackup Snapshot Manager サーバーとリモートホスト間の接続を確立する必要があります。接続の構成 (エージェントを使用しているか、エージェントレス機能を使用しているか) に応じて、NetBackup Snapshot Manager は、すべての資産を検出し、ホストで操作を実行するために使用されるプラグインを管理するエージェントを使用します。

リモートホストを保護のために構成すると、エージェント登録とプラグインの構成情報が NetBackup Snapshot Manager サーバーの NetBackup Snapshot Manager データベースに追加されます。必要に応じて、NetBackup UI から切断操作を実行して、NetBackup Snapshot Manager データベースからエージェントのエントリを削除できます。

エージェントを構成解除する前に、次の点を考慮してください。

- エージェントを構成解除すると、そのホストに NetBackup Snapshot Manager エージェントをインストールしている場合、同じホストでは NetBackup Snapshot Manager プラグインを再構成できません。ホストでプラグインを再度構成できるようにするには、最初にホストからエージェントパッケージをアンインストールし、ホストを接続して、エージェントを NetBackup Snapshot Manager サーバーに再度インストールして登録する必要があります。
- 接続解除操作に進む前に、まずホストから NetBackup Snapshot Manager プラグインを構成解除する必要があります。NetBackup Snapshot Manager プラグインがホストに構成されている場合、接続解除オプションは有効になりません。
- NetBackup Snapshot Manager サーバーからエージェントエントリの構成を解除しても、エージェントパッケージはホストからアンインストールされません。接続解除操作が完了した後、ホストからエージェントのバイナリを手動で削除する必要があります。
- エージェントの構成を解除すると、そのホストに属するすべてのファイルシステム資産が NetBackup Snapshot Manager 構成から削除されます。

NetBackup Snapshot Manager サーバーからエージェントエントリの構成を解除するには

1. NetBackup UI にサインインします。
2. 接続解除するホストから NetBackup Snapshot Manager プラグイン構成を削除します。

   p.304 の「NetBackup Snapshot Manager プラグインの構成解除」を参照してください。
3. 左側のメニューで[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックし、[仮想マシン (Virtual machines)]タブをクリックします。
4. [仮想マシン (Virtual machines)]タブで、エージェントの構成を解除するホストを選択し、上部に表示されるメニューバーから[接続切断 (Disconnect)]をクリックします。

   NetBackup Snapshot Manager は、エージェントの構成解除を開始します。[接続切断 (Disconnect)]ボタンが[接続 (Connect)]に変わることを確認します。これは、切断操作が成功し、エージェントが正常に構成解除されたことを示します。

   エージェントと、エージェントによって検出された資産の情報は、NetBackup Snapshot Manager データベースから削除されます。
5. 次の手順では、切断操作を実行したホストからエージェントを手動でアンインストールします。これは、後で NetBackup Snapshot Manager を使用してこのホストとその資産を保護する場合に必要です。

   p.306 の「NetBackup Snapshot Manager エージェントの削除」を参照してください。

NetBackup Snapshot Manager エージェントの削除

NetBackup Snapshot Manager エージェントを削除する前に、まず NetBackup Snapshot Manager を削除する必要があります。エージェントは、アプリケーションが稼働するホストに直接インストールされます。NetBackup Snapshot Manager エージェントは、資産を検出してホストでスナップショット操作を実行する NetBackup Snapshot Manager プラグインを管理します。

NetBackup Snapshot Manager オンホストエージェントをアンインストールするには

1 NetBackup Snapshot Manager エージェントをインストールしたホストに接続します。

接続に使用するユーザーアカウントに、ホストに対する管理権限があることを確認します。

2 Linux ベースのエージェントの場合は、次の手順を実行します。

次のコマンドを使用して .rpm パッケージを削除します。

```
# sudo yum -y remove <snapshotmanager_agent_package>
```

ここで、<*snapshotmanager_agent_package*> はエージェント rpm パッケージの名前であり、バージョン番号とファイル拡張子 (.rpm) は付けません。

たとえば、エージェント rpm パッケージの名前が VRTSflexsnap-agent-11.1.x.x-xxxx-RHEL.x86_64.rpm の場合、コマンドの構文は次のようになります。

```
# sudo yum -y remove VRTSflexsnap-agent
```

3 Windows ベースのエージェントの場合は、次の手順を実行します。

Windows の [コントロールパネル] の [プログラムと機能] で、NetBackup Snapshot Manager エージェントのエントリ (Cohesity NetBackup Snapshot Manager エージェント) を選択し、[アンインストール] をクリックします。

ウィザードのワークフローに従って、Windows インスタンスからエージェントをアンインストールします。

メモ: アンインストールを許可するには、管理者ユーザーは Windows UAC プロンプトで [はい (Yes)] をクリックする必要があります。管理者以外のユーザーは、UAC プロンプトで管理者ユーザーのクレデンシャルを指定する必要があります。

---

4 これにより、エージェントのアンインストールが完了します。

これで、NetBackup Snapshot Manager のアンインストールに進めます。

p.308 の「NetBackup Snapshot Manager のスタンドアロン Docker ホスト環境からの削除」を参照してください。

NetBackup Snapshot Manager のスタンドアロン Docker ホスト環境からの削除

NetBackup Snapshot Manager のアンインストール手順は、インストールのための手順と同じです。唯一の違いは、コマンドで "uninstall" を指定します。これにより、ホストからコンポーネントを削除するようにインストーラに指示されます。

アンインストール中に、インストーラにより NetBackup Snapshot Manager ホストで次のタスクが実行されます。

- 稼働中のすべての NetBackup Snapshot Manager コンテナの停止
- NetBackup Snapshot Manager コンテナの削除
- NetBackup Snapshot Manager イメージのロード解除と削除

NetBackup Snapshot Manager をアンインストールする方法

1. NetBackup Snapshot Manager エージェントを NetBackup Snapshot Manager 構成に含まれているすべてのホストからアンインストールしたことを確認します。

   p.306 の「NetBackup Snapshot Manager エージェントの削除」を参照してください。

2. 保護ポリシーのスナップショットまたは他の操作が進行中でないことを確認してから、次のコマンドをホストで実行して NetBackup Snapshot Manager をアンインストールします。

   (Docker/Podman の場合)

   ```
   flexsnap_configure uninstall
   ```

   インストーラによって、ホストから関連する NetBackup Snapshot Manager コンテナパッケージのロード解除が開始されます。進行状況を示す次のようなメッセージが表示されます。

   ```
   Uninstalling NetBackup Snapshot Manager
   -----------------------------------------
   Stopping flexsnap-mongodb ... done
   Stopping flexsnap-rabbitmq ... done
   Stopping flexsnap-auth ... done
   Stopping flexsnap-core ... done
   Removing flexsnap-mongodb ... done
   Removing flexsnap-rabbitmq ... done
   Removing flexsnap-auth ... done
   Removing flexsnap-core ... done
   ```

```
Unloading flexsnap-mongodb ... done
Unloading flexsnap-rabbitmq ... done
Unloading flexsnap-auth ... done
Unloading flexsnap-core ... done
```

3. NetBackup Snapshot Manager コンテナが削除されたことを確認します。

   次の docker コマンドを使用します。

   (*Docker の場合*) `# sudo docker ps -a`

   (*Podman の場合*) `# sudo podman ps -a`

4. 必要に応じて、ホストから NetBackup Snapshot Manager コンテナイメージを削除します。

   Snapshot Manager をイメージと一緒にアンインストールするには、次のコマンドを使用します。

   ```
   flexsnap_configure uninstall --purge
   ```

   ホストにロードされている docker イメージを表示するには、次の docker コマンドを使用します。

   - (*Docker の場合*) `# sudo docker images -a`
   - (*Podman の場合*) `# sudo podman images -a`

   次の各コマンドを使用して、ホストから NetBackup Snapshot Manager コンテナイメージを削除します。

   - (*Docker の場合*) `# sudo docker rmi`*<image ID>*
   - (*Podman の場合*) `# sudo podman rmi`*<image ID>*

5. これにより、ホストで NetBackup Snapshot Manager のアンインストールが完了します。

   次の手順は、NetBackup Snapshot Manager を再配備することです。

   p.43 の「Docker/Podman 環境への NetBackup Snapshot Manager のインストール」を参照してください。

NetBackup Snapshot Manager 拡張機能の削除 - VM ベースまたは管理対象 Kubernetes クラスタベース

アンインストール中に、インストーラにより NetBackup Snapshot Manager 拡張機能ホストで次のタスクが実行されます。

- 稼働中のすべての NetBackup Snapshot Manager コンテナの停止
- NetBackup Snapshot Manager コンテナの削除

VM ベースの拡張機能をアンインストールするには

1. Docker 環境の場合:

   次のコマンドを実行します。

   ```
   # flexsnap_configure uninstall
   ```

2. 必要に応じて、拡張機能ホストから NetBackup Snapshot Manager コンテナイメージを削除します。

   ホストにロードされている docker イメージを表示して、ID に基づいて NetBackup Snapshot Manager イメージを削除するには、次の docker コマンドを使用します。

   ```
   # sudo docker images -a

   # sudo docker rmi <image ID>
   ```

これにより、VM ホストで NetBackup Snapshot Manager 拡張機能のアンインストールが完了します。

管理対象 Kubernetes クラスタベースの拡張機能をアンインストールするには

- 拡張機能のインストール時にダウンロードした拡張機能スクリプト `cp_extension.sh` を、`kubectl` がインストールされているホストから実行します。

  次のコマンドを実行します。

  ```
  bash cp_extension.sh uninstall
  ```

  アンインストールがトリガされた後、拡張機能サービスをアンインストールする必要がある名前空間を入力として指定します。

アンインストール後に、アンインストールした拡張機能に関連付けられているプロビジョニングされたクラウドリソースを終了または削除できます。

NetBackup Snapshot Manager のリストア

次のいずれかの方法を使用して NetBackup Snapshot Manager をリストアできます。

- クラウドにあるスナップショットを使用した NetBackup Snapshot Manager のリカバリ
- (GCP クラウドプロバイダの場合のみ) GCP クロスプロジェクトリストアを使用した NetBackup Snapshot Manager のリカバリ

クラウドにある NetBackup Snapshot Manager スナップショットの使用

クラウドにあるスナップショットを使用して NetBackup Snapshot Manager をリカバリするには

1. クラウドプロバイダのダッシュボードまたはコンソールを使用して、既存のスナップショットからボリュームを作成します。
2. 以前の NetBackup Snapshot Manager サーバーと同等以上の仕様の新しい仮想マシンを作成します。
3. 新しいサーバーに Docker/Podman をインストールします。

   p.34 の「コンテナプラットフォーム (Docker、Podman) のインストール」を参照してください。
4. 新しく作成されたボリュームをこの NetBackup Snapshot Manager サーバーインスタンスに接続します。
5. このサーバーに NetBackup Snapshot Manager のインストールディレクトリを作成します。

   次のコマンドを使用します。

   ```
   # mkdir /full_path_to_cloudpoint_installation_directory
   ```

   例:

   ```
   # mkdir /cloudpoint
   ```
6. 作成したインストールディレクトリに接続されたボリュームをマウントします。

   次のコマンドを使用します。

   ```
   # mount /dev/device-name
   /full_path_to_cloudpoint_installation_directory
   ```

   例:

   ```
   # mount /dev/xvdb /cloudpoint
   ```
7. 関連するすべての NetBackup Snapshot Manager 構成データとファイルがディレクトリにあることを確認します。

   次のコマンドを入力します。

   ```
   # ls -l /cloudpoint
   ```
8. NetBackup Snapshot Manager のインストーラバイナリを新しいサーバーにダウンロードするかコピーします。

9 NetBackup Snapshot Manager をインストールします。

次のコマンドを使用します。

(Docker/Podman の場合)

```
flexsnap_configure install
```

インストールプログラムは、NetBackup Snapshot Manager の既存のバージョンを検出し、既存の内容を上書きせずにすべての NetBackup Snapshot Manager サービスを再インストールします。

次のようなメッセージがコマンドプロンプトに表示されます。

```
Configuration started at time Wed May 13 22:20:47 UTC 2020
This is a re-install.
Checking if a 1.0 release container exists ...
```

操作が再インストールであることを示す行に注意してください。

10 インストールが完了したら、既存のクレデンシャルを使用して NetBackup Snapshot Manager での作業を再開できます。

14

NetBackup Snapshot Manager for Cloud のトラブルシューティング

この章では以下の項目について説明しています。

- 子ジョブが長時間ハングしているように見える
- (AWS の場合) ファイルシステムの整合性スナップショットではなく、クラッシュ整合スナップショットが作成される

NetBackup Snapshot Manager のトラブルシューティング

次のトラブルシューティングのシナリオを参照してください。

- NetBackup Snapshot Manager エージェントホストが突然再起動された場合、このエージェントが NetBackup Snapshot Manager サーバーへの接続に失敗する。
  この問題は、NetBackup Snapshot Manager エージェントがインストールされているホストが突然停止した場合に発生することがあります。ホストが正常に再起動した後でも、エージェントは NetBackup Snapshot Manager サーバーとの接続の確立に失敗し、オフライン状態になります。
  エージェントログファイルには、次のエラーが記録されます。

  ```
  Flexsnap-agent-onhost[4972] mainthread
  flexsnap.connectors.rabbitmq: error - channel 1 closed
  unexpectedly: (405) resource_locked - cannot obtain exclusive
  access to locked queue '
  flexsnap-agent.a1f2ac945cd844e393c9876f347bd817' in vhost '/'
  ```

  この問題は、エージェントホストが突然シャットダウンされた場合でも、エージェントと NetBackup Snapshot Manager サーバー間の RabbitMQ 接続が終了していないために発生します。エージェントホストでハートビートポーリングが失われるまで、NetBackup Snapshot Manager サーバーはそのエージェントを利用できないことを検出できません。RabbitMQ 接続は、次のハートビートサイクルまで開いたままになります。次のハートビートポーリングがトリガされる前にエージェントホストが再ブートすると、エージェントは NetBackup Snapshot Manager サーバーとの新しい接続の確立を試行します。ただし、以前の RabbitMQ 接続がすでに存在するため、新しい接続の試行はリソースのロックエラーで失敗します。
  この接続エラーが発生すると、エージェントはオフラインになり、ホストで実行されたすべてのスナップショット操作およびリストア操作が失敗します。
  回避方法:
  エージェントホストで Cohesity NetBackup Snapshot Manager Agent サービスを再起動します。

  - Linux ホストで、次のコマンドを実行します。

    ```
    # sudo systemctl restart flexsnap-agent.service
    ```

  - Windows ホストの場合:
    Windows サービスコンソールから `Cohesity NetBackup Snapshot Manager™ Agent` サービスを再起動します。

- Windows ホストでの NetBackup Snapshot Manager エージェント登録がタイムアウトまたは失敗することがある。

  Windows でアプリケーションを保護するには、Windows ホストに NetBackup Snapshot Manager エージェントをインストールして登録する必要があります。エージェントの登録には、通常よりも時間がかかることがあります。また、タイムアウトまたは失敗することがあります。

  回避方法:

  この問題を回避するには、次の手順を試行します。

  - 新しいトークンを使用して、Windows ホストにエージェントを再登録します。
  - 登録処理が再度失敗した場合は、NetBackup Snapshot Manager サーバーで NetBackup Snapshot Manager サービスを再起動してから、エージェントの登録を再試行します。

  詳しくは、次を参照してください。

  p.224 の「Windows ベースのエージェントの登録」を参照してください。
  p.66 の「NetBackup Snapshot Manager の再起動」を参照してください。

- DR パッケージが消失した場合、またはパスフレーズが失われた場合のディザスタリカバリ。

  この問題は、DR パッケージが失われた場合、またはパスフレーズが失われた場合に発生する可能性があります。

  カタログバックアップの場合、次の 2 つのバックアップパッケージが作成されます。

  - すべての証明書を含む DR パッケージ
  - データベースを含んでいるカタログパッケージ

  DR パッケージには NetBackup UUID 証明書が含まれ、カタログデータベースにも UUID があります。DR パッケージを使用してディザスタリカバリを実行し、その後にカタログリカバリを実行すると、UUID 証明書と UUID の両方がリストアされます。これにより、UUID が変更されないため、NetBackup は NetBackup Snapshot Manager と通信できるようになります。

  ただし、DR パッケージまたはパスフレーズが失われた場合は、DR 操作を完了できません。NetBackup の再インストール後に、DR パッケージなしでのみカタログをリカバリできます。この場合、NetBackup Snapshot Manager で認識されない新しい UUID が NetBackup に対して作成されます。NetBackup と NetBackup Snapshot Manager との 1 対 1 のマッピングは失われます。

  回避方法:

  この問題を解決するには、NetBackup プライマリが作成された後で新しい NBU UUID とバージョン番号を更新する必要があります。

  - このタスクを実行するためには、NetBackup 管理者が NetBackup Web 管理サービスにログインしている必要があります。次のコマンドを使用してログオンします。

    ```
    /usr/openv/netbackup/bin/bpnbat -login -loginType WEB
    ```

- プライマリサーバーで次のコマンドを実行して、NBU UUID を取得します。
  `/usr/openv/netbackup/bin/admincmd/nbhostmgmt -list -host <primary server host name> | grep "Host ID"`
- 次のコマンドを実行してバージョン番号を取得します。
  `/usr/openv/netbackup/bin/admincmd/bpgetconfig -g <primary Ssrver host name> -L`

NBU UUID とバージョン番号を取得した後、NetBackup Snapshot Manager ホストで次のコマンドを実行してマッピングを更新します。

`/cloudpoint/scripts/cp_update_nbuuid.sh -i <NBU UUID> -v <Version Number>`

- マスターサーバーで ECA_CRL_CHECK が無効な場合、スナップショットジョブは成功するが、バックアップジョブがエラー「NetBackup Snapshot Manager の証明書が無効か存在しません。(The NetBackup Snapshot Managers certificate is not valid or doesn't exist.) (9866)」で失敗する。
  ECA_CRL_CHECK がマスターサーバーで構成され、無効になっている場合は、NetBackup Snapshot Manager の `bp.conf` セットアップでも同じ値を使用して構成する必要があります。
  たとえば、NetBackup で外部証明書が構成されており、証明書が失効している場合に、スナップショットからバックアップを実行するシナリオがあるとします。この場合、マスターで ECA_CRL_CHECK が DISABLE に設定されているときは、NetBackup Snapshot Manager 設定の `bp.conf` でも同じ値を設定します。そうしないと、スナップショット操作は成功しても、バックアップ操作は証明書エラーで失敗します。
  p.259 の「Azure Stack のセキュリティの構成 」を参照してください。
- ファイアウォールが無効な場合、RHEL システムで NetBackup Snapshot Manager のクラウド操作が失敗する
  NetBackup Snapshot Manager サービスの実行中に RHEL システムでファイアウォールが無効になっている場合、RHEL システムでサポートされるすべてのクラウドプラグインで NetBackup Snapshot Manager 操作が失敗します。これはネットワーク構成の問題で、NetBackup Snapshot Manager がクラウドプロバイダの REST API エンドポイントにアクセスできないようにします。
  回避方法:
  - NetBackup Snapshot Manager を停止します
    `flexsnap_configure stop`
  - Docker を再起動します。
    `# systemctl restart docker`
  - NetBackup Snapshot Manager を再起動します
    `flexsnap_configure start`
- スナップショットジョブとインデックス付けジョブからのバックアップがエラーで失敗する

```
Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) SSL
Connection failed with string, broker:<hostname>
Jun 10, 2021 2:17:48 PM - Error mqclient (pid=1054) Failed SSL
handshake, broker:<hostname>
Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Invalid
operation for asset: <asset_id>
Jun 10, 2021 2:19:16 PM - Error nbcs (pid=29079) Acknowledgement
not received for datamover <datamover_id>
```

および/または

```
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - Cannot retrieve the exported snapshot details
for the disk with UUID:<disk_asset_id>
Jun 10, 2021 3:06:13 PM - Info bptm (pid=32582) waited for full
buffer 1 times, delayed 220 times
Jun 10, 2021 3:06:13 PM - Critical bpbrm (pid=32373) from client
<asset_id>: FTL - cleanup() failed, status 6
```

これは、ポート 5671 および 443 での NetBackup Snapshot Manager へのインバウンドアクセスが OS ファイアウォールレベル (firewalld) でブロックされた場合に発生する可能性があります。それにより、(スナップショットおよびインデックス付けジョブからのバックアップに使用される) datamover コンテナから、NetBackup Snapshot Manager への通信が遮断されます。その結果、datamover コンテナはバックアップまたはインデックス付けを開始できません。
回避方法:
OS ファイアウォールのルールを変更して、ポート 5671 および 443 からのインバウンド接続を許可します。

- VM のエージェントレス接続が失敗し、エラーメッセージが表示される。
  ユーザーが、ポータルを介して VM の認証形式を SSH キーベースからパスワードベースに変更すると、VM のエージェントレス接続が失敗し、次のエラーメッセージが表示されます。

  ```
  User does not have the required privileges to establish an
  agentless connection
  ```

  このエラーメッセージが示すように、この問題は sudoers ファイルでユーザーの権限が正しく定義されていない場合に発生します。
  回避方法:
  パスワードレスの sudo 操作を実行するために必要な権限を指定することで、ユーザーの sudoers ファイルの問題を解決します。

- プライベートサブネット (インターネットなし) に NetBackup Snapshot Manager を配備すると、NetBackup Snapshot Manager 機能が失敗する

この問題は、ファイアウォールが有効になっているプライベートネットワークまたは無効なパブリック IP に NetBackup Snapshot Manager が配備されている場合に発生します。顧客の情報セキュリティチームでは、仮想マシンへのフルインターネットアクセスが許可されない場合があります。

回避方法:

次のコマンドを使用して、ファイアウォールのコマンドラインからポートを有効にします。

```
firewall-cmd --add-port=22/tcp
firewall-cmd --add-port=5671/tcp
firewall-cmd --add-port=443/tcp
```

- バックアップコピーからの資産のリストアが失敗する

  一部のシナリオでは、Docker コンテナで接続が断続的にリセットされる場合があります。このため、サーバーは、アドバタイズされたクライアントウィンドウよりも多い tcp ペイロードを送信します。Docker コンテナは、新しい TCP 接続ハンドシェークからの SYN+ACK パケットをドロップする場合があります。これらのパケットを許可するには、`nf_conntrack_tcp_be_liberal` オプションを使用します。

  `nf_conntrack_tcp_be_liberal = 1` の場合、次のパケットが許可されます。

  - ACK が下限を下回っている (ACK の過度な遅延の可能性)
  - ACK が上限を超えている (ACK 処理されたデータがまだ見られない)
  - SEQ が下限を下回っている (すでに ACK 処理されたデータが再送信された)
  - SEQ が上限を超えている (レシーバのウィンドウを超えている)

  `nf_conntrack_tcp_be_liberal = 0` の場合、これらも無効として拒否されます。

  回避方法:

  バックアップコピーからのリストアの問題を解決するには、`nf_conntrack_tcp_be_liberal = 1` オプションを使用して、datamover コンテナを実行中のノードでこの値を設定します。

  `nf_conntrack_tcp_be_liberal` の値を設定するには、次のコマンドを使用します。

  ```
  sysctl -w net.netfilter.nf_conntrack_tcp_be_liberal=1
  ```

- Kubernetes 拡張機能の一部のポッドが完了状態に進んだ

  回避方法:

  Kubernetes 拡張機能を無効にします。

  次のコマンドを使用してリスナーポッドを削除します。

  ```
  #kubectl delete pod flexnsap-listener-xxxxx -n <namespace>
  ```

  Kubernetes 拡張機能を有効にします。

- ユーザーがクラウド保護計画をカスタマイズできない

  回避方法:

  目的の構成を使用して新しい保護計画を作成し、資産に割り当てます。

- デフォルトの 6 時間のタイムアウトでは、大きいデータベース (サイズが 300 GB を超える) をリストアできない
  回避方法:
  より大きいデータベースをリストアできるように、構成可能なタイムアウトパラメータ値を設定できます。タイムアウト値は、`flexsnap-coordinator` コンテナの `/etc/flexsnap.conf` ファイルで指定できます。コーディネータコンテナの再起動は必要ありません。タイムアウト値は、次のデータベースリストアジョブで読み取られます。
  ユーザーは、タイムアウト値を次のように秒単位で指定する必要があります。

```
docker exec -it flexsnap-coordinator bash
root@flexsnap-coordinator:/# cat /etc/flexsnap.conf [global] target
= flexsnap-rabbitmq grt_timeout = 39600
```

- バックアップからリストアされた VM に 50 個のタグがアタッチされていると、リストアされたホストへのエージェントレス接続と個別リストアが失敗する
  回避方法:
  (AWS の場合) バックアップからリストアされた Windows VM に 50 個のタグがあり、プラットフォームタグがない場合、ユーザーは不要なタグを削除して Platform: windows タグを追加できます。

- いくつかの GKE バージョンでは、失敗したポッドの問題が名前空間で発生する
  名前空間では、次のようにいくつかの失敗したポッドが `NodeAffinity` というエラー状態で表示されます。

```
$ kubectl get pods -n <cp_extension_namespace>

NAME                                          READY     STATUS
  RESTARTS     AGE
flexsnap-datamover-
2fc2967943ba4ded8ef653318107f49c-664tm        0/1     Terminating
    0          4d14h
flexsnap-fluentd-collector-c88f8449c-5jkqh    0/1     NodeAffinity
   0          3d15h
flexsnap-fluentd-collector-c88f8449c-ph8mx    0/1     NodeAffinity
   0          39h
flexsnap-fluentd-collector-c88f8449c-rqw7w    1/1     Running
    0          10h
flexsnap-fluentd-collector-c88f8449c-sswzr    0/1     NodeAffinity
   0          5d18h
flexsnap-fluentd-ftlnv                        1/1     Running
    3 (10h ago)10h
flexsnap-listener-84c66dd4b8-6l4zj            1/1     Running
    0          10h
flexsnap-listener-84c66dd4b8-ls4nb            0/1     NodeAffinity
```

```
   0          17h
flexsnap-listener-84c66dd4b8-x84q8           0/1     NodeAffinity
   0          3d15h
flexsnap-listener-84c66dd4b8-z7d5m           0/1     NodeAffinity
   0          5d18h
flexsnap-operator-6b7dd6c56c-cf4pc            1/1     Running
    0          10h
flexsnap-operator-6b7dd6c56c-qjsbs           0/1     NodeAffinity
   0          5d18h
flexsnap-operator-6b7dd6c56c-xcsgj           0/1     NodeAffinity
   0          3d15h
flexsnap-operator-6b7dd6c56c-z86tc           0/1     NodeAffinity
   0          39h
```

ただし、これらのエラーは、NetBackup Snapshot Manager Kubernetes 拡張機能の機能には影響しません。

回避方法:

次のコマンドを使用して、失敗したポッドを手動でクリーンアップします。

```
kubectl get pods -n <cp_extension_namespace> | grep NodeAffinity
| awk '{print $1}' | xargs kubectl delete pod -n
<cp_extension_namespace>
```

- NetBackup Snapshot Manager 登録が以前に失敗している場合、プラグイン情報が重複する

  これは、MarketPlace 配備メカニズムを使用して NetBackup Snapshot Manager が配備されている場合にのみ発生します。この問題は、登録前にプラグイン情報が追加されている場合に発生します。この問題により、CloudPoint_plugin.conf ファイルに、重複するプラグイン情報が作成されます。

  回避方法:

  重複したプラグイン情報を CloudPoint_plugin.conf ファイルから手動で削除します。たとえば、CloudPoint_plugin.conf ファイルに GCP プラグイン構成の重複エントリ (太字) がある、次のような例を考えてみます。

```
{
    "CPServer1": [
      {
        "Plugin_ID": "test",
        "Plugin_Type": "aws",
        "Config_ID": "aws.8dda1bf5-5ead-4d05-912a-71bdc13f55c4",
        "Plugin_Category": "Cloud",
        "Disabled": false
      }
    ]
  },
```

```
{
  "CPServer2": [
    {
      "Plugin_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Type": "gcp",
      "Config_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Category": "Cloud",
      "Disabled": false
    },
    {
      "Plugin_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Type": "gcp",
      "Config_ID": "gcp.2080179d-c149-498a-bf1f-4c9d9a76d4dd",
      "Plugin_Category": "Cloud",
      "Disabled": false
    }
  ]
}
```

- NetBackup Snapshot Manager のクローンが NetBackup に追加されるとプラグイン情報が重複する

  これは、NetBackup Snapshot Manager を RHEL 8.6 VM に移行するときに、NetBackup Snapshot Manager のクローンが NetBackup に追加された場合にのみ発生します。NetBackup Snapshot Manager のクローン作成では、既存の NetBackup Snapshot Manager ボリュームを使用して新しい NetBackup Snapshot Manager が作成されます。これにより、重複するエントリが CloudPoint_plugin.conf ファイルに作成されます。

  回避方法:

  重複したプラグイン情報を CloudPoint_plugin.conf ファイルから手動で編集および削除します。

  たとえば、CloudPoint_plugin.conf ファイルに Azure プラグイン構成の重複エントリ (太字) がある、次のような例を考えてみます。

```
{
    "CPServer1": [
      {
        "Plugin_ID": "config10",
        "Plugin_Type": "azure",
       "Config_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

        "Plugin_Category": "Cloud",
        "Disabled": false
      }
```

```
    ]
  },
  {
    "CPServer2": [
      {
       "Plugin_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

        "Plugin_Type": "azure",
       "Config_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

        "Plugin_Category": "Cloud",
        "Disabled": false
      },
       {
    "cpserver101.yogesh.joshi2-dns-zone": [
      {
       "Plugin_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

        "Plugin_Type": "azure",
       "Config_ID": "azure.327ec7fc-7a2d-4e94-90a4-02769a2ba521",

        "Plugin_Category": "Cloud",
        "Disabled": false
      },
      {
        "Plugin_ID": "AZURE_PLUGIN",
        "Plugin_Type": "azure",
       "Config_ID": "azure.4400a00a-8d2b-4985-854a-74f48cd4567e",

        "Plugin_Category": "Cloud",
        "Disabled": false
      }
    ]
  }
 ]
}
```

- Azure に配備された Snapshot Manager バージョン 10.0 を使用したスナップショット操作からのバックアップが、SSL 証明書エラーにより失敗する
  Azure に配備された Snapshot Manager バージョン 10.3 以降を使用したスナップショット操作からのバックアップが、CRL (curl) に関連する SSL 証明書エラーにより失敗します。
  回避方法:

Snapshot Manager `bp.conf` ファイルに `ECA_CRL_CHECK = 0` を追加し、Azure エンドポイントがメディアサーバーからアクセスできることを確認します。

Windows インスタンスが NetBackup Snapshot Manager ホストとの接続性を失った場合、SQL スナップショットまたはリストアおよび個別リストア操作が失敗する

この問題は、Windows インスタンスで設定されている NetBackup Snapshot Manager エージェントが、NetBackup Snapshot Manager ホストとのネットワーク接続性を失った場合に発生します。SQL Server のスナップショットの作成またはリストアおよび個別リストアなどの NetBackup Snapshot Manager 操作が、Windows インスタンスで失敗し始めます。

NetBackup Snapshot Manager ソフトウェアのアップグレードや一般的なネットワークの停止の一環として、NetBackup Snapshot Manager ホストでのサービスの再起動など、さまざまな理由により接続エラーが発生することがあります。

flexsnap エージェントのログに次のようなメッセージが出力されることがあります。

```
flexsnap-agent-onhost[2720] MainThread flexsnap.connectors.rabbitmq:
ERROR - Unexpected exception() in main loop
flexsnap-agent-onhost[2720] MainThread agent: ERROR - Agent failed
unexpectedly
```

NetBackup Snapshot Manager が Cohesity NetBackup 環境に配備されている場合、NetBackup ログに次のようなメッセージが含まれることがあります。

```
Error nbcs (pid=5997) Failed to create snapshot for asset: <sqlassetname>
Error nbcs (pid=5997) Operation failed. Agent is unavailable.
```

回避方法:

この問題を解決するには、Windows インスタンスで `Cohesity NetBackup Snapshot Manager` **エージェント**サービスを再起動します。

元のディスクがインスタンスから切断されていると、ディスクレベルのスナップショットのリストアが失敗する

この問題は、同じ場所へのディスクレベルのスナップショットのリストアを実行している場合に発生します。

同じ場所にディスクレベルのスナップショットのリストアをトリガすると、最初に NetBackup は既存の元のディスクをインスタンスから切断し、ディスクのスナップショットから新しいボリュームを作成して、その新しいボリュームをインスタンスに接続します。元のディスクは、リストア操作が正常に完了した後に自動的に削除されます。

ただし、リストアがトリガされる前に、スナップショットをリストアしている元のディスクがインスタンスから手動で切断された場合、リストア操作は失敗します。

NetBackup UI に次のメッセージが表示されることがあります。

```
Request failed unexpectedly: [Errno 17] File exists:
'/<app.diskmount>'
```

NetBackup コーディネータのログに次のようなメッセージが出力されます。

```
flexsnap.coordinator: INFO - configid : <app.snapshotID> status
changed to
 {u'status': u'failed', u'discovered_time': <time>, u'errmsg': u'
Could not connect to <application> server localhost:27017:
[Errno 111]Connection refused'}
```

回避方法:

リストアが環境ですでに失敗している場合、最初にディスクのクリーンアップを手動で実行し、次にリストアジョブを再びトリガする必要がある場合があります。

次の手順を実行します。

1. リストア操作が失敗したインスタンスにログオンします。

   接続に使用するユーザーアカウントに、インスタンスに対する管理権限があることを確認します。

2. 次のコマンドを実行して、アプリケーションディスクを正常にマウント解除します。

   ```
   # sudo umount /<application_diskmount>
   ```

   ここで、<application_diskmount> はインスタンスの元のアプリケーションディスクマウントパスです。

   「デバイスがビジー状態」であることを示すメッセージが表示された場合は、しばらく待ってから、umount コマンドを再度実行してください。

3. NetBackup UI からディスクレベルのリストア操作を再びトリガします。

通常、インスタンスから元のアプリケーションディスクを切断する場合は、次のリストア処理を実行します。

1. 最初に、インスタンスのディスクレベルのスナップショットを作成します。
2. スナップショットが正常に作成された後、手動でインスタンスからディスクを切断します。

たとえば、インスタンスが AWS クラウドにある場合は、AWS 管理コンソールを使用して、インスタンスを編集してデータディスクを切断します。インスタンスに変更を保存していることを確認します。

3. 管理者ユーザーアカウントを使用してインスタンスにログオンし、次のコマンドを実行します。

   ```
   # sudo umount /<application_diskmount>
   ```

   「デバイスがビジー状態」であることを示すメッセージが表示された場合は、しばらく待ってから、umount コマンドを再度実行してください。

4. NetBackup UI からディスクレベルのリストア操作をトリガします。

システム管理 ID を制御ノードプールに割り当てた後も検出が機能しない

システム管理 ID が NetBackup Snapshot Manager (Kubernetes クラスタに配備) で有効になっておらず、ユーザーがシステム管理 ID を使用して Azure クラウドプロバイダを (すでに追加されているユーザー管理 ID を使用して) 追加した場合、Azure クラウドプロバイダの追加のためにユーザー管理 ID は自動的に選択され、プラグインの追加が成功します。

ただし、システム管理 ID に十分な権限が追加されていないと、資産は検出できません。後からシステム管理 ID を有効にし、必要な権限/役割をシステム管理 ID に追加しても、検出や NetBackup Snapshot Manager 関連の操作は機能しません。これは、NetBackup Snapshot Manager のバックエンドでは常にユーザー管理 ID が使用されるためです。

この問題を解決するには、次の手順を実行します。

1 必要な権限または役割を更新してからユーザー管理 ID に権限を追加し、必要な操作を再実行します。

2 NetBackup Web UI で対応する Azure プロバイダ構成を編集し、必要な操作を再実行します。

次の表に、さまざまな Azure プラグイン構成のシナリオと予想される結果を示します。

表 14-1 さまざまな Azure プラグイン構成のシナリオと予想される結果

NetBackup Snapshot Manager 構成	Azure での VM の構成		スナップショット
	システム管理 ID (MI)	ユーザー管理 ID (MI)	
System MI	CP-Permissions	該当なし	はい
	該当なし	CP-Permissions	はい
	該当なし	■ CP-Permissions ■ Reader	該当なし
	Reader	CP-Permissions	いいえ
	CP-Permissions	Reader	はい
	Reader	Reader	いいえ
	CP-Permissions	CP-Permissions	はい
User MI	CP-Permissions	該当なし	該当なし
	該当なし	CP-Permissions	はい
	Reader	CP-Permissions	はい
	CP-Permissions	Reader	いいえ
	Reader	Reader	いいえ
	CP-Permissions	CP-Permissions	はい
User MI (Reader)	該当なし	■ CP-Reader ■ CP-Permissions	いいえ

メモ: 上記の表では、CP-Permissions はスナップショットを取得する権限を持つ役割であり、Reader はスナップショットを取得する権限を持たない役割です。

スナップショットからの GCP バックアップでのパフォーマンスの問題

スナップショット操作からの GCP バックアップの際、データは Snapshot Manager に接続された永続ディスクから読み取られます。読み取り操作が、同じマシン上の複数のディスクで行われている場合、永続ディスクの IOPS 速度はディスク間で分散されます。

スナップショット操作からの GCP バックアップの場合、最大 15 のジョブを (15 を上回るジョブに対応できるマシンで) 起動できます。マシンで対応できるジョブ数が 15 未満の場合は、スナップショット操作からの多数のバックアップを NetBackup Snapshot Manager で並行して実行できます。

スナップショットジョブからのバックアップが複数実行されている場合、単一ディスクでの効果的な IOPS = マシンでの読み取り操作における 1 秒あたりのディスク入出力操作 (IOPS) の合計 / 読み取り操作が進行中のディスクの数となります。このため、多数の並列バックアップジョブを実行している場合、サイズが大きい VM のバックアップ時間が長くなります。

パフォーマンスを改善するには、次の手順を実行します。

1. NetBackup Snapshot Manager に対し、より高い設定を選択します。

   GCP ディスクの IOPS は、VM の種類、ディスクの種類、ディスクのサイズ、CPU などの要因によって変わります。

   IOPS を上げるため、より高い設定を選択します。詳しくは、「パフォーマンス要件を満たすようにディスクを構成する」を参照してください。

2. NetBackup Snapshot Manager で実行するジョブの数を制限します。

   `/cloudpoint/flexsnap.conf` ファイルの次の設定を使用して、NetBackup Snapshot Manager で実行する並列ジョブの数を制限します。

   ```
   [capability_limit]
   max_jobs = <num>
   ```

   NetBackup Snapshot Manager マシンの性能が `max_jobs` を下回る場合は、マシンの性能が考慮されます。マシンの性能が `max_jobs` を上回る場合は、`max_jobs` の値を使用して、マシンで実行される NetBackup Snapshot Manager ジョブ数が決定されます。

   たとえば、max_jobs=8 の場合、最大 8 GB のメモリが利用可能です。これにより、32 のメモリのチャンク (チャンクあたり 8 GB/ 0.256 GB) と 8 つのジョブのみのうち、上限を超えたジョブによって新しいタスクのスケジュール設定が停止されます。

   構成を変更したら、NetBackup Snapshot Manager を再起動し、NetBackup で手動検出を実行します。

/dev/mapper/<VG>-<LV> のスーパーブロックの読み取り失敗

OCI インスタンスのインプレースリストアの後、LVM がディスクパーティションの一部として作成された場合、LVM はボリュームグループの状態を判断できず、LVM はデフォルトではマウントされません。

回避方法:

ボリュームグループを再アクティブ化して問題を解決するには、次のコマンドを 1 つずつ実行してください。

```
vgchange -a n <volume group name>
```

```
vgchange -a y <volume group name>
```

```
mount /dev/<volume group name>/<Logical_Volume> <mount_point>
```

ホストエージェントでの移行後にエラーメッセージが表示されて失敗する

ホストエージェントでの移行後に次のエラーメッセージが表示されて失敗します。

```
[1864] Failed to execute script flexsnap-agent
```

この問題を解決するには、次の該当するコマンドを実行します。

- Windows の場合: コマンドプロンプトで、エージェントのインストールディレクトリ (`C:¥Program Files¥Veritas¥CloudPoint¥`) に移動して、次のコマンドを実行します。
  ```
  #flexsnap-agent.exe --renew --token <auth_token>
  ```
  このコマンドは最初の試行で失敗します。コマンドを再実行して、成功させます。
- Linux の場合: Linux ホストで次のコマンドを再実行します。
  ```
  sudo flexsnap-agent --renew --token <auth_token>{}
  ```

ファイルのリストアジョブがエラーメッセージで失敗する

ファイルのリストアジョブが失敗し、次のエラーメッセージがアクティビティモニターに表示されます。

```
Unable to detect volume for disk <disk_name>
```

この問題を解決するには、次を実行します。

- ネットワークデバイスがデバイスに接続されている場合は、切断します。
- 管理者権限でコマンドプロンプトを開き、次のコマンドを実行します。
  ```
  diskpart
  ```
- diskpart プロンプト内で「rescan」と入力し、Enter キーを押します。
- diskpart プロンプトとコマンドラインを終了します。
- ファイルのリストア操作を再度実行します。

データムーバーの通知が受信されない

データムーバーの通知が受信されない場合に、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。

```
Oct 10, 2022 5:06:21 AM - begin SnapDupe Mount: Import Snapshot
Oct 10, 2022 5:06:21 AM - Info nbjm (pid=7578)
BackupId=aws-ec2-us-east-2-xxxxxxxxxxxxx_1665303611
Oct 10, 2022 5:06:23 AM - Info nbcs (pid=523) Start
Oct 10, 2022 5:06:23 AM - Info nbcs (pid=523)
Requesting data mover container
Oct 10, 2022 5:18:36 AM - Error nbcs (pid=523)
Invalid operation for asset: aws-ec2-us-east-2-xxxxxxxxxxxxx
Oct 10, 2022 5:18:36 AM - Error nbcs (pid=523)
Acknowledgment not received for datamover
datamover.a2d3dc2249da45a0a839bc77eface2a4
Oct 10, 2022 5:18:36 AM - Info nbcs (pid=523) End
```

上記のエラーメッセージは、次の場合にクラスタで発生します。

- ポッドが ContainerCreating の状態です。例:

```
flexsnap-workflow-general-1665398188-4d03f27e-fblxb
                                    0/1     ContainerCreating   0
    142m
flexsnap-workflow-general-1665398188-538a8846-zrgtl
                                    0/1     ContainerCreating   0
    142m
flexsnap-workflow-general-1665398188-87cb301a-5bqss
                                    0/1     ContainerCreating   0
    142m
flexsnap-workflow-general-1665398188-f61f5f42-g2rhv
                                    0/1     ContainerCreating   0
    142m
```

- 説明ポッドで、次のようにイベントが表示されます。

```
 Type     Reason                  Age                    From
Message
 ----   ------                  ----                   ----
-------
  Normal   SandboxChanged          25m (x1874 over 140m)  kubelet

  Pod sandbox changed, it will be killed and re-created.
  Warning  FailedCreatePodSandBox  56s (x2079 over 140m)  kubelet
```

```
  (combined from similar events): Failed to create pod sandbox:
  rpc error: code = Unknown desc
=failed to set up sandbox container
"45f90b441cc4ea83efca63eacff1028779d4114fb213a5200e76f2e25373e054"

  network for pod
"flexsnap-workflow-general-1665398189-f46e636e-vrcdz":
  networkPlugin cni failed to set up pod
"flexsnap-workflow-general-1665398189-f46e636e-vrcdz_nbuxsystest"

network: add cmd: failed to assign an IP address to container
```

この問題を解決するには、AWS のトラブルシューティングのセクションを参照し、ソリューションを実装します。トラブルシューティングについて詳しくは、AWS のサポートにお問い合わせください。

Google Cloud Platform でディスクのスナップショット ID が表示される

GCP では、(設計上) ユーザーが GCP コンソールでスナップショット ID を表示することはできません。

回避方法:

ユーザーは gcloud CLI を通して次の問い合わせを使ってスナップショット ID 名を取得できます。

例: `Snapshot ID: google-gcepdsnap-us-west1-a-6370700417460427698`

次の出力が表示されます。

```
$gcloud compute snapshots list --filter="id='6370700417460427698'"
NAME: nbu133419417943333447O1snap1736762714
DISK_SIZE_GB: 20
SRC_DISK: us-east1-b/disks/ranjit-test1-lx
STATUS: READY
```

NetBackup Snapshot Manager バージョン 11.x へのアップグレード後に、接続済みまたは構成済みのクラウド VM のアプリケーション状態にエラーが表示される

Linux と Windows サーバープラットフォームで RPM または MSI インストーラを使って、配備された以前のバージョンのオンホストエージェントが、それぞれ NetBackup Snapshot Manager に接続できないことがあります。この問題は、NetBackup Snapshot Manager で使用されている OpenSSL のバージョンとオンホストエージェントの以前のバージョン間の不一致が原因で発生します。

flexsnap ログでは、次のようなエラーが表示されます。

```
834b7a6daed641f340577844d22d6ecc7a714a30e3fa2f5e960bc15cd65f1191:
"2024-12-10T14:40:12.375335088+05:30 ^[[38;5;87m2024-12-10
09:10:12.375116+00:00 [notice] <0.2749.0> TLS server: In state
wait_cert_verify received CLIENT ALERT: Fatal - Handshake Failure^[[0m
```

回避方法:

この問題を解決するには、次の手順を実行します。

- Linux または Windows プラットフォームのオンホストエージェントをアップグレードします。
- アップグレード後に、flexsnap ログにエラーが表示されていないことを確認します。[作業負荷 (Workloads)]、[クラウド (Cloud)]、[仮想マシン (Virtual machines)] タブの順に移動し、[アプリケーションの状態 (Application state)] が[接続状態 (connected)]または[設定済み (configured)]に変更されているかどうかを確認します。

p.294 の「アップグレード後のタスク」を参照してください。

バックアップジョブとリストアジョブがタイムアウトエラーで失敗する

NetBackup Snapshot Manager サーバー上のリソース可用性の低下が原因で、ジョブが継続的にメモリを検索している状態になるため、バックアップジョブとリストアジョブが失敗します。このため、他のサービスもタイムアウトエラーで失敗する可能性があります。この問題は、ホストの容量を超えて複数のジョブが同時に実行されている場合に発生する可能性があります。クラスタ設定では、ノードあたりの最大ポッド数の設定により、ジョブがノードでのスケジュール設定に失敗する場合があります。ノードあたりの最大ポッド数がノードの容量に従った推奨値より小さい数に設定されている場合、バックアップジョブまたはリストアジョブが失敗することがあります。

回避方法:

この問題を解決するには、ホストを次のように手動で構成し、単一ノードで一度に実行できるジョブの最大数を設定します。

- ホスト: `/cloudpoint/flexsnap.conf` ファイルを使用
  または
- クラスタ: `flexsnap-conf` 構成マップを使用

```
[capability_limit]
max_jobs = <num>
```

ここで、**<num>** は、ノード上で一度に実行できるジョブの最大数です。

複数のジョブが平行して実行されるケースで、リソースの可用性が十分でないためにサービスが失敗する場合は、指定されたノード形式で実行できる並列ジョブの数を減らします。

暗号化キーを使用した GCP リストアがエラーメッセージで失敗する

暗号化キーを使用した GCP リストアが、次のエラーメッセージで失敗しました。

```
Creating disk "disk1" failed. Error: Cloud KMS error when using key
projects/cloudpoint-development/locations/global/keyRings/test-ring/cryptoKeys/test-key2:
Permission 'cloudkms.cryptoKeyVersions.useToEncrypt' denied on
resource
'projects/cloudpoint-development/locations/global/keyRings/test-ring/cryptoKeys/test-key2'
(or it may not exist).
```

回避方法:

Google Cloud Platform は、
`service-<default-service-account>@compute-system.iam.gserviceaccount.com` サービスアカウントで欠落している `Cloud KMS CryptoKey Encrypter/Decrypter` 権限で構成されています。

この問題を解決するには、サービスアカウントに次の権限を割り当てます。

```
bash# gcloud kms keys add-iam-policy-binding test-key2 --keyring
test-ring --location global --member
serviceAccount:service-<default-service-account>@compute-system.iam.gserviceaccount.com
 --role roles/cloudkms.cryptoKeyEncrypterDecrypter

Updated IAM policy for key [test-key2].
bindings:
```

```
- members:
  -
serviceAccount:service-<default-service-account>@compute-system.iam.gserviceaccount.com

  role: roles/cloudkms.cryptoKeyEncrypterDecrypter
etag: BwX-yNgMdSE=
version: 1
```

検出後に Amazon Redshift クラスタおよびデータベースを利用できない

説明:

このエラーは、検出を実行する NetBackup Snapshot Manager に Redshift クラスタへのアクセス権がない場合に表示されます。flexsnap のログに次のエラーが表示されます。

```
Connect timeout on endpoint URL:
"https://redshift.us-east-2.amazonaws.com/
```

回避方法:

アクセス権がない場合、Snapshot Manager では、「Redshift サービスの VPC エンドポイント」のセキュリティグループに含まれるスナップショットマネージャに対してインバウンドルールを設定する必要があります。

AWS ポータルで、クラスタを選択します。[Properties]、[Network and security settings]、[virtual private cloud object]、[Endpoints]の順に選択します。検索フィールドで「redshift-endpoint」を検索し、VPC エンドポイント ID をクリックして[Security Groups]タブをクリックします。[Security Group ID]、[Edit Inbound rules]の順に選択して、スナップショット管理サーバーに次を追加します。

```
Type : HTTPS

Protocol : TCP

Port range : 443

Source : 10.177.77.210/32
```

* ここで、ソースは Snapshot Manager インスタンスを参照します。

NetBackup Web UI からリカバリを再び実行します。

共有 VPC サブネットが表示されない

VPC を別のアカウントと共有するアカウントに AWS プラグインを構成するときに、VPC を所有するアカウントがプラグインとして構成されていない場合、レプリカまたはバックアップからのリストア中に共有 VPC サブネットが表示されません。

回避方法:

VPC を所有するアカウントのプラグイン構成を追加し、その VPC の下にあるサブネットリソースの Name タグを設定します。

または

レプリカまたはバックアップコピーから共有 VPC のサブネットに VM をリカバリするには、リストア API を使用します。

コンテナマネージャがエフェメラル登録コンテナを適時に量産しないことがある

システムリソースの使用率が高いために、コンテナマネージャ (Podman/Docker) がエフェメラル登録コンテナを適時に量産しない場合があります。これらのエフェメラルコンテナは、ランダムに生成されたトークンでサービスを登録するために使用されます。コンテナマネージャがエージェント登録のエフェメラルコンテナを量産するのにトークンの有効期限の制限を超える場合、登録は正しく続行されず、資産を検出できません。

回避方法:

1. 実行中の既存のジョブがないことを確認し、NetBackup Snapshot Manager を NetBackup Web UI から無効にします。
2. `<flexsnap-agent>-temp` コンテナを停止します。
3. 前述の手順 1 で、子コンテナのオフホストエージェントの親コンテナを停止します。
4. `flexsnap-coordinator` サービスを再起動して、プロセスを再試行します。
5. NetBackup Web UI から NetBackup Snapshot Manager を有効にします。

VM からの GCP リストアがファイアウォールルールの取得に失敗する

VM から GCP リストアを実行すると、Web UI に次のエラーメッセージが表示されて処理が失敗します。

```
Snapshot Manager failed to retrieve network security groups against
 the specified plug-in instance.
```

回避方法:

GCP プロバイダの構成に使用されるサービスアカウントに割り当てられた役割に、次の必要な権限を提供します。

```
compute.networks.getEffectiveFirewalls
```

パラメータ化された VM のリストアで暗号化キーの取得に失敗する

(GCP の場合) パラメータ化された VM のリストアを実行すると、Web UI に次のエラーメッセージが表示されて、暗号化キーの取得に失敗します。

```
Snapshot Manager failed to retrieve encryption keys for the specified
 plugin instance.
```

回避方法:

GCP プロバイダの構成に使用されるサービスアカウントに割り当てられた役割に、次の必要な権限を付与します。

```
"cloudkms.cryptoKeys.get",
"cloudkms.cryptoKeyVersions.get",
"cloudkms.cryptoKeys.list",
"cloudkms.keyRings.list",
"cloudkms.cryptoKeyVersions.useToDecrypt",
"cloudkms.cryptoKeyVersions.useToEncrypt",
"cloudkms.locations.get",
"cloudkms.locations.list"
```

セキュリティの形式がトラステッド起動の VM のスナップショットからのリストアが失敗する

セキュリティタイプが*トラステッド起動の* VM のスナップショットが 10.2.0.1 より前の NetBackup Snapshot Manager バージョンから取得された場合、リストアが次のエラーで失敗します。

```
Failure: flexsnap.GenericError: (BadRequest) Security type of VM is
 not compatible with the security type of attached OS Disk..Code:
BadRequest.Message:
Security type of VM is not compatible with the security type of
attached OS Disk.
```

回避方法:

次の手順を実行して、スナップショットからのリストアを有効にします。

1. Microsoft Azure portal にサインインします。
2. 検索ボックスに、「リストアポイントコレクション」と入力します。
3. `nbsm-rpc-<VM-ID>` リストアポイントコレクションを選択します。

   <VM-ID> の値は、[インスタンス ID (Instance ID)]プロパティの Web UI 仮想マシンの詳細からフェッチできます。
4. リストアポイントコレクションに存在するリストアポイントのリストから、復元するリストアポイントを選択します。
5. 「復元ポイントから VM を復元する」で説明されている手順を使用して、VM をリストアポイントからリストアします。

Snapshot Manager が、指定されたプラグインインスタンスに対して、指定されたクラウドドメインを取得できない

この問題は、NetBackup Snapshot Manager を正常に停止せずに Docker/Podman デーモンを再起動すると発生します。これにより、コンテナの IP が不一致になり、NetBackup Snapshot Manager サービスの通信または解決が失敗します。

回避方法:

次の手順を実行します。

- コンテナマネージャデーモンを再起動するには、次のコマンドを実行して NetBackup Snapshot Manager サービスを正常に停止します。

  ```
  flexsnap_configure stop
  ```

  これにより、すべての NetBackup Snapshot Manager サービスが正しい順序で停止され、コンテナマネージャデーモンの停止または再起動によるエラーの発生が回避されます。
- コンテナマネージャデーモンを再起動し、次のコマンドを使用して NetBackup Snapshot Manager サービスを起動します。

  ```
  flexsnap_configure start
  ```

  このコマンドは、サービス間の通信を維持しながら、すべての NetBackup Snapshot Manager サービスを正しい順序で起動します。
- コンテナマネージャデーモンが再起動された場合は、NetBackup Snapshot Manager サービスを正常に停止する代わりに、次のコマンドを実行する必要があります。

  ```
  flexsnap_configure restart
  ```

これにより、サービスが正しい順序で停止および起動されるため、NetBackup Snapshot Manager が正しく動作することが保証されます。

SELinux の構成に関する問題

SELinuxを以前に無効にしたシステムで有効にした場合、または標準以外の構成でサービスを実行した場合、SELinux 構成の問題が発生します。

SELinux で問題が発生することは、構成の誤りを示唆しています。

回避方法:

次の手順を実行します。

1. 次のように ausearch ユーティリティを使用して、SELinux 監査ログで Snapshot Manager 関連の問題を確認します。

```
# ausearch -m avc -se VRTSflexsnap.process | audit2allow

allow VRTSflexsnap.process container_var_lib_t:dir watch;

allow VRTSflexsnap.process container_var_lib_t:file watch;
```

2. Snapshot Manager に関連する SELinux の問題を特定し、次のコマンドを使用して対応するポリシー変更を適用します。

```
# flexsnap_configure updatecil -i
```

Snapshot Manager で検出された SELinux ポリシーの更新を次に示します。

```
allow VRTSflexsnap.process default_t:dir create;

allow VRTSflexsnap.process default_t:file { create read };

Do you want to update Snapshot Manager's SELinux policy? (y/n):
y

Updating runtime SELinux policy ...done
```

変更を有効にするには、次のコマンドを実行します。

```
flexsnap_configure restart
```

3. 次のコマンドを使用してポリシーの変更を検証します。

```
# ausearch -m avc -se VRTSflexsnap.process | audit2allow
```

検証のために、次のメッセージが表示される必要があります。

```
!!!! This avc is allowed in the current policy
allow VRTSflexsnap.process container_var_lib_t:dir watch;
```

```
!!!! This avc is allowed in the current policy
allow VRTSflexsnap.process container_var_lib_t:file watch;
```

スナップショットからの OCI バックアップとバックアップコピーからのリストアに関するパフォーマンスの問題

スナップショットからの OCI バックアップ操作の際、データは Snapshot Manager に接続された永続ディスクから読み取られます。バックアップジョブの速度は IOPS によって決まります。バックアップコピージョブからのリストアでも同じ問題が発生します。

回避方法:

NetBackup Snapshot Manager の `flexsnap.conf` ファイルに次のエントリを追加します。

```
[oci]
vol_max_vpu_cnt_in_bfs_restore = 50
```

値は、20 から 120 の範囲の 10 の倍数として指定できます。

次の点に注意してください。

- バックアップされたボリュームについては、自動チューニングが有効な場合、NetBackup は IOPS を自動的に増やします。ただし、IOPS が高いほど、コストが高くなる可能性があります。
- VPU を増やして VM をリストアする場合は、リストア後に、OCI コンソールから VPU を通常の値に再度構成します。OCI コンソールから `flexsnap.conf` ファイルで提供される VPU 値を再構成できます。

スナップショットコピーからのシングルファイルリストアがエラーで失敗する

スナップショットのコピーからのシングルファイルリストア操作では、スナップショットから新しいディスクが作成され、ターゲット VM に接続されます。これは内部で検出されません。このため、ターゲット VM に接続されたディスクは、ターゲット VM に配備された NetBackup Snapshot Manager のオンホストエージェントで検出されません。

次のエラーメッセージが NetBackup ジョブモニターに表示されます。

```
Warning nbcs (pid=49733) Failed to restore file(s) / folder(s) from
 snapshot/backup. Internal status code: 2060017
.
```

.

```
Failed to restore file(s) and folder(s) from snapshot for asset:
<asset-id>
```

/cloudpoint/logs/flexsnap.log* の NetBackup Snapshot Manager ログには、次の対応するエラーが表示されます。

```
<redacted> flexsnap-agent-onhost[525538] Thread-32709
flexsnap.connectors.base: ERROR - Request failed unexpectedly
Traceback (most recent call last):
  File "flexsnap/connectors/base.py", line 112, in run
  File "flexsnap-agent.py", line 472, in handle_get
  File "flexsnap/agent.py", line 785, in find_asset
flexsnap.NotFoundError: <disk-id> not found
```

回避方法:

次に示すように、Windows および Linux システムでターゲット VM のディスクの再スキャンを手動でトリガします。

Windows の場合:

- ネットワークデバイスがデバイスに接続されている場合は、切断します。
- 管理者権限でコマンドプロンプトを開き、次のコマンドを実行します。
  `diskpart`
- diskpart プロンプト内で「rescan」と入力し、Enter キーを押します。
- diskpart プロンプトとコマンドラインを終了します。
- スナップショットコピーからのシングルファイルリストア操作を再度実行します。

Linux の場合:

- 次のコマンドを実行します。
  `echo "- - -" > /sys/class/scsi_host/hostX/scan`
  ここで、*X* はスキャンする SCSI ホストの数です。
  利用可能な各 SCSI ホストに対して上記のコマンドを確実に実行します。
  たとえば、3 つのデバイスがある場合は、次のコマンドを実行します。

  ```
  # echo "- - -" > /sys/class/scsi_host/host0/scan
  # echo "- - -" > /sys/class/scsi_host/host1/scan
  # echo "- - -" > /sys/class/scsi_host/host2/scan
  ```

- 問題が解決しない場合は、ターゲット VM を再起動します。

Windows クラウド VM で MS SQL アプリケーションのバックアップ、リストア、SFR ジョブがエラーで失敗する

Windows クラウド VM で MS SQL アプリケーションのバックアップ、リストア、または SFR ジョブが次のエラーで失敗します。

- Web UI:

```
Error nbcs (pid=880197) Failed to create snapshot for asset:
mssql-MSSQLSERVER-aws-ec2-us-west-2-<instance_id>
Error nbcs (pid=880197) Request failed unexpectedly: <WMIException:
 Invalid syntax COM Error code: 0x800401e4
```

- NetBackup Snapshot Manager の `flexsnap.log`ファイル内:

```
WMIException: Invalid syntax COM Error code: 0x800401e4
```

この問題は、MS SQL アプリケーションのバックアップ、リストアを取得している間、または、SFR ジョブで、ホストに配備されたエージェントを使用して WMI を介して接続されたデバイス情報をフェッチしている間に断続的に発生します。

回避方法:

操作を再試行します。問題が解決しない場合は、ターゲットの Windows VM を再起動します。

状態 49 エラーが表示される

NetBackup Snapshot Manager が構成されている多数の BLOB コンテナをバックアップしようとすると、アクティビティモニターで次のような状態 49 エラーが発生します。

```
Feb 06, 2024 8:17:44 AM - Info nbjm (pid=14024) started backup
(backupid=azure_azure-obj-account_perfobjectacct.obj-poc6_1707229064)
 job for client azure_azure-obj-account_perfobjectacct.obj-poc6,
policy policy-100, schedule full on storage unit azure-poc-msdp-c-stu
Feb 06, 2024 8:25:47 AM - Error bpbrm (pid=19853) Failed to spawn
DataMover container on host:obj-nbsm-server.internal.cloudapp.net
Feb 06, 2024 8:25:47 AM - Info bpbkar (pid=0) done. status: 49: client
 did not start
Feb 06, 2024 8:25:47 AM - Error nbpem (pid=14068) backup of client
azure_azure-obj-account_perfobjectacct.obj-poc6 exited with status
49 (client did not start)
Feb 06, 2024 8:25:47 AM - end writing
client did not start(49)
```

setroubleotd プロセスが実行されていて、より多くの CPU 領域を消費している場合に多数のバックアップを試みると、状態エラーコード 49 が表示されます。setroubleshootd は SELinux (Security-Enhanced Linux) を使用するシステムで動作するデーモンプロセスです。このデーモンは、SELinux によって生成されたシステムイベントとログを監視し、潜在的な問題またはポリシー違反を検出したときに管理者に通知と推奨事項を提供します。

回避方法:

setroubleshootd プロセスを無効にして実行を停止し、次の各ファイルの sedispatch 監査プラグインを無効にして、SELinux に関連する通知または推奨事項を生成しないようにします。

- RHEL7 の場合: `/etc/audisp/plugins.d/sedispatch.conf`
- RHEL8 以降の場合: `/etc/audit/plugins.d/sedispatch.conf`

RHEL7 を例として考慮した次の手順では、setroubleshootd プロセスを無効にする手順を示します。

1. 構成ファイルを次のように変更します。

   ```
   sed -i "s/active = yes/active = no/"
   /etc/audisp/plugins.d/sedispatch.conf
   ```

2. auditd サービスを再起動します。

   ```
   service auditd restart
   ```

   dbus は D-Bus API 要求によって setroubleshootd プロセスを起動します。

3. setroubleshootd プロセスを無効にするには、次の定義を削除して dbus を再ロードします。

   ```
   mv
   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootFixit.service

   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootFixit.service.back
     ## RHEL 8 and 9 only
   mv
   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootPrivileged.service

   /usr/share/dbus-1/system-services/org.fedoraproject.SetroubleshootPrivileged.service.back
   mv
   /usr/share/dbus-1/system-services/org.fedoraproject.Setroubleshootd.service

   /usr/share/dbus-1/system-services/org.fedoraproject.Setroubleshootd.service.back
   ```

   dbus を再ロードします: `systemctl reload dbus`

メモ: これは永続的な変更ではありません。setroubleshoot-server パッケージを更新すると、/usr/share/dbus-1/system-services/ ファイルがリカバリされます。

バックアップからのリストアがエラーで失敗する

リストアを作成するための前提条件に時間がかかりすぎると、次のエラーメッセージが表示されます。

```
Restore failed as the pre-requisites for restore operation were not
 satisfied for the asset.
```

これらの前提条件には、ブートボリュームとデータボリュームの作成が含まれます。リストアジョブのタイムアウトが発生し、ジョブが失敗します。

回避方法:

この問題を解決するには、前提条件を満たすようにリストアのタイムアウトを手動で構成します。

/cloudpoint/flexsnap.conf ファイル [agent] でパラメータ *pre_recovery_timeout = <num>* を構成します。たとえば、*pre_recovery_timeout = 1800* です。

ここで *<num>* はリストアの最大タイムアウト (秒) です。300 秒より大きい値を使用することをお勧めします。

(AWS の場合) 指定した AMI が特定のリージョンでサブスクライブされていない場合、エラーメッセージが表示されます。

指定した AMI が特定のリージョンでサブスクライブされていない場合に、スナップショットコピーからリストアしようとすると、次のエラーメッセージが表示されます。

```
botocore.exceptions.ClientError: An error occurred (OptInRequired)
when calling the RunInstances operation: In order to use this AWS
Marketplace product you
need to accept terms and subscribe. To do so please visit
https://aws.amazon.com/marketplace/pp?sku=b23ibdl39h2okr9co7jf8hr90";
```

回避方法:

リストアを実行する前に、特定のリージョンでサブスクライブされている AMI を選択するか、AMI をサブスクライブします。

Azure ディスク暗号化 VM のリストアがエラーで失敗する場合

Azure ディスク暗号化 VM のリストアが失敗し、次のエラーメッセージが表示されます。

```
CMK encryption cannot be applied on disks of a VM having Azure Disk
 Encryption enabled. In this case, only PMK is applicable.
```

回避方法:

リストア時に、暗号化を二重暗号化から PMK に変更し、再起動します。

(Azure の場合) スナップショットジョブからのバックアップでプロキシサーバーが飽和状態になっている

`*.blob.storage.azure.net` に対して通信する際、スナップショットジョブからのバックアップによりプロキシサーバーが飽和状態になっています。NetBackup Snapshot Manager の配備中、プロキシパラメータを設定する必要があります。

回避方法配備中に設定されているプロキシパラメータを見直し、トラフィックが構成どおりにルーティングされているかどうか確認します。

NetBackup Snapshot Manager 配備の no_proxy 構成に次のパラメータを追加します:

```
.blob.storage.azure.net
```

Kubernetes 拡張機能で Snapshot Manager が構成されている場合、バックアップジョブがエラー 2060017 で失敗する

この問題は、Snapshot Manager が Kubernetes 拡張機能で構成されている NetBackup 11.1 環境で発生します。バックアップジョブが Snapshot Manager ホストで実行するようにスケジュール設定されていて、必要なリソースが利用できない場合、エラーコード 2060017 で断続的に失敗することがあります。Kubernetes 統合環境において、Snapshot Manager で Snapshot Manager ホストと Kubernetes 拡張機能リソースを組み合わせた累積機能が公開されます。Snapshot Manager ホストで Data Mover ワークフローを起動すると、必要なリソースがローカルで利用できず、エラーが発生する可能性があります。

回避方法:

リソースの競合を解消するために、Snapshot Manager ホストの並列実行ジョブの数を制限します。

Snapshot Manager ホストで次の手順を実行します。

1. 次のファイルを開いて編集します。

   ```
   /usr/openv/var/global/flexsnap.conf
   ```

2. 次のセクションを追加または更新します。

   ```
   [capability_limit]

   max_jobs=1
   ```

3. ファイルを保存し、Snapshot Manager サービスを再起動します。

   ```
   systemctl restart nbsm
   ```

変更を適用した後、ジョブの成功率とリソース使用率を監視します。作業負荷と利用可能なリソースに基づいて、必要に応じて `max_jobs` 値を調整します。

メモ: この回避方法は、Snapshot Manager が Kubernetes 拡張機能で構成されており、Snapshot Manager ホストでスケジュール設定されている場合に、バックアップジョブがエラーコード 2060017 で失敗する環境にのみ適用できます。

Snapshot Manager のリソースが増えた後も、スナップショットからのバックアップジョブが、キューに投入された状態のまま残る

この問題は、並列ストリーム/読み取りが有効になっている NetBackup 11.1 環境で発生します。認可された親イメージまたはアンカーイメージに対するスナップショットからのバックアップジョブは、Snapshot Manager サーバーでリソース容量が増えた後も、キューに投入された状態のまま残ることがあります。このような場合、ジョブは利用可能なメモリユニットを Snapshot Manager サーバーリソースごとに待機し、[ジョブの詳細 (Job Details)] タブに次のメッセージが表示されます。

```
Limit has been reached for the logical resource <Snapshot Manager
Server name>.Cloud.Memory units per CloudPoint
```

この動作は、NetBackup Snapshot Manager サーバーで公開されるリソース制限容量に、システムリソースの最近の変更がすぐに反映されない場合があるために発生します。RAM や CPU を増やすように NetBackup Snapshot Manager インスタンスタイプが変更された場合、または Cloud Scale の配備でポッド数が増えた場合、更新された容量が NetBackup ですぐに使用されないことがあります。その結果、キューに登録済みのジョブは、容量が増えた場合でもリソースを待機し続けます。

回避方法:

更新されたリソース機能が検出され、NetBackup で使用されるようにするには、次の手順を実行します。

1. NetBackup Snapshot Manager の検出を実行し、完了します。これにより、NetBackup Snapshot Manager サーバーで公開されたリソース容量データが更新されます。
2. 任意の VM インスタンスの新しいバックアップジョブを開始します。これにより、Policy Execution Manager (PEM) のキャッシュされたリソース制限情報の更新がトリガされます。
1. 問題が解決しない場合は、プライマリサーバーで NetBackup サービスを再起動し、強制的にリソース容量データの完全な再ロードを行います。

メモ: NetBackup Snapshot Manager サーバーのリソース容量の増減が NetBackup に反映されるまで時間がかかる場合があります。上の手順を実行することで、後続のバックアップジョブのスケジュール設定時に更新された構成が認識され、使用されるようになります。

Snapshot Manager ホストの応答がない

特定の環境では、クラウドインスタンスの保護 (CIP) 操作中に NetBackup Snapshot Manager ホストが応答しなくなる場合があります。

この問題は、Azure B シリーズや AWS T シリーズなどのバースト可能なインスタンスタイプで発生しており、Azure D シリーズなどの他のインスタンスタイプでは発生していません。

CIP の実行中に複数のデータムーバーが短期間で起動されると、バースト可能な NetBackup Snapshot Manager インスタンスの CPU クレジットが 0 (ゼロ) に低下する場合があります。その結果、ホストは短時間応答しない状態になることがあります。

この動作は、ノードが B シリーズのインスタンスで構成されている場合に、Cloud Scale の配備でも発生する可能性があります。

回避方法:

稼働中の環境の NetBackup Snapshot Manager ホストには、バースト可能なインスタンスタイプ (Azure B シリーズ、AWS T シリーズなど) を使用しないことをお勧めします。

スナップショットからのクラウド VM のバックアップがエラー 20 で失敗する

並列ストリーム/読み取りが有効になっている NetBackup 11.1 環境では、認可された親イメージまたはアンカーイメージに対するスナップショットからのバックアップジョブが、エラー 20 で失敗する場合があります。

スナップショットからのバックアップジョブは、次のエラーで失敗します。

```
invalid command parameter(20)
```

[ジョブの詳細 (job details)]タブに、次のようなメッセージが表示されます。

```
Failed to update jobid info in Media Descriptor.
```

この問題は、NetBackup Snapshot Manager サーバーのリソース容量と、NetBackup によって現在認識されているリソースとの不一致が原因で発生します。ジョブのスケジュール中は、リソース容量が変わっても (増加または減少)、更新内容が NetBackup にすぐに反映されないため、スナップショットからのバックアップジョブが失敗する場合があります。

回避方法:

この問題を解決するには、次の手順を実行します。

1. 失敗したジョブの詳細を開き、バックアップ ID を書き留めます。
2. 失敗したバックアップ ID を取り消します。
   - プライマリサーバーで、次のコマンドを実行して、失敗したバックアップ ID を取り消します。
     ```
     nbstlutil cancel -backupid <backupid>
     ```
   - これにより、失敗したバックアップ ID に対するストレージライフサイクルポリシー (SLP) の反復が続行されなくなります。
3. 失敗したバックアップ ID を取り消したら、スナップショットからのバックアップジョブを再スケジュールするか、再実行します。

スナップショットからのバックアップがエラー 129 で失敗する

NetBackup 11.1 環境では、MSDP または MSDP-C ストレージユニットがいっぱいになり、バックアップデータを書き込むのに利用可能な領域がない場合にこの問題が発生します。

スナップショットからのバックアップジョブは、次のエラーで失敗します。

```
Disk storage unit is full (129)
```

回避方法:

MSDP または MSDP-C ストレージユニットの領域を解放して、新しいバックアップジョブが正常に完了できるようにします。

1. 不要なバックアップイメージを期限切れに設定
   - リストア操作に不要になったバックアップイメージを特定して期限切れにします。
   - これにより、新しいバックアップ向けにストレージ容量が解放されます。
2. MSDP の領域の再生利用
   - イメージを期限切れにしても、MSDP ですぐに解放された領域が再生されないことがあります。
   - この処理を加速させるには、MSDPトランザクションキューを手動で処理します。

詳しくは、『NetBackup™ 重複排除ガイド』の「MSDPトランザクションキューの手動処理」の項を参照してください。

リストアの低速化

Cloud Scale 環境では、リストア操作が遅くなる場合があります。

リストア速度は、NetBackup Snapshot Manager ホストまたは Cloud Scale ノードプールインスタンスで利用可能なネットワーク帯域幅によって制限されます。使用するインスタンスタイプの帯域幅が低い場合、データ転送とリストアの全体的なパフォーマンスに大きな影響を与える可能性があります。

回避方法:

リストアパフォーマンスを向上させる方法:

- NetBackup Snapshot Manager ホストまたは Cloud Scale ノードプールインスタンスで利用可能なネットワーク帯域幅を確認します。高帯域幅インスタンスの使用
- 10 Gbps 以上のネットワーク帯域幅を提供するインスタンスタイプを選択します。

子ジョブが長時間ハングしているように見える

NetBackup 11.1 環境では、特に断片化が進行したディスクを持つ VM の場合、バックアップ最適化に予想より長い時間がかかると、クラウド VM のバックアップジョブがハングしているように見えることがあります。

特定の仮想ディスクに関連付けられた子ジョブのデータ転送アクティビティがアクティビティモニターで長時間表示されないため、ジョブが停止しているか、応答していないという印象を受けます。

回避方法:

最適化処理をバイパスしてバックアップを正常に続行するには、/cloudpoint/openv/netbackup/bp.conf ファイルに次のエントリを追加します。

AZURE_DISABLE_OPTIMIZATION_THRESHOLD=12

(AWS の場合) ファイルシステムの整合性スナップショットではなく、クラッシュ整合スナップショットが作成される

Windows Server 2025 で AWS Systems Manager (SSM) を介して作成されたスナップショットは、ファイルシステムの整合性スナップショットではなく、クラッシュ整合のイメージになります。これは Web UI でプロバイダ管理の一貫性とファイルシステムの整合性が true に設定されている場合でも発生します。

次のエラーメッセージが表示されます。

```
485}    Writer Instance Id: {6d67b7e3-a3f1-43e0-b46d-3e91a65550b7}
   State: [1] Stable    Last error: No error  ¥¥r¥¥nec2-vss-agent is
 not running.
¥¥r¥¥nRunning tasklist /m ec2vssprovider.dll ¥¥r¥¥nINFO: No tasks
are running which match the specified criteria. ¥¥r¥¥nEC2 VSS Agent
 Version: 2.3.2.21
¥¥r¥¥nPowerShell version: ¥¥r¥¥n5.1.26100.6584 ¥¥r¥¥nActive
AWSPowerShell version: ¥¥r¥¥n¥r¥nAWS Tools for PowerShell¥r¥nVersion
 4.1.892¥r¥nCopyright
Amazon.com, Inc. or its affiliates. All Rights Reserved.¥r¥n¥r¥nAmazon
 Web Services SDK for .NET¥r¥nCore Runtime Version
3.7.500.13¥r¥nCopyright Amazon.com,
Inc. or its affiliates. All Rights Reserved.¥r¥n¥r¥nRelease notes:
```

この問題は、AWS VSS コンポーネントが AWS VSS SSM ドキュメントとともに最新バージョン (2.5.x) にアップグレードされた場合に発生します。

更新された VSS エージェントが Windows Server 2025 で正しく登録または起動されないため、ファイルシステムの一貫性インジケータが true と表示されても、クラッシュ整合スナップショットが作成されます。

回避方法:

NetBackupSnapshot Manager (ホストのエージェントベースまたはエージェントレス) を使用して、Windows Server 2025 のファイルシステムの整合性スナップショットを作成します。