

Veritas NetBackup™ CloudPoint インストールおよび アップグレードガイド

Ubuntu, RHEL, SLES

リリース 9.1

Veritas NetBackup CloudPoint インストールおよびアップグレードガイド

マニュアルバージョン: 2.7.1

法的通知と登録商標

Copyright © 2021 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴは、Veritas Technologies LLC または関連会社の米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、サードパーティ (「サードパーティプログラム」) の所有物であることをベリタスが示す必要のあるサードパーティソフトウェアが含まれている場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このベリタス製品付属のサードパーティ法的通知ドキュメントをご参照いただくか、次の場所をご覧ください。

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

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

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC は、この文書の供給、履行、または使用に関連して付随的または間接的に起こる損害に対して責任を負いません。本書に記載の情報は、予告なく変更される場合があります。

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

Veritas Technologies LLC
2625 Augustine Drive.
Santa Clara, CA 95054

<http://www.veritas.com>

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。テクニカルサポートの主な役割は、製品の特徴や機能に関する具体的な問い合わせに対応することです。テクニカルサポートグループは、オンラインナレッジベースのコンテンツも作成します。テクニカルサポートグループは、その他の部門と連携して、迅速にお客様の質問に回答します。

ベリタスが提供しているメンテナンスには、次のものが含まれます。

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

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

www.veritas.com/support

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

テクニカルサポートへの連絡

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

www.veritas.com/support

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

テクニカルサポートに連絡するときは、次の情報を用意してください。

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

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

ライセンスと登録

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

www.veritas.com/support

カスタマサービス

カスタマサービスの情報は次の URL で入手可能です。

www.veritas.com/support

カスタマサービスを利用すると、次の問題のような非技術的な疑問に役立ちます。

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

サポート契約のリソース

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

世界共通 (日本を除く)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

目次

テクニカルサポート	4
第 1 部 CloudPoint のインストールおよび構成	13
第 1 章 CloudPoint のインストールの準備	14
配備方法について	14
CloudPoint を実行する場所の決定	15
クラウドでの CloudPoint の配備について	17
システム要件への準拠	17
CloudPoint ホストのサイズの決定に関する推奨事項	25
クラウドプラットフォームでの CloudPoint のサイズの決定に関する推 奨事項	26
CloudPoint 拡張機能のサイズの決定に関する推奨事項	29
CloudPoint 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	30
コンテナプラットフォーム (Docker、Podman) のインストール	31
CloudPoint データを格納するボリュームの作成とマウント	32
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	34
CloudPoint 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	34
第 2 章 コンテナイメージを使用した CloudPoint の配備	35
CloudPoint のインストールを開始する前に	35
Docker 環境への CloudPoint のインストール	36
Podman 環境での CloudPoint のインストール	41
CloudPoint が正常にインストールされたことの確認	47
CloudPoint の再起動	48
第 3 章 CloudPoint 拡張機能の配備	51
CloudPoint 拡張機能のインストールを開始する前に	51
VM への拡張機能のインストールの準備	52
VM への CloudPoint 拡張機能のインストール	53
管理対象 Kubernetes クラスタへの拡張機能のインストールの準備	55

CloudPoint 拡張機能のダウンロード	60
管理対象 Kubernetes クラスタへの CloudPoint 拡張機能のインストール	61
拡張機能の管理	67

第 4 章

CloudPoint クラウドプラグイン	70
CloudPoint クラウドプラグインを構成する方法	70
AWS プラグインの構成に関する注意事項	71
AWS プラグイン構成の前提条件	75
CloudPoint の AWS アクセス権の構成	77
CloudPoint に必要な AWS アクセス権	78
クロスアカウントの構成を作成する前に	82
Google Cloud Platform プラグインの構成に関する注意事項	85
CloudPoint で必要な Google Cloud Platform アクセス権	87
CloudPoint の GCP サービスアカウントの構成	89
プラグイン構成のための GCP サービスアカウントの準備	89
Microsoft Azure プラグインの構成に関する注意事項	91
Microsoft Azure でのアクセス権の設定	93
Azure のスナップショットについて	96
Microsoft Azure Stack Hub プラグインの構成に関する注意事項	96
Microsoft Azure Stack Hub でのアクセス権の設定	98
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	101

第 5 章

CloudPoint ストレージアレイプラグイン	102
CloudPoint ストレージアレイのプラグインの構成方法	103
NetApp プラグインの構成に関する注意事項	103
NetApp プラグインの構成パラメータ	104
NetBackup アクセスの専用 LIF の構成	104
NetApp ストレージでサポートされる CloudPoint 操作	105
NetApp アレイの ACL の構成	108
Nutanix Files プラグインの構成に関する注意事項	108
Nutanix Files プラグイン構成の前提条件	108
Nutanix Files プラグインの考慮事項および制限事項	109
Nutanix Files ファイルサーバーでサポートされる CloudPoint 操作	110
Nutanix Files の NetBackup 問題のトラブルシューティング	111
Nutanix アレイの ACL の構成	112
Dell EMC Unity アレイプラグインの構成に関する注意事項	113
Dell EMC Unity アレイプラグインの構成パラメータ	113
サポートされる Dell EMC Unity アレイ	114
Dell EMC Unity アレイでサポートされる CloudPoint 操作	115

Pure Storage FlashArray プラグインの構成に関する注意事項	117
サポート対象の Pure Storage FlashArray モデル	117
Pure Storage FlashArray モデルでサポートされている CloudPoint 操作	118
HPE RMC プラグインの構成に関する注意事項	119
RMC プラグインの構成パラメータ	119
サポート対象の HPE ストレージシステム	120
HPE ストレージアレイでサポートされている CloudPoint 操作	120
HPE XP プラグインの構成に関する注意事項	123
HPE XP プラグインの構成パラメータ	123
HPE XP ストレージアレイでサポートされている CloudPoint 操作	124
Hitachi プラグインの構成に関する注意事項	125
Hitachi プラグインの構成パラメータ	126
サポート対象の Hitachi ストレージアレイ	126
Hitachi アレイでサポートされる CloudPoint 操作	127
Hitachi (HDS VSP 5000) プラグインの構成に関する注意事項	129
Hitachi (HDS VSP 5000) プラグインの構成パラメータ	129
Hitachi (HDS VSP 5000) アレイでサポートされる CloudPoint 操作	131
InfiniBox プラグインの構成に関する注意事項	131
InfiniBox プラグインの構成パラメータ	132
InfiniBox アレイでサポートされる CloudPoint 操作	132
Dell EMC PowerScale (Isilon) プラグインの構成に関する注意事項	135
Dell EMC PowerScale (Isilon) プラグインの構成の前提条件	135
Dell EMC PowerScale (Isilon) プラグインのサポート対象の CloudPoint 操作	136
Dell EMC PowerMax および VMax プラグインの構成に関する注意事項	138
Dell EMC PowerMax および VMax プラグインの構成の前提条件	138
Dell EMC PowerMax および VMax のサポート対象の CloudPoint 操作	140
Qumulo プラグインの構成に関する注意事項	141
Qumulo プラグインの構成の前提条件	142
Qumulo プラグインの考慮事項および制限事項	143
Qumulo プラグインのサポート対象の CloudPoint 操作	144
 第 6 章 CloudPoint アプリケーションエージェントとプラグイ ン	 145
Microsoft SQL プラグインの構成に関する注意事項	146
Oracle プラグインの構成に関する注意事項	147

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	148
MongoDB プラグインの構成に関する注意事項	148
インストールと構成の処理について	149
Linux ベースエージェントのインストールの準備	150
Windows ベースエージェントのインストールの準備	150
CloudPoint エージェントのダウンロードとインストール	150
Linux ベースのエージェントの登録	153
Windows ベースのエージェントの登録	156
CloudPoint アプリケーションプラグインの構成	159
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	160
クラウド資産に対する NetBackup 保護計画の作成	161
NetBackup 保護計画へのクラウド資産のサブスクリプション	162
スナップショットのリストアについて	163
SQL AG データベースをリストアするためのプロセス	166
Microsoft SQL Server のリストアの要件および制限事項	166
Oracle のリストアの要件および制限事項	167
Oracle スナップショットのリストア後に必要な追加手順	168
MongoDB のリストアの要件および制限事項	169
MongoDB スナップショットのリストア後に必要な追加手順	170
SQL AG データベースをリストアする前に必要な手順	171
SQL データベースの同じ場所へのリカバリ	172
代替の場所への SQL データベースのリカバリ	174
SQL Server スナップショットのリストア後に必要な追加手順	176
SQL Server 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	176
SQL AG データベースをリストアした後に必要な追加手順	179
Windows インスタンスが CloudPoint 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	180
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	180
AWS RDS データベースインスタンスをリストアした後に必要な追加手順	182

第 7 章

CloudPoint のエージェントレス機能を使用した資産の保護	184
エージェントレス機能について	184
エージェントレス構成の前提条件	185
Windows での SMB の構成 (省略可能)	187
Windows における WMI のセキュリティの構成 (省略可能)	187
エージェントレス機能の構成	187
CloudPoint のアップグレード後のエージェントレス機能の構成	188

第 8 章	NetBackup CloudPoint でのボリュームの暗号化	189
	CloudPoint でのボリュームの暗号化のサポートについて	189
	Azure でのボリュームの暗号化	189
	GCP でのボリュームの暗号化	190
	AWS でのボリュームの暗号化	191
第 9 章	CloudPoint セキュリティ	192
	Azure および Azure Stack のセキュリティの構成	192
	Azure および Azure Stack 用クラウドコネクタの構成	192
	Azure Stack の CA 構成	194
	CloudPoint への接続の保護	194
第 2 部	CloudPoint のメンテナンス	196
第 10 章	CloudPoint のログ	197
	CloudPoint のログ記録のしくみについて	197
	Fluentd ベースの CloudPoint ログ記録のしくみ	198
	CloudPoint fluentd 構成ファイルについて	198
	fluentd 構成ファイルの変更	199
	CloudPoint ログ	200
	エージェントレスログ	201
	CloudPoint ログ記録のトラブルシューティング	202
第 11 章	CloudPoint のアップグレード	203
	CloudPoint のアップグレードについて	203
	サポート対象のアップグレードパス	204
	アップグレードのシナリオ	204
	CloudPoint のアップグレードの準備	205
	CloudPoint のアップグレード	206
	Docker 環境でのアップグレード	206
	Podman 環境でのアップグレード	215
	パッチまたは Hotfix を使用した CloudPoint のアップグレード	221
	CloudPoint の移行とアップグレード	223
	CloudPoint の移行を開始する前に	223
	RHEL 8.3 での CloudPoint の移行とアップグレード	224
	アップグレード後のタスク	230

第 12 章	CloudPoint のアンインストール	233
	CloudPoint のアンインストールの準備	233
	CloudPoint のバックアップ	235
	CloudPoint プラグインの構成解除	238
	CloudPoint エージェントの構成解除	239
	CloudPoint エージェントの削除	240
	CloudPoint のスタンドアロン Docker ホスト環境からの削除	241
	CloudPoint 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	244
	CloudPoint のリストア	247
第 13 章	CloudPoint のトラブルシューティング	251
	CloudPoint のトラブルシューティング	251

CloudPoint のインストールおよび構成

- 第1章 CloudPoint のインストールの準備
- 第2章 コンテナイメージを使用した CloudPoint の配備
- 第3章 CloudPoint 拡張機能の配備
- 第4章 CloudPoint クラウドプラグイン
- 第5章 CloudPoint ストレージアレイプラグイン
- 第6章 CloudPoint アプリケーションエージェントとプラグイン
- 第7章 CloudPoint のエージェントレス機能を使用した資産の保護
- 第8章 NetBackup CloudPoint でのボリュームの暗号化
- 第9章 CloudPoint セキュリティ

CloudPoint 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。

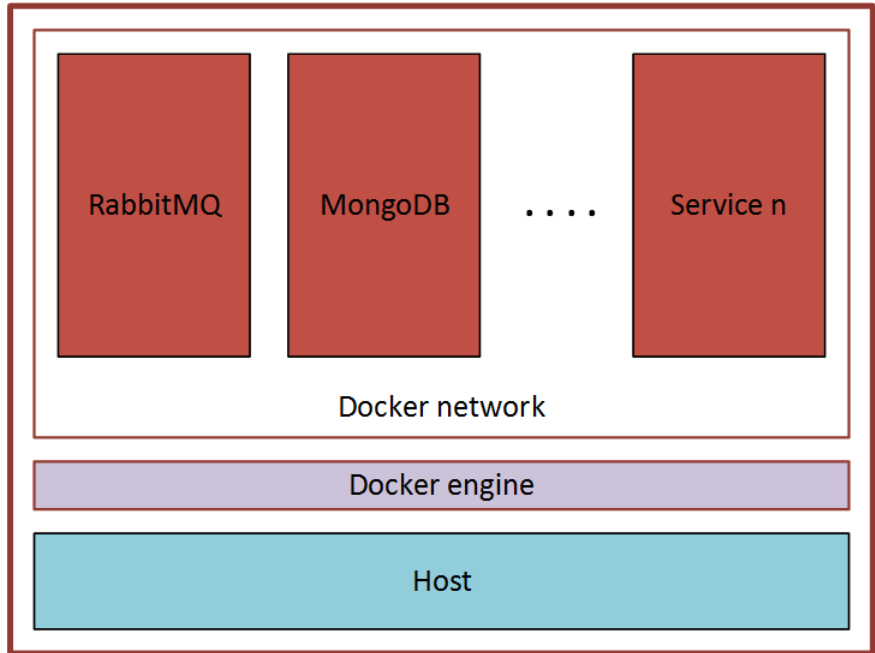
- 配備方法について
- CloudPoint を実行する場所の決定
- クラウドでの CloudPoint の配備について
- システム要件への準拠
- CloudPoint ホストのサイズの決定に関する推奨事項
- CloudPoint 拡張機能のサイズの決定に関する推奨事項
- CloudPoint をインストールするインスタンスの作成またはホストの準備
- コンテナプラットフォーム (Docker、Podman) のインストール
- CloudPoint データを格納するボリュームの作成とマウント
- インスタンスまたは物理ホストで特定のポートが開いていることの確認
- CloudPoint 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

配備方法について

CloudPoint 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、CloudPoint 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 MongoDB です。RabbitMQ は CloudPoint のメッセージブローカーであり、MongoDB は CloudPoint 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、CloudPoint マイクロサービスモデルを示しています。

図 1-1 CloudPoint のマイクロサービスモデル



この配備方法には、次の利点があります。

- CloudPoint 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。

CloudPoint を実行する場所の決定

CloudPoint を次の方法で配備できます。

- CloudPoint をクラウドに配備し、そのクラウドの資産を管理します。
- CloudPoint 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。

Veritas は、CloudPoint 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、CloudPoint ホストインスタンスを同じクラウド環境に配備します。同様に、オンプレミス資産を保護する場合は、CloudPoint ホストを同じオンプレミス環境に配備します。

CloudPoint は NetBackup メディアサーバーに配備できますが、NetBackup プライマリサーバーには配備できません。

複数のホストに CloudPoint をインストールする場合は、各 CloudPoint インスタンスが独立したリソースを管理することを強くお勧めします。たとえば、2 つの CloudPoint 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 CloudPoint 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。

- CloudPoint インスタンス A および CloudPoint 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。
- CloudPoint 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。CloudPoint 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、CloudPoint 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。CloudPoint 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なくなります。

同じホストで CloudPoint サーバーとメディアサーバーをホスティングする場合、スナップショットジョブからのバックアップを適切に動作させるには、次の操作を実行します。

- CloudPoint サーバーとメディアサーバーに個別の IP と NBU クライアント名を割り当てて、各サーバーが異なる NetBackup 証明書を取得できるようにします。これは、各サーバーが通信用に異なる NetBackup ホスト ID 証明書を使用するために必要です。次の構成を使用します。
 - 2 つのネットワークアダプタを使用してホストを構成する
 - /etc/hosts ファイルを編集し、以下の例に示すエントリを作成します。

```
<IP Address MediaServer Host1> <MediaServer Host1>
<IP Address CloudPoint Host2> <CloudPoint Host2>
```
 - メディアサーバーのインストール時のメディアサーバー名には、/etc/hosts ファイルに記載されている MediaServer Host1 を指定します。
 - 同様に、CloudPoint インストール時には /etc/hosts ファイルから CloudPoint Host 2 を選択し、443 以外の非デフォルトポートを指定します。
 - CloudPoint サービスとメディアサービスを起動し、NetBackup プライマリサーバーに登録します。
- CloudPoint サーバーが登録されたら、異なる HOST DB エントリが存在することを確認します。

- 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前に、DISABLE SHM と NOSHMM の最適化を実行します。参照:

https://www.veritas.com/support/en_US/article.100016170

これにより、NetBackup データムーバードプロセス間の通信で、共有メモリが使用されなくなります。

クラウドでの CloudPoint の配備について

CloudPoint の一般的な配備方法は、クラウドで CloudPoint インスタンスを設定し、次に、クラウド内のすべての資産を保護および管理するようにインスタンスを構成することです。CloudPoint は、手動で配備するか、オンラインのマーケットプレイスで利用可能な CloudPoint テンプレートを使用して配備できます。

手動で CloudPoint を配備する場合は、CloudPoint サーバー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 CloudPoint インスタンスを配備する方法について詳しくは、次を参照してください。

<http://veritas.com/netbackupcloud>

システム要件への準拠

CloudPoint ホストの要件

CloudPoint 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.25 の「[CloudPoint 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 1-1 CloudPoint ホストのオペレーティングシステムとプロセッサの要件

カテゴリ	要件
オペレーティングシステム	■ Ubuntu 18.04 および 20.04 Server LTS ■ Red Hat Enterprise Linux (RHEL) 8.3 および 7.x メモ: IPV6 を使用した RHEL 8.3 への CloudPoint の配備はサポートされていません。 ■ SUSE Linux Enterprise Server (SLES) 15 SP2
プロセッサアーキテクチャ	x86_64、AMD64、64 ビットプロセッサ

表 1-2 CloudPoint ホストのシステム要件

CloudPoint 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: 8 GB ■ ルートディスク: 64 GB の SSD (GP2) ■ 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。このサイズ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。
Microsoft Azure VM	■ 仮想マシン形式: D2s_V3 標準 ■ CPU コア: 2 ■ RAM: 8 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 プレミアム SSD。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 CloudPoint 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 ■ 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して、必要な最小ディスク領域の要件を満たすようにする
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 プレミアム SSD。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 CloudPoint 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 ■ 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して、必要な最小ディスク領域の要件を満たすようにする

CloudPoint がインストールされているホスト	要件
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 標準永続ディスク、Ubuntu 16.04 Server LTS ■ 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
VMware VM	■ 仮想マシンの形式: CloudPoint サポート対象オペレーティングシステムを搭載した 64 ビット ■ vCPU: 8 ■ RAM: 16 GB 以上 ■ ルートディスク: 標準永続ディスクを備えた 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用の 50 GB
物理ホスト (x86_64 / AMD64)	■ オペレーティングシステム: 64 ビット CloudPoint サポート対象オペレーティングシステム ■ CPU: x86_64 (64 ビット)、シングルソケット、マルチコア、8 個以上の CPU 数 ■ RAM: 16 GB 以上 ■ ブートディスク: 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用の 50 GB

ディスク容量の要件

CloudPoint 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、コンテナのランタイムにさらに使用されます。CloudPoint 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 1-3 CloudPoint 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
CloudPoint コンテナ	30 GB の空き容量

コンポーネント	空き容量の要件
CloudPoint エージェントとプラグイン	350 MB の空き容量 (構成する各 CloudPoint プラグインおよびエージェント用)

さらに、CloudPoint は CloudPoint 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 CloudPoint ホストの /cloudpoint に確実にマウントします。

表 1-4 CloudPoint 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.25 の「[CloudPoint 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。

CloudPoint 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、ストレージのプラットフォーム

CloudPoint 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、ストレージの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、CloudPoint の構成方法、CloudPoint クラウドまたはストレージ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、CloudPoint 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 CloudPoint 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 1-5 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、ストレージのプラットフォーム

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 2014、SQL 2016、SQL 2017、SQL 2019 p.146 の「Microsoft SQL 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。 ■ MongoDB Enterprise Edition 3.6 および 4.0 p.148 の「MongoDB 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。 ■ Oracle 12c、Oracle 12c R1、Oracle 18c、Oracle 19c 単一ノード構成がサポート対象です。 p.147 の「Oracle 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。 注意: ■ Oracle データベースアプリケーションは、GCP (Google Cloud Platform) クラウド環境ではサポートされません。 これは、これらの製品とサービスを所有している会社によって課せられた制限であり、現在の CloudPoint の範囲外です。 ■ CloudPoint では、ext2 ファイルシステム上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はサポートされません。 ■ CloudPoint では、GCP クラウド環境の Microsoft SQL Server の作業負荷はサポートされません。
サポート対象資産のオペレーティングシステム	■ Red Hat Enterprise Linux (RHEL) 7.x Red Hat Enterprise Linux (RHEL) 8.2 および 8.3 ■ Windows Server 2012、2012 R2、Windows Server 2016 メモ: CloudPoint エージェントは英語以外のオペレーティングシステムではサポートされません。

カテゴリ	サポート
クラウドプラットフォーム	

カテゴリ	サポート
	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、CloudPoint 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 の場合: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/device_naming.html Linux の場合: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/device_naming.html 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。 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: CloudPoint Azure 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 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。 https://docs.microsoft.com/ja-jp/azure-stack/user/azure-stack-vm-sizes?view=azs-2008 を参照してください。 メモ: CloudPoint 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。 GCP (Google Cloud Platform)

カテゴリ	サポート
	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。
ストレージプラットフォーム	■ NetApp ストレージアレイ p.103 の「NetApp 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。 ■ Dell EMC Unity アレイ p.113 の「Dell EMC Unity アレイプラグインの構成パラメータ」を参照してください。 ■ HPE ストレージアレイ p.119 の「HPE RMC 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。 ■ Pure Storage FlashArray p.117 の「Pure Storage FlashArray 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。 ■ Hitachi ストレージアレイ p.125 の「Hitachi 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。 ■ InfiniBox エンタープライズアレイ p.131 の「InfiniBox 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。

CloudPoint タイムゾーン

CloudPoint 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、CloudPoint は CloudPoint 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

CloudPoint 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、CloudPoint 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、CloudPoint 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。CloudPoint インストーラは、プロキシサーバーの情報を、CloudPoint コンテナ固有の一連の環境変数に格納します。

次の表に、CloudPoint 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。CloudPoint 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 1-6 CloudPoint に必要なプロキシサーバーの詳細

CloudPoint 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 HTTPS プロキシ値が格納されます。たとえば、 "https://proxy.mycompany.com:8080/" です。
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。

プロキシサーバー経由で外部と通信する必要がある CloudPoint サービスは、CloudPoint 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。

CloudPoint ホストのサイズの決定に関する推奨事項

主に CloudPoint ホストの構成は、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 CloudPoint サーバー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 CloudPoint を使用する方法です。CloudPoint 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、CloudPoint 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。

Veritas は、CloudPoint ホストに対して次の構成をお勧めします。

表 1-7 並列実行タスクの数に基づく標準的な CloudPoint ホストの構成

作業負荷メトリック	CloudPoint ホスト構成
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、CloudPoint 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、CloudPoint 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:

CloudPoint 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、Veritas は CloudPoint 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は、Veritas はアプリケーションホストの /tmp 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。CloudPoint 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、CloudPoint 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設定する場合、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 CloudPoint 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、CloudPoint 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、CloudPoint ホスト構成の容量で処理できる数よりも多い場合は、CloudPoint 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。

クラウドプラットフォームでの CloudPoint のサイズの決定に関する推奨事項

標準サイズの構成を検討する際には、次の点が重要です。

- 20% のインスタンスが CloudPoint ホストに接続され、個別リストアを実行し、アプリケーションの一貫性のあるスナップショットを作成する
- 保護された各インスタンスに 100 GB サイズのディスクを 3 台接続する
- 保護サイクルは 1 日 2 回、保持期間は 3 カ月
- /cloudpoint ボリュームのサイズは、インスタンスが 400 個の場合は 50 GB 以上、インスタンスが 500 個の場合は 100 GB 以上
- クラウドプラットフォームとインスタンスタイプに基づき、該当する場合は、選択したインスタンスタイプに適切な CPU クレジットが利用可能

次の表に、CloudPoint ホストの構成例を示します。

表 1-8 Google Cloud Platform

CloudPoint ホスト	vCPU	メモリ	インスタンス
■ n1-standard-2 ■ n2-standard-2	2	8	200
■ n1-standard-4 ■ n2-standard-4	4	16	400
■ n1-standard-16 ■ n2-standard-16	8	32	500

表 1-9 アマゾンウェブサービス

CloudPoint ホスト	vCPU	メモリ	インスタンス
■ t2.large ■ t3.large ■ m4.large	2	8	200
■ t2.xlarge ■ t3.xlarge ■ t3a.xlarge	4	16	400
■ m5.4xlarge ■ m4.4xlarge	8	32	500

表 1-10 Microsoft Azure

CloudPoint ホスト	vCPU	メモリ	インスタンス
- Standard_B2ms - Standard_D2s_v3 - Standard_D2_v4、 Standard_D2s_v4 - Standard_D2d_v4、 Standard_D2ds_v4	2	8	200
- Standard_B4ms - Standard_D4s_v3 - Standard_D4_v4、 Standard_D8s_v4 - Standard_D4d_v4、 Standard_D4ds_v4	4	16	400
- Standard_B16ms - Standard_D16s_v3 - Standard_D16_v4、 Standard_D16s_v4 - Standard_D16d_v4、 Standard_D16ds_v4	8	32	500

表 1-11 Microsoft Azure Stack Hub

CloudPoint ホスト	vCPU	メモリ	インスタンス
- Standard_DS2_v2 - Standard_D2_v2 - Standard_DS2 - Standard_D2	2	7	200
- Standard_DS3_v2 - Standard_D3_v2 - Standard_DS3 - Standard_D3 - Standard_NV4as_v4	4	14	400
- Standard_DS4_v2 - Standard_D4_v2 - Standard_DS4 - Standard_D4	8	28	500

CloudPoint 拡張機能のサイズの決定に関する推奨事項

CloudPoint 拡張機能の目的は、パフォーマンス容量がピークになるように CloudPoint サーバー上で多数の要求を同時に実行するため、CloudPoint 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 CloudPoint 拡張機能をオンプレミスまたは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、CloudPoint の処理容量を増加できます。

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

p.17 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 CloudPoint 拡張機能の環境:

- オンプレミスの VM ベースの拡張機能
- 管理対象の Kubernetes クラスタを使用したクラウドベースの拡張機能

メモ: CloudPoint 9.1 では、拡張機能は Azure と Azure Stack でのみサポートされます。

Veritas は、CloudPoint 拡張機能の次の構成をお勧めします。

表 1-12 オンプレミスまたはクラウドにおける一般的な CloudPoint 拡張機能の構成

作業負荷メトリック	CloudPoint 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、AWS クラウドでは、CloudPoint 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: 8 個の CPU メモリ: 32 GB 以上 たとえば、AWS クラウドでは、CloudPoint 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:

CloudPoint 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、Veritas は CloudPoint 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、CloudPoint 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、CloudPoint 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、CloudPoint 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。
- 同時並行処理の数が、CloudPoint 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、CloudPoint 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ものみ取得されます。

CloudPoint 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

CloudPoint 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。

- CloudPoint のインストール要件を満たすサポート対象の Ubuntu、RHEL、または SLES インスタンスイメージを選択します。
- 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。

CloudPoint をオンプレミスのインスタンスに配備している場合は、次の手順を実行します。

- サポート対象の Ubuntu、RHEL、または SLES オペレーティングシステムを物理または仮想 x86 サーバーにインストールします。
- インストール要件を満たすように、サーバー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 1-13 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手順については、次のマニュアルを参照してください。 https://docs.docker.com/install/linux/docker-ce/ubuntu/#set-up-the-repository
RHEL 7.x 上の Docker	サポート対象バージョン: Docker 1.13.x 以降 RHEL に Docker をインストールするには、次のプロセスを使用します。CloudPoint がオンプレミスまたはクラウドのどちらかに配備されるかによって、手順が異なる場合があります。 ■ CloudPoint 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。 <pre># sudo yum-config-manager --enable rhui-REGION-rhel-server-extras</pre> ■ CloudPoint がオンプレミスに配備される場合、サブスクリプションを有効にします。 <pre># sudo subscription-manager register --auto-attach --username=<username> --password=<password> # subscription-manager repos --enable=rhel-7-server-extras-rpms # subscription-manager repos --enable=rhel-7-server-optional-rpms</pre> ■ 次のコマンドを使用して Docker をインストールします。 <pre># sudo yum -y install docker</pre> ■ 次のコマンドを使用して、システムマネージャ構成を再ロードします。 <pre># sudo systemctl daemon-reload</pre> ■ 次のコマンドを使用して、docker サービスを有効にして再起動します。 <pre># sudo systemctl enable docker # sudo systemctl restart docker</pre> ■ 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。 ■ システムを再ブートして変更を反映させます。 ■ SELinux モードの変更が反映されていることを、次のコマンドを使用して確認します。 <pre># sudo sestatus</pre> 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。 RHEL に Docker をインストールする手順について詳しくは、次を参照してください。 https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux_atomic_host/7/html-single/getting_started_with_containers/index#getting_docker_in_rhel_7

プラットフォーム	説明
RHEL 8.3 の Podman	サポート対象のバージョン: Podman 2.0.5、2.2.1 注意: ■ CloudPoint 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 ■ CloudPoint がオンプレミスに配備される場合、サブスクリプションを有効にします。 # sudo subscription-manager register --auto-attach --username=<username> --password=<password> ■ 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。 ■ システムを再起動して変更を反映させます。 ■ SELinux モードの変更が反映されていることを、次のコマンドを使用して確認します。 # getenforce 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。

CloudPoint 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 CloudPoint または CloudPoint 拡張機能を配備する前に、以下を確認してください。

- CloudPoint 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。

表 1-14 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 次の手順を使用して、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上の /cloudpoint にマウントします。 http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-using-volumes.html
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。 https://cloud.google.com/compute/docs/disks/add-persistent-disk
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。 https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/attach-disk-portal 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。 https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/attach-disk-portal#use-azure-managed-disks 2 ディスクを初期化し、/cloudpoint にマウントします。 詳しくは、次のリンクで、新しいディスクをマウントするための Linux VM への接続方法を参照してください。 https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/add-disk
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。 https://docs.microsoft.com/ja-jp/azure-stack/user/azure-stack-manage-vm-disks/adding-new-disks 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、次のリンクで、新しいディスクをマウントするための Linux VM への接続方法を参照してください。 https://docs.microsoft.com/ja-jp/azure/virtual-machines/linux/add-disk

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 1-15 CloudPoint で使用するポート

ポート	説明
443	CloudPoint 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。
5671	CloudPoint 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。
- CloudPoint 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。

CloudPoint 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 9.1 以降が必要です。

必要なポート:

- NetBackup プライマリサーバーで必要なポート: 1556
- 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/openssl/etc/hosts` ファイルに `/etc/hosts` ファイルと同様のエントリを追加します。
- CloudPoint のインストール時と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。

コンテナイメージを使用した CloudPoint の配備

この章では以下の項目について説明しています。

- [CloudPoint のインストールを開始する前に](#)
- [Docker 環境への CloudPoint のインストール](#)
- [Podman 環境での CloudPoint のインストール](#)
- [CloudPoint が正常にインストールされたことの確認](#)
- [CloudPoint の再起動](#)

CloudPoint のインストールを開始する前に

CloudPoint をインストールする前に、次の手順を完了していることを確認してください。

- CloudPoint をインストールする場所を決定します。
p.15 の「[CloudPoint を実行する場所の決定](#)」を参照してください。

メモ: CloudPoint 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.17 の「[システム要件への準拠](#)」を参照してください。
- CloudPoint 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.30 の「[CloudPoint 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.31 の [表 1-13](#) を参照してください。

- CloudPoint 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.32 の「[CloudPoint 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.34 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。したがって、RHEL 8.3 ホストに CloudPoint を配備する場合は、p.41 の「[Podman 環境での CloudPoint のインストール](#)」を参照してください。。RHEL 7.x ホストの場合は、p.36 の「[Docker 環境への CloudPoint のインストール](#)」を参照してください。

Docker 環境への CloudPoint のインストール

メモ: CloudPoint 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。

CloudPoint をインストールするには

- 1 CloudPoint イメージを、CloudPoint を配備するシステムにダウンロードします。ベリタスのサポートサイトを参照してください。

[ja_JP/downloads](#)

メモ: ダウンロードするには、サポートサイトにログオン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。

CloudPoint イメージ名は次のような形式です。

`VRTScloudpoint-docker-x.x.x.x.x.img.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 CloudPoint イメージをダウンロードしたディレクトリに移動します。

3 次のコマンドを入力して、イメージを Docker にロードします。

```
# sudo docker load -i CloudPoint_image_name
```

次に例を示します。

```
# sudo docker load -i Veritas_CloudPoint_8.3.0.8549.img.gz
```

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。

```
538bd068cab5: Loading layer [=====>] 38.26MB/38.26MB
ed4b778f8d1d: Loading layer [=====>] 1.166GB/1.166GB
c8b269899686: Loading layer [=====>] 49.15kB/49.15kB
Loaded image: veritas/flexsnap-cloudpoint:8.3.0.8549
```

出力の最後の行に表示される、ロードされたイメージの名前とバージョンを書き留めておきます。このバージョンは、インストールされる CloudPoint 製品バージョンを表します。これらの詳細は、次の手順で指定します。

4 次のコマンドを入力して、CloudPoint コンテナを実行します。

```
# sudo docker run -it --rm
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> install
```

CloudPoint ホストがプロキシサーバーの内側にある場合は、代わりに次のコマンドを使用します。

```
# sudo docker run -it --rm
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-e VX_HTTP_PROXY=<http_proxy_value>
-e VX_HTTPS_PROXY=<https_proxy_value>
-e VX_NO_PROXY=<no_proxy_value>
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> install
```

環境に応じて、次のパラメータを置き換えます。

パラメータ	説明
<full_path_to_volume_name>	CloudPoint データボリュームへのパスを表します。通常は /cloudpoint です。
<version>	前の手順でメモした CloudPoint 製品バージョンを表します。
<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。 (インスタンスがプロキシサーバーを使用する場合のみ必要) たとえば、"http://proxy.mycompany.com:8080/" です。

パラメータ	説明
<code><https_proxy_value></code> (インスタンスがプロキシサーバーを使用する場合のみ必要)	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、"https://proxy.mycompany.com:8080/" です。
<code><no_proxy_value></code> (インスタンスがプロキシサーバーを使用する場合のみ必要)	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: CloudPoint 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設定していることを確認します。 ■ AWS インスタンスの場合は、次を追加します。 169.254.169.254 ■ GCP 仮想マシンの場合は、次を追加します。 169.254.169.254,metadata,metadata.google.internal ■ Azure 仮想マシンの場合は、次を追加します。 169.254.169.254 CloudPoint 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。

たとえば、CloudPoint バージョンが 8.3.0.8549 の場合、コマンド構文は次のようになります。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:8.3.0.8549 install
```

プロキシサーバーを使用している場合、前の表に示した例を使用すると、コマンドの構文は次のようになります。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -e  
VX_HTTP_PROXY="http://proxy.mycompany.com:8080/" -e  
VX_HTTPS_PROXY="https://proxy.mycompany.com:8080/" -e  
VX_NO_PROXY="localhost,mycompany.com,192.168.0.10:80" -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:8.3.0.8549 install
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

インストーラに次のようなメッセージが表示されます。

```
Installing the services
Configuration started at time: Fri Mar 13 06:11:42 UTC 2020
WARNING: No swap limit support
Docker server version: 18.09.1
This is a fresh install of CloudPoint 8.3.0.8549
Checking if a 1.0 release container exists ...
CloudPoint currently is not configured.
Starting initial services before configuration.
Creating network: flexsnap-network ...done
Starting docker container: flexsnap-fluentd ...done
Creating docker container: flexsnap-mongodb ...done
Creating docker container: flexsnap-rabbitmq ...done
Creating docker container: flexsnap-certauth ...done
Creating docker container: flexsnap-api-gateway ...done
Creating docker container: flexsnap-coordinator ...done
Creating docker container: flexsnap-agent ...done
Creating docker container: flexsnap-onhostagent ...done
Creating docker container: flexsnap-scheduler ...done
Creating docker container: flexsnap-policy ...done
Creating docker container: flexsnap-notification ...done
Creating docker container: flexsnap-idm ...done
Starting docker container: flexsnap-config ...done
Creating self signed keys and certs for nginx ...done
Starting docker container: flexsnap-nginx ...done
```

この手順で、CloudPoint は次を実行します。

- 各 CloudPoint 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。

次の点に注意してください。

- ボリュームを `-v full_path_to_volume_name:/full_path_to_volume_name` として指定しない場合、コンテナは Docker ホストファイルシステムに書き込みます。

- 5 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
管理者ユーザー名 (Admin username)	CloudPoint 管理者ユーザーアカウントのユーザー名を指定します。
管理者パスワード (Admin password)	管理者ユーザーのパスワードを指定します。
新しい admin パスワードの確認 (Confirm Admin password)	管理者ユーザーのパスワードを確認します。
TLS 証明書のホスト名 (Host name for TLS certificate)	CloudPoint 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。 異なる名前を使用してホストに接続する場合、たとえば、myserver、myserver.mydomain、myserver.mydomain.mycompany.com などの名前を使用して CloudPoint アクセスを有効にする場合は、ここにすべての名前を追加します。 複数のエントリを指定するにはカンマ (,) を使用します。ここで指定する名前は、同じ CloudPoint ホストを指す必要があります。 指定した名前または IP アドレスは、CloudPoint の構成に使用するホスト名のリストに追加されます。インストーラはこれらの名前を使用して、CloudPoint ホストのサーバー証明書を生成します。
ポート	CloudPoint サーバーが通信に使用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 CloudPoint configuration to complete (21/21) ...done
Configuration complete at time Fri Mar 13 06:15:43 UTC 2020!
```

- 6 これにより **CloudPoint** の配備プロセスは終了します。次の手順では、**CloudPoint** サーバーを **Veritas NetBackup** プライマリサーバーに登録します。

CloudPoint 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。**CloudPoint** がオンプレミスに配備されている場合の手順については、『**NetBackup Snapshot Client 管理者ガイド**』を参照してください。

メモ: CloudPoint を再起動する必要がある場合は、`docker run` 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.48 の「[CloudPoint の再起動](#)」を参照してください。

Podman 環境での CloudPoint のインストール

Podman での CloudPoint 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 (`lvm2`、`udev`、`dnsmasq`) 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 python3-pyudev-<version>

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

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

CloudPoint をインストールするには

メモ: CloudPoint 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インストールと関連す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。

- 1 CloudPoint イメージを、CloudPoint を配備するシステムにダウンロードします。

CloudPoint イメージ名は次のような形式です。

```
VRTScloudpoint-podman-9.x.x.x.x.tar.gz
```

- 2 CloudPoint イメージをダウンロードしたディレクトリに移動します。

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。

```
# gunzip VRTScloudpoint-podman-9.x.x.x.x.tar.gz  
  
# ls
```

出力は次のようになります。

```
VRTScloudpoint-podman-9.x.x.x.x.tar  
[root@<user>-RHEL8 ec2-user]# tar -xvf  
VRTScloudpoint-podman-9.x.x.x.x.tar  
flexsnap-cloudpoint-9.x.x.x.x.img  
flexsnap-coordinator-9.x.x.x.x.img  
flexsnap-agent-9.x.x.x.x.img  
flexsnap-onhostagent-9.x.x.x.x.img  
flexsnap-policy-9.x.x.x.x.img  
flexsnap-scheduler-9.x.x.x.x.img  
flexsnap-config-9.x.x.x.x.img  
flexsnap-certauth-9.x.x.x.x.img  
flexsnap-rabbitmq-9.x.x.x.x.img  
flexsnap-api-gateway-9.x.x.x.x.img  
flexsnap-notification-9.x.x.x.x.img  
flexsnap-fluentd-9.x.x.x.x.img  
flexsnap-nginx-9.x.x.x.x.img  
flexsnap-idm-9.x.x.x.x.img  
flexsnap-workflow-9.x.x.x.x.img  
flexsnap-listener-9.x.x.x.x.img  
flexsnap-datamover-9.x.x.x.x.img  
flexsnap-mongodb-9.x.x.x.x.img  
flexsnap-podman-api.service  
flexsnap-podman-containers.service  
flexsnap_preinstall.sh  
dnsname
```

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

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

出力は次のようになります。

```
Executing the following changes on this node to prepare the
CloudPoint
server for installation:
    1) Loading CloudPoint service images.
    2) Copying dnsname plugin to the /usr/libexec/cni folder.
    3) Check if dnsmasq rpm is installed on the host, if not,
        installation is done automatically.
    4) Creating and starting the systemd service for the Podman
API server.
Do you want to continue? (Yes/No): Yes
Loaded image(s): localhost/veritas/flexsnap-agent:9.x.x.x.x
Loaded image(s): localhost/veritas/flexsnap-api-gateway:9.x.x.x.x
Loaded image(s): localhost/veritas/flexsnap-certauth:9.x.x.x.x
.....
.....
Loaded image(s): localhost/veritas/flexsnap-workflow:9.x.x.x.x
Copying dnsname plugin...done
Starting Podman API service...done
Enabling Podman Containers service...done
```

5 次のコマンドを使用して、NetBackup CloudPoint をインストールします。

```
# podman run -it --rm --privileged -v /cloudpoint:/cloudpoint -v
/run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:9.x.x.x.x install
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

この手順で、CloudPoint は次を実行します。

- 各 CloudPoint 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。

出力は次のようになります。

```
Installing the services
Configuration started at time: Thu Feb 18 09:20:12 UTC 2021
podman server version: 2.0.5 Supported: true
```

```
This is a fresh install of NetBackup CloudPoint 9.x.x.x.x
CloudPoint currently is not configured. Starting initial services
before configuration.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Creating container: flexsnap-mongodb ...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-idm ...done
Starting container: flexsnap-config ...done
Creating self signed keys and certs for nginx ...done
Please provide CloudPoint admin credentials for configuration:
```

CloudPoint ホストがプロキシサーバーの内側にある場合は、代わりに次のコマンドを使用します。

```
# podman run -it --rm --privileged
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-e VX_HTTP_PROXY=<http_proxy_value>
-e VX_HTTPS_PROXY=<https_proxy_value>
-e VX_NO_PROXY=<no_proxy_value>
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:9.x.x.x.x install
```

環境に応じて、次のパラメータを置き換えます。

パラメータ	説明
<http_proxy_value> (インスタンスがプロキシサーバーを使用する場合のみ必要)	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> (インスタンスがプロキシサーバーを使用する場合のみ必要)	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、“https://proxy.mycompany.com:8080/” です。

パラメータ

<no_proxy_value>

(インスタンスがプロキシサーバーを使用する場合のみ必要)

説明

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:

CloudPoint 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設定していることを確認します。

- AWS インスタンスの場合は、次を追加します。
169.254.169.254
- GCP 仮想マシンの場合は、次を追加します。
169.254.169.254,metadata,metadata.google.internal
- Azure 仮想マシンの場合は、次を追加します。
169.254.169.254

CloudPoint 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。

- 6 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
管理者ユーザー名 (Admin username)	CloudPoint 管理者ユーザーアカウントのユーザー名を指定します。
管理者パスワード (Admin password)	管理者ユーザーのパスワードを指定します。
新しい admin パスワードの確認 (Confirm Admin password)	管理者ユーザーのパスワードを確認します。
TLS 証明書のホスト名 (Host name for TLS certificate)	CloudPoint 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。 異なる名前を使用してホストに接続する場合、たとえば、 myserver 、 myserver.mydomain 、 myserver.mydomain.mycompany.com などの名前を使用して CloudPoint アクセスを有効にする場合は、ここにすべての名前を追加します。 複数のエントリを指定するにはカンマ (,) を使用します。ここで指定する名前は、同じ CloudPoint ホストを指す必要があります。 指定した名前または IP アドレスは、 CloudPoint の構成に使用するホスト名のリストに追加されます。インストーラはこれらの名前を使用して、 CloudPoint ホストのサーバー証明書を生成します。
ポート	CloudPoint サーバーが通信に使用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。

```
Starting container: flexsnap-nginx ...done
Waiting for CloudPoint configuration to complete (22/22) ...done
Configuration complete at time Thu Feb 18 09:26:36 UTC 2021!
```

- 7 これにより **CloudPoint** の配備プロセスは終了します。次の手順では、**CloudPoint** サーバーを **Veritas NetBackup** プライマリサーバーに登録します。

CloudPoint 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。**CloudPoint** がオンプレミスに配備されている場合の手順については、『**NetBackup Snapshot Client 管理者ガイド**』を参照してください。

メモ: CloudPoint を再起動する必要がある場合は、`podman run` 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.48 の「[CloudPoint の再起動](#)」を参照してください。

CloudPoint が正常にインストールされたことの確認

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、CloudPoint 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!
```

- 次のコマンドを実行して、CloudPoint 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: # `podman ps -a`

コマンドの出力は次のようになります。

CONTAINER ID	IMAGE	CREATED	STATUS
076d3c2252fb	veritas/flexsnap-workflow:9.0.1.0.9261	system 3 days ago	Up 3 days ago
flexsnap-workflow-system-0-min			
07df8d5d083e	veritas/flexsnap-rabbitmq:9.0.1.0.9261	3 days ago	Up 3 days ago
flexsnap-rabbitmq			
1d30b1922dad	veritas/flexsnap-onhostagent:9.0.1.0.9261	3 days ago	Up 3 days ago
flexsnap-onhostagent			
4ecca5996401	veritas/flexsnap-notification:9.0.1.0.9261	3 days ago	Up 3 days ago
flexsnap-notification			
5c2763afe3bd	veritas/flexsnap-nginx:9.0.1.0.9261	3 days ago	Up 3 days ago
0.0.0.0:443->443/tcp	flexsnap-nginx		
5d5805787cda	veritas/flexsnap-coordinator:9.0.1.0.9261	3 days ago	Up 3 days ago
flexsnap-coordinator			
64ebf4083dbd	veritas/flexsnap-config:9.0.1.0.9261	3 days ago	Exited (15) 3 days ago
flexsnap-config			
6ca231fc35c2	veritas/flexsnap-certauth:9.0.1.0.9261	3 days ago	Up 3 days ago
flexsnap-certauth			
7356cabb486	veritas/flexsnap-agent:9.0.1.0.9261	3 days ago	Up 3 days ago flexsnap-agent
756ba92314fb	veritas/flexsnap-mongodb:9.0.1.0.9261	3 days ago	Up 3 days ago
flexsnap-mongodb			
79b7ad032fb7	veritas/flexsnap-workflow:9.0.1.0.9261	general 3 days ago	Up 3 days ago
flexsnap-workflow-general-0-min			

```
9018a4a7cb08 veritas/flexsnap-workflow:9.0.1.0.9261 indexing general 3 days ago Up 3
days ago flexsnap-workflow-indexing-0-min
b9db2708f7f6 veritas/flexsnap-policy:9.0.1.0.9261 3 days ago Up 3 days ago flexsnap-policy
cb3e69c27ab1 veritas/flexsnap-idm:9.0.1.0.9261 3 days ago Up 3 days ago flexsnap-idm
d25d774ed2e8 veritas/flexsnap-scheduler:9.0.1.0.9261 3 days ago Up 3 days ago
flexsnap-scheduler
d58206a3c3d7 veritas/flexsnap-api-gateway:9.0.1.0.9261 3 days ago Up 3 days ago
0.0.0.0:8472->8472/tcp flexsnap-api-gateway
f522cedea280 veritas/flexsnap-listener:9.0.1.0.9261 3 days ago Up 3 days ago
flexsnap-listener
feced68604cc veritas/flexsnap-fluentd:9.0.1.0.9261 3 days ago Up 3 days ago
0.0.0.0:24224->24224/tcp flexsnap-fluentd
```

メモ: イメージ名列に表示される数字 (9.0.1.0.9261) は、CloudPoint 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場合があります。

CloudPoint の再起動

CloudPoint 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。

Docker 環境で CloudPoint を再起動するには

警告: `docker restart` または `docker stop` および `docker start` などのコマンドを CloudPoint の再起動に使用しないでください。次に示す `docker run` コマンドを使用します。

- ◆ CloudPoint がインストールされているインスタンスで、次のコマンドを入力します。

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> restart
```

ここで、**version** は、現在インストールされている CloudPoint 製品のバージョンを表します。

次に例を示します。

```
# sudo docker run -it -rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.0.8549 restart
```

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。

Podman 環境で CloudPoint を再起動するには

- 1 まず、CloudPoint がインストールされているインスタンスで、次のコマンドを使用して CloudPoint を停止します。

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<version> stop
```

- 2 その後、次のコマンドを使用して再起動します。

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<version> start
```

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。

CloudPoint の再起動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。

RHEL 8.3 環境の CloudPoint 層に古い IP アドレスエントリが保持されている場合、CloudPoint サービスの開始または再起動が失敗する場合があります。

CloudPoint サービスコンテナの再起動時に、次のエラーが発生する場合があります。

```
Error adding network: failed to allocate for range 0: 10.89.0.140
has been allocated to
02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc,
duplicate allocation is not allowed
ERRO[0000] Error while adding pod to CNI network "flexsnap-network":
failed to allocate for
range 0: 10.89.0.140 has been allocated to
02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc,
duplicate allocation is not allowed
Error: error configuring network namespace for container
02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc:
failed to allocate for rangae 0:
10.89.0.140 has been allocated to
02da9e9aab2f79303c53dfb10b5ae6b6b70288d36b8fffbdfabba046da5a9afc,
duplicate allocation is not allowed"
```

この問題は、コンテナが停止したときに、コンテナに割り当てられている既存の IP を `dir /var/lib/cni/networks/flexsnap-network/` から削除できない、Podman サブシステムに存在します。

回避方法

古いエントリを削除するには

- 1 コンテナが停止するときに保持される古い IP アドレスを検索します。たとえば、上記のエラーでは 10.89.0.140 です。

- 2 次のコマンドを実行して、`dir` から古いエントリを削除します。

```
# rm /var/lib/cni/networks/flexsnap-network/<stale IP address>
```

- 3 続いて、次のコマンドを使用してサービスを起動します。

```
# podman start <service-name>
```

CloudPoint 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。

- [CloudPoint 拡張機能のインストールを開始する前に](#)
- [VM への拡張機能のインストールの準備](#)
- [VM への CloudPoint 拡張機能のインストール](#)
- [管理対象 Kubernetes クラスタへの拡張機能のインストールの準備](#)
- [CloudPoint 拡張機能のダウンロード](#)
- [管理対象 Kubernetes クラスタへの CloudPoint 拡張機能のインストール](#)
- [拡張機能の管理](#)

CloudPoint 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 **CloudPoint** 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。

CloudPoint 拡張機能のインストールにも適用される、CloudPoint をインストールする際の一般的な準備手順を参照してください。

- CloudPoint 拡張機能をインストールする場所を決定します。
p.15 の「[CloudPoint 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.17 の「[システム要件への準拠](#)」を参照してください。

- (VM ベースの拡張機能の場合) CloudPoint 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.30 の「[CloudPoint 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。
- (VM ベースの拡張機能の場合) 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.31 の [表 1-13](#) を参照してください。
- CloudPoint 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。管理対象の Kubernetes クラスタベースの拡張機能の場合、ファイル共有サイズは 30 GB になる場合があります。
p.32 の「[CloudPoint 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 CloudPoint 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。CloudPoint ホストで RabbitMQ 通信を行う場合は、ポート 5671 を開く必要があります。
p.34 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。

拡張機能のインストールおよび構成処理について

CloudPoint 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からタスクを実行します。

- p.52 の「[VM への拡張機能のインストールの準備](#)」を参照してください。
- p.53 の「[VM への CloudPoint 拡張機能のインストール](#)」を参照してください。
- p.55 の「[管理対象 Kubernetes クラスタへの拡張機能のインストールの準備](#)」を参照してください。
- p.61 の「[管理対象 Kubernetes クラスタへの CloudPoint 拡張機能のインストール](#)」を参照してください。

VM への拡張機能のインストールの準備

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。

- CloudPoint 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 CloudPoint イメージを選択し、ホストを作成します。
p.30 の「[CloudPoint 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.34 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.31 の [表 1-13](#) を参照してください。
- ベリタスのサポートサイトから OS 固有の **CloudPoint** イメージをダウンロードします。
 - **Docker** 環境では、ホストにイメージをロードします。

```
# sudo docker load -i CloudPoint_image_name
```
 - **Podman** 環境では、イメージファイルを解凍します。

```
# gunzip VRTScloudpoint-podman-9.x.x.x.x.tar.gz
```


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

```
# ./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。
- p.53 の「[VM への CloudPoint 拡張機能のインストール](#)」を参照してください。

VM への CloudPoint 拡張機能のインストール

CloudPoint 拡張機能をインストールする前に

p.52 の「[VM への拡張機能のインストールの準備](#)」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 Docker 環境の場合:

次のコマンドを実行します。

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

メモ: これは改行のない 1 つのコマンドです。

Podman 環境の場合:

次のコマンドを実行します。

```
# podman run -it --rm --privileged
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<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、CloudPoint は次を実行します。

- 各 CloudPoint 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 次に、NetBackup Web UI に移動し、「CloudPoint 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、検証トークンを生成してコピーします。
- p.60 の「[CloudPoint 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
Cloudpoint IP アドレス/FQDN	メイン CloudPoint ホストの IP アドレスまたは FQDN を指定します。
Cloudpoint トークン	手順 8 でコピーしたトークンを貼り付けます。
拡張機能の識別名	NetBackup UI に表示される拡張機能の識別名

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 CloudPoint 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)]、[CloudPoint サーバー (CloudPoint Servers)] タブの順に移動して[詳細設定 (Advanced Settings)]をクリックし、[CloudPoint 拡張機能 (CloudPoint extensions)]タブに移動して確認します。
- 次のコマンドを実行し、CloudPoint 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-workflow:9.1.x.x.xxxxx
"/usr/bin/flexsnap-w..." 13 minutes ago Up 13 minutes
flexsnap-workflow-system-b17e4dd9f6b04d41a08e3a638cd91f61-0
26472ebc6d39 veritas/flexsnap-workflow:9.1.x.x.xxxxx
"/usr/bin/flexsnap-w..." 13 minutes ago Up 13 minutes
flexsnap-workflow-general-b17e4dd9f6b04d41a08e3a638cd91f61-0
4f24f6acd290 veritas/flexsnap-listener:9.1.x.x.xxxxx
"/usr/bin/flexsnap-l..." 13 minutes ago Up 13 minutes
flexsnap-listener
4d000f2d117d veritas/flexsnap-cloudpoint:9.1.x.x.xxxxx
"/root/ipv6_configur..." 13 minutes ago Exited (137) 13 minutes ago
flexsnap-ipv6config
92b5bdf3211c veritas/flexsnap-fluentd:9.1.x.x.xxxxx
"/root/flexsnap-flue..." 13 minutes ago Up 13 minutes 5140/tcp,
0.0.0.0:24224->24224/tcp flexsnap-fluentd
db1f0bff1797 veritas/flexsnap-datamover:9.1.x.x.xxxxx
"/entrypoint.sh -c d..." 13 minutes ago Up 13 minutes
flexsnap-datamover.134b6158ea5a443dba3c489d553098c5
c4ae0eb61fb0 veritas/flexsnap-datamover:9.1.x.x.xxxxx
"/entrypoint.sh -c d..." 13 minutes ago Up 13 minutes
flexsnap-datamover.8e25f89f04e74b01b4fe04e7e5bf8644
1bcaa2b646fb veritas/flexsnap-datamover:9.1.x.x.xxxxx
"/entrypoint.sh -c d..." 13 minutes ago Up 13 minutes
flexsnap-datamover.b08591bdde0f445f83f4ada479e6ddfd
```

管理対象 Kubernetes クラスタへの拡張機能のインストールの準備

CloudPoint 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、CloudPoint のクラウドベース拡張機能を管理対象 Kubernetes クラスタに配備できます。

メモ: 現在、この拡張機能は Azure クラウド環境内にある管理対象 Kubernetes クラスタでのみサポートされます。

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 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、CloudPoint 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、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 Container Registry 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、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。
- 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、CloudPoint 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。
- CloudPoint 拡張機能のイメージ (flexsnap-cloudpoint、flexsnap-listener、flexsnap-workflow、flexsnap-fluentd、flexsnap-datamover) を Azure Container Registry にアップロードする必要があります。

Azure でホストと管理対象 Kubernetes クラスタを準備する

- CloudPoint 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 CloudPoint イメージを選択し、ホストを作成します。
p.30 の「CloudPoint 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 CloudPoint ホストでポート 5671 が開いていることを確認します。
p.34 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.31 の表 1-13 を参照してください。
- Azure 環境内で CloudPoint 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。
<https://docs.microsoft.com/ja-jp/cli/azure/install-azure-cli-linux?pivots=apt>
- Kubernetes CLI をインストールします。
<https://kubernetes.io/ja/docs/tasks/tools/#install-using-native-package-management>
- 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>
```
- CloudPoint イメージのプッシュ (アップロード) 先となる Azure Container Registry 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。
<https://docs.microsoft.com/ja-jp/azure/container-registry/container-registry-get-started-portal>
<https://docs.microsoft.com/ja-jp/azure/container-registry/container-registry-get-started-azure-cli>

Create Kubernetes cluster

[Basics](#)
[Node pools](#)
[Authentication](#)
[Networking](#)
[Integrations](#)
[Tags](#)
[Review + create](#)

Connect your AKS cluster with additional services.

Azure Container Registry
Connect your cluster to an Azure Container Registry to enable seamless deployments from a private image registry. You can create a new registry or choose one you already have. [Learn more about Azure Container Registry](#) ⓘ

Container registry [Create new](#)

Azure Monitor
In addition to the CPU and memory metrics included in AKS by default, you can enable Container Insights for more comprehensive data on the overall performance and health of your cluster. Billing is based on data ingestion and retention settings.
[Learn more about container performance and health monitoring](#)
[Learn more about pricing](#)

Container monitoring ☒ Enabled ☐ Disabled

Log Analytics workspace ⓘ [Create new](#)

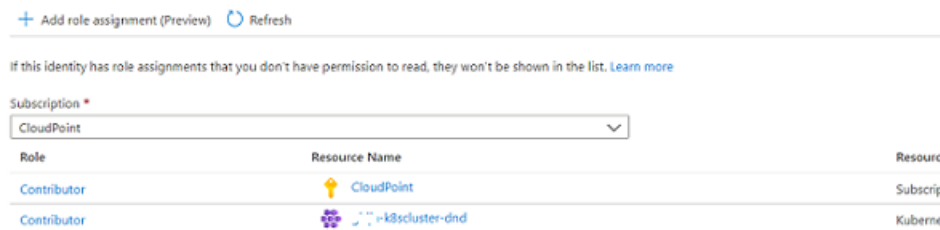
Azure Policy
Apply at-scale enforcements and safeguards for AKS clusters in a centralized, consistent manner through Azure Policy. [Learn more about Azure Policy for AKS](#) ⓘ

Azure Policy ☐ Enabled ☒ Disabled

[Review + create](#)
[< Previous](#)
[Next : Tags >](#)

- ホストシステムから `kubectl` および **Container Registry** 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 (**Virtual Machine**)]に移動して左側の[ID (**Identity**)]をクリックし、[システム割り当て済み (**System assigned**)]タブで[状態 (**Status**)]を[オン (**ON**)]に変更し、[Azure ロールの割り当て (**Azure role assignment**)]、[ロールの割り当ての追加 (**Add role assignments**)]の順にクリックし、[スコープ (**Scope**)]で[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、[ロール (**Role**)]で **Azure Kubernetes Service RBAC ライター**、**AcrPush**、**Azure Kubernetes Service クラスタユーザーロール**を割り当てて[保存 (**Save**)]を選択します。
- **Kubernetes** クラスタに移動し、左側の [アクセス制御 (**IAM**) (**Access Control** (**IAM**))]、[ロールの割り当ての追加 (**Add role assignments**)]の順にクリックし、[ロール (**Role**)]で[共同作成者 (**Contributor**)]、[アクセスの割り当て先 (**Assign access to**)]で[仮想マシン (**Virtual Machines**)]、ドロップダウンで VM の順に選択し、[保存 (**Save**)]をクリックします。

Azure role assignments



- **Kubernetes** クラスタが存在するのと同じサブスクリプションおよび領域にストレージアカウントを作成し、そこにファイル共有を作成します(**Azure** のデフォルトの設定に従います)。

<https://docs.microsoft.com/ja-jp/azure/storage/files/storage-how-to-create-file-share?tabs=azure-portal>

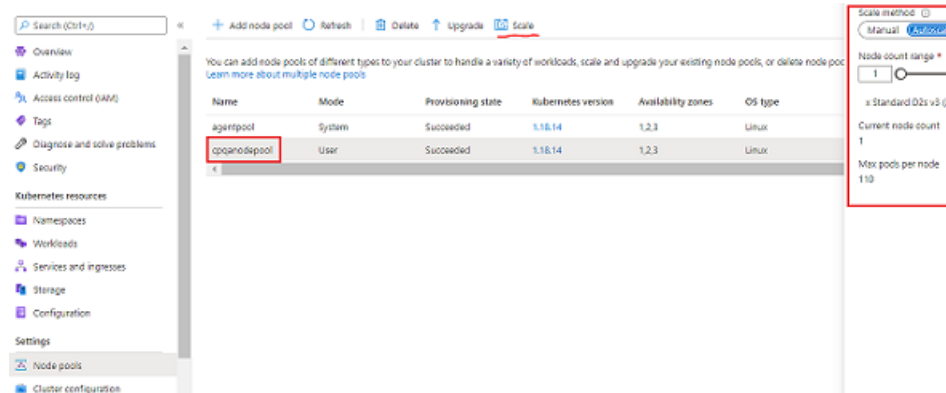
- ホストシステムのコマンドラインから **CloudPoint** の名前空間を作成します。
`kubectl create namespace cloudpoint-system`
- ファイル共有にアクセスするための **Kubernetes Secret** を作成します。**CloudPoint** 拡張機能を構成する際に、この **Secret** を指定する必要があります。
`kubectl create secret generic <secret_name> --namespace cloudpoint-system`
--from-literal=azurestorageaccountname=<storage_account_name>
--from-literal=azurestorageaccountkey=<storage_account_key>
コマンドで次のパラメータを渡します。

パラメータ	説明
<code>secret_name</code>	作成する Secret の名前を指定します。
<code>storage_account_name</code>	Azure ストレージアカウント名を指定します。
<code>storage_account_key</code>	アカウントのアクセスキーを取得するには、Azure ストレージアカウントに移動し、左側で「アクセスキー (Access Keys)」, 「キーを表示 (Show Keys)」の順にクリックし、 Key1 をコピーします。次に、コマンドでアクセスキーを指定します。

例:

```
# kubectl create secret generic mysecret --namespace
cloudpoint-system --from-literal=azurestorageaccountname=mystorage
--from-literal=azurestorageaccountkey=IusI10S9w6n1Ve4N3lpFCaWNCWWFQMw0WzDQT....
```

- 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、**CloudPoint** 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.91 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。
- p.60 の「[CloudPoint 拡張機能のダウンロード](#)」を参照してください。
- p.61 の「[管理対象 Kubernetes クラスタへの CloudPoint 拡張機能のインストール](#)」を参照してください。

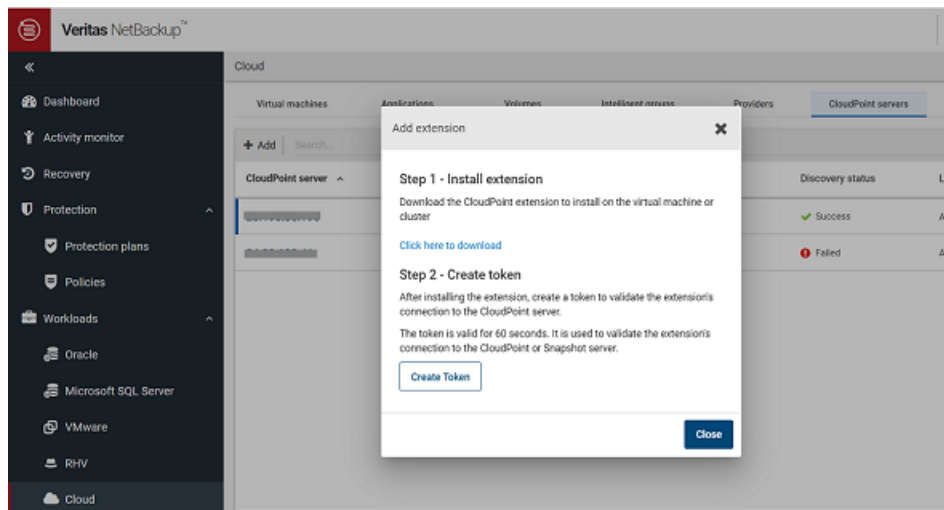
CloudPoint 拡張機能のダウンロード

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 左側のナビゲーションペインで、[クラウド (Cloud)]をクリックし、次に[CloudPoint サーバー (CloudPoint servers)]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 CloudPoint サーバーが表示されます。

- 3 目的の CloudPoint サーバー行で、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 (Azure クラウド上の) 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 ブラウザのタブが起動します。

[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。拡張機能スクリプトがダウンロードされます。
- 6 次の手順に進んで検証トークンを生成する前に、ダウンロードしたスクリプトを CloudPoint ホストにコピーし、コマンドプロンプトから拡張スクリプトを実行して拡張機能を構成します。

p.53 の「[VM への CloudPoint 拡張機能のインストール](#)」を参照してください。

p.61 の「[管理対象 Kubernetes クラスタへの CloudPoint 拡張機能のインストール](#)」を参照してください。
- 7 検証トークンを生成するには、[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。

管理対象 Kubernetes クラスタへの CloudPoint 拡張機能のインストール

CloudPoint 拡張機能をインストールする前に

- p.55 の「[管理対象 Kubernetes クラスタへの拡張機能のインストールの準備](#)」を参照してください。
- p.60 の「[CloudPoint 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 拡張スクリプト `cp_extension_start.sh` がダウンロード済みであることを確認します。

p.60 の「CloudPoint 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 CloudPoint 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、CloudPoint コンテナのイメージ (`flexsnap-cloudpoint`、`flexsnap-listener`、`flexsnap-workflow`、`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-cloudpoint`

- 3 以前に準備手順で作成した 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。

p.55 の「管理対象 Kubernetes クラスタへの拡張機能のインストールの準備」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
<code>container_registry_path</code>	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: <code>mycontainer.azurecr.io</code>
<code>tag</code>	CloudPoint イメージのバージョン。 例: <code>9.0.1.0.9129</code>

- 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-cloudpoint:tag`
 - ターゲットイメージタグ:
`<container_registry_path>/<source_image_name>:<CloudPoint_version_tag>`

例:

```
# docker tag veritas/flexsnap-cloudpoint:9.0.1.0.9129
mycontainer.azurecr.io/veritas/flexsnap-cloudpoint:9.0.1.0.9129
# docker tag veritas/flexsnap-listener:9.0.1.0.9129
mycontainer.azurecr.io/veritas/flexsnap-listener:9.0.1.0.9129
# docker tag veritas/flexsnap-fluentd:9.0.1.0.9129
mycontainer.azurecr.io/veritas/flexsnap-fluentd:9.0.1.0.9129
# docker tag veritas/flexsnap-workflow:9.0.1.0.9129
mycontainer.azurecr.io/veritas/flexsnap-workflow:9.0.1.0.9129
# docker tag veritas/flexsnap-datamover:9.0.1.0.9129
mycontainer.azurecr.io/veritas/flexsnap-datamover:9.0.1.0.9129
```

- 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-cloudpoint:9.0.1.0.9129
# docker push
mycontainer.azurecr.io/veritas/flexsnap-listener:9.0.1.0.9129
# docker push
mycontainer.azurecr.io/veritas/flexsnap-fluentd:9.0.1.0.9129
# docker push
mycontainer.azurecr.io/veritas/flexsnap-workflow:9.0.1.0.9129
# docker push
mycontainer.azurecr.io/veritas/flexsnap-datamover:9.0.1.0.9129
```

- 5 イメージをコンテナレジストリにプッシュしたら、kubect1 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_start.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
cloudpoint_ip	メイン CloudPoint 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-cloudpoint イメージのターゲットイメージタグ。 例: 'mycontainer.azurecr.io/veritas/flexsnap-cloudpoint:9.0.1.0.9129'
namespace	以前に準備手順で作成した CloudPoint 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せん。 1 ノードの名前を取得します。 <pre># kubectl get nodes grep <node_name></pre> 2 タグの key=value ラベルを取得します。 <pre># kubectl describe node <node_name> -n <namespace> grep -i labels</pre> 出力例: agentpool=cpuserpool
secret_name	以前に準備手順で作成した Kubernetes Secret。 例: mysecret
fileshare_name	Azure ポータルのストレージアカウントで、ファイル共有の名前を確認できます。ストレージアカウントと Kubernetes クラスタを同じ領域に配置することをお勧めします。 例: mysharename
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.60 の「CloudPoint 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_start.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_start.sh install -c <cloudpoint_ip> -i <target_image:tag> -n <namespace> -p <tag_key=tag_val> -s <secret_name> -f <fileshare_name> -t <workflow_token>
例:


```
# ./cp_extension_start.sh install
-c 10.20.xx.xxx
-i
mycontainer.azurecr.io/veritas/flexsnap-cloudpoint:9.0.1.0.9271

-n cloudpoint-system
-p agentpool=cpuserpool
-s mysecret
-f mysharename
-t
workflow-3q3ou4jxiircp9tk0eer2g9jx7mwuyypwz10k4i3sms2e7k4ee7-.....
```

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_start.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。

```
CloudPoint IP or fully-qualified domain name: 10.20.xx.xxx
Veritas CloudPoint image repository path.
Format=<Login-server/image:tag>:
mycontainer.azurecr.io/veritas/flexsnap-cloudpoint:9.0.1.0.9255
CloudPoint extension namespace: cloudpoint-system
Node pool with format key=value: agentpool=cpuserpool
Azure Fileshare Secret: mysecret
Azure Fileshare Name: mysharename
CloudPoint extension token:

Getting CloudPoint service file ...done
Getting CloudPoint CRD file ...done
Azure Fileshare Secret Validation ...done

Starting CloudPoint service deployment

namespace/cloudpoint-system configured

deployment.apps/flexsnap-cloudpoint 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

CloudPoint service deployment ...done

customresourcedefinition.apiextensions.k8s.io/cloudpoint-servers.veritas.com
condition met

Generating CloudPoint Custom Resource Definition object

cloudpointrule.veritas.com/cloudpoint-config-rule created

CloudPoint extension installation ...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、CloudPoint 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)]、[CloudPoint サーバー (CloudPoint Servers)]タブの順に移動して[詳細設定 (Advanced Settings)]をクリックし、[CloudPoint 拡張機能 (CloudPoint extensions)]タブに移動して確認します。
- 次のコマンドを実行し、flexsnap-cloudpoint-xxx、flexsnap-fluentd-xxx、flexsnap-listener-xxx、flexsnap-fluentd-collector-xxx、flexsnap-datamover-xxxx 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。

表 3-1 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)]、[CloudPoint サーバー (CloudPoint Servers)] タブの順に移動して[詳細設定 (Advanced Settings)]をクリックし、[CloudPoint 拡張機能 (CloudPoint 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: CloudPoint 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。その後、同じ CloudPoint 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。
VM ベースの拡張機能の停止、起動、または再起動 拡張機能を停止するには:	拡張機能のホスト VM で次のコマンドを実行して、拡張機能を停止、起動、再起動します。 Docker の場合: <pre># sudo docker run -it --rm -v /<full_path_to_volume_name>:<full_path_to_volume_name> -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-cloudpoint:<version> stop</pre> Podman の場合: <pre># podman run -it --rm --privileged -v /<full_path_to_volume_name>:<full_path_to_volume_name> -v /run/podman/podman.sock:/run/podman/podman.sock veritas/flexsnap-cloudpoint:<version> stop</pre>

オプション	手順
拡張機能を起動するには:	Docker の場合: <pre># sudo docker run -it --rm -v /<full_path_to_volume_name>:/<full_path_to_volume_name> -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-cloudpoint:<version> start</pre> Podman の場合: <pre># podman run -it --rm --privileged -v /<full_path_to_volume_name>:/<full_path_to_volume_name> -v /run/podman/podman.sock:/run/podman/podman.sock veritas/flexsnap-cloudpoint:<version> start</pre>
拡張機能を再起動するには:	Docker の場合: <pre># sudo docker run -it --rm -v /<full_path_to_volume_name>:/<full_path_to_volume_name> -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-cloudpoint:<version> restart</pre> Podman の場合: <pre># podman run -it --rm --privileged -v /<full_path_to_volume_name>:/<full_path_to_volume_name> -v /run/podman/podman.sock:/run/podman/podman.sock veritas/flexsnap-cloudpoint:<version> restart</pre>

オプション	手順
VM ベースの拡張機能の証明書の更新	1 拡張機能のホストで次のコマンドを実行します。 <pre># sudo docker run -it --rm -v /<full_path_to_volume_name>:/<full_path_to_volume_name> -v /var/run/docker.sock:/var/run/docker.sock veritas/flexsnap-cloudpoint:<version> renew_extension</pre> 2 次に、証明書の更新を開始するために、CloudPoint IP/FQDN および拡張機能のトークン (NetBackup Web UI から生成可能) を指定します。 p.53 の「VM への CloudPoint 拡張機能のインストール」を参照してください。
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_start.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。 <pre># chmod +x cp_extension_start.sh # ./cp_extension_start.sh renew</pre> 3 次に、証明書の更新を開始するために、CloudPoint 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.61 の「管理対象 Kubernetes クラスタへの CloudPoint 拡張機能のインストール」を参照してください。

CloudPoint クラウドプラグイン

この章では以下の項目について説明しています。

- [CloudPoint クラウドプラグインを構成する方法](#)
- [AWS プラグインの構成に関する注意事項](#)
- [Google Cloud Platform プラグインの構成に関する注意事項](#)
- [Microsoft Azure プラグインの構成に関する注意事項](#)
- [Microsoft Azure Stack Hub プラグインの構成に関する注意事項](#)

CloudPoint クラウドプラグインを構成する方法

CloudPoint プラグインは、クラウドまたはオンプレミス環境の資産の検出を可能にするソフトウェアモジュールです。NetBackup プライマリサーバーに CloudPoint サーバーを登録した後、NetBackup を使用して作業負荷を保護できるように CloudPoint プラグインを構成する必要があります。

プラグインをどのように構成するかは、資産タイプと CloudPoint の配備方法によって決まります。CloudPoint サーバーがクラウドに配備されており、クラウドの作業負荷を保護する場合は、NetBackup Web UI を使用して CloudPoint サーバーを登録し、CloudPoint クラウドとアプリケーションのプラグインを構成する必要があります。資産タイプに関係なく、プラグインを構成するための全体的な手順は類似しています。構成パラメータのみが異なります。

クラウドプラグイン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。

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

メモ: AWS プラグインを構成する前に、CloudPoint 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。

CloudPoint は、次の AWS リージョンをサポートします。

表 4-1 CloudPoint 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-south-1, ap-northeast-1, ap-northeast-2, ap-southeast-1, ap-southeast-2 ■ eu-central-1, eu-west-1, eu-west-2, eu-west-3, eu-north-1, eu-south-1 Milan, eu-south-1 Cape Town ■ cn-north-1, cn-northwest-1 ■ ca-central-1 ■ me-south-1 ■ sa-east-1	■ us-gov-east-1 ■ us-gov-west-1

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

CloudPoint がオンプレミスホストまたは仮想マシンに配備されている場合:

表 4-2 AWS プラグインの構成パラメータ

CloudPoint の構成パラメータ	AWS の同等の用語と説明
アクセスキー	アクセスキー ID をシークレットアクセスキーと共に指定すると、AWS API との通信が CloudPoint に許可されます。
シークレットキー	シークレットアクセスキー。
地域	クラウド資産を検出する 1 つ以上の AWS リージョン。

メモ: CloudPoint は、AES-256 暗号化を使用してクレデンシアルを暗号化します。

CloudPoint が AWS クラウドに配備されている場合:

表 4-3 AWS プラグインの構成パラメータ: クラウド配備

CloudPoint の構成パラメータ	説明
ソースアカウントの構成	
地域	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 CloudPoint 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。
クロスアカウントの構成	
アカウント ID	ソースアカウントに設定されている CloudPoint 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。
ロール名	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。
地域	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。

CloudPoint 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。

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

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。

- CloudPoint 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。

CloudPoint 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、CloudPoint 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 CloudPoint 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
```

```
\¥列举¥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

- RDS インスタンスと Aurora クラスタの自動スナップショットは、CloudPoint からは削除できません。

- **AWS RDS** インスタンスについて、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できません。**CloudPoint** では、このようなインスタンスに対して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できますが、作成される実際のスナップショットではアプリケーションとの整合性は確保されていません。これは **AWS** からの制限事項であり、現在 **CloudPoint** 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。
- **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、**CloudPoint** 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。

- **CloudPoint** 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** インスタンスまたは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 **CloudPoint** 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、**CloudPoint** 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、CloudPoint 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。

- 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。
- CloudPoint 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。
- CloudPoint 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、CloudPoint 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。

<https://aws.amazon.com/premiumsupport/knowledge-center/rds-ipv6/>

- CloudPoint 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。

AWS プラグイン構成の前提条件

CloudPoint 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、CloudPoint で必要なアクセス権を割り当てます。
p.77 の「CloudPoint の AWS アクセス権の構成」を参照してください。
IAM ロールを作成する方法については、AWS のマニュアルを参照してください。
[#create-iam-role](https://docs.aws.amazon.com/IAM/latest/UserGuide/iam-roles-for-amazon-ec2.html#create-iam-role)
- CloudPoint 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は、AWS のマニュアルを参照してください。
[#attach-iam-role](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html#attach-iam-role)

メモ: CFT (CloudFormation テンプレート) を使用して CloudPoint を配備した場合は、CloudPoint 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。

- 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.82 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 (カスタム管理キー) 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。
 - CloudPoint プラグイン構成用の IAM ユーザーを使用している場合は、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、CloudPoint 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 のマニュアルを参照してください。

<https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html#key-policy-default-allow-users>

CloudPoint の AWS アクセス権の構成

AWS (Amazon Web Services) 資産を保護するには、最初に CloudPoint 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 CloudPoint 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。

ユーザーアカウントまたはロールに、CloudPoint 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.78 の「[CloudPoint に必要な AWS アクセス権](#)」を参照してください。

Amazon Web Services 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.71 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。

CloudPoint に必要な AWS アクセス権

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2AutoScaling",
      "Effect": "Allow",
      "Action": [
        "autoscaling:UpdateAutoScalingGroup",
        "autoscaling:AttachInstances"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "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>CreateDBSecurityGroup",
    "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"  
      ],  
      "Resource": [  
        "*"   
      ]  
    },  
    {  
      "Sid": "EC2Recovery",  
      "Effect": "Allow",  
      "Action": [  
        "ec2:RunInstances",  
        "ec2:AttachNetworkInterface",  
        "ec2:DetachVolume",  
      ]  
    }  
  ]  
}
```



```

        "ec2:AttachVolume",
        "ec2:DeleteTags",
        "ec2:CreateTags",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:CreateVolume",
        "ec2:DeleteVolume",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:AssociateIamInstanceProfile",
        "ec2:AssociateAddress",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:RestoreSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:UpdateSecret",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "EBS",
    "Effect": "Allow",
    "Action": [
        "ebs:ListSnapshotBlocks"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "SNS",
    "Effect": "Allow",
    "Action": [
        "sns:Publish",
        "sns:GetTopicAttributes"
    ],
    "Resource": [

```

```
        "arn:aws:sns:*:*:*"
    ],
    },
    {
        "Sid": "IAM",
        "Effect": "Allow",
        "Action": [
            "iam:ListAccountAliases"
        ],
        "Resource": [
            "*"
        ]
    }
]
```

クロスアカウントの構成を作成する前に

CloudPoint 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、CloudPoint 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。

Policies > cp-pun-test-policy
Delete policy

Policy ARN

arn:aws:iam:::cp-pun-test-policy

Description

To test EC2 permission template required for CP.

Permissions
Policy usage
Policy versions
Access Advisor

Policy summary

{ } JSON

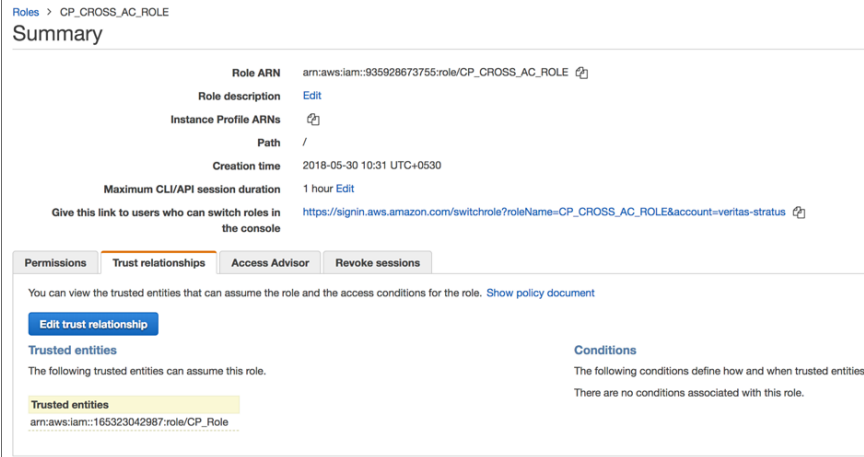
Edit policy

Q Filter

Service	Access level	Resource	Request condition
Allow (3 of 146 services) Show remaining 143			
EC2	Limited: List, Read, Write	Multiple	None
RDS	Limited: List, Read, Write	All resources	None
STS	Limited: Read	All resources	None

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。



The screenshot displays the AWS IAM console interface for a role named **CP_CROSS_AC_ROLE**. The **Summary** tab is active, showing the following details:

- Role ARN:** `arn:aws:iam::935928673755:role/CP_CROSS_AC_ROLE`
- Role description:** [Edit](#)
- Instance Profile ARNs:** [Edit](#)
- Path:** `/`
- Creation time:** 2018-05-30 10:31 UTC+0530
- Maximum CLI/API session duration:** 1 hour [Edit](#)
- Give this link to users who can switch roles in the console:** https://signin.aws.amazon.com/switchrole?roleName=CP_CROSS_AC_ROLE&account=veritas-status

Below the summary, the **Trust relationships** tab is selected. It shows a single trusted entity:

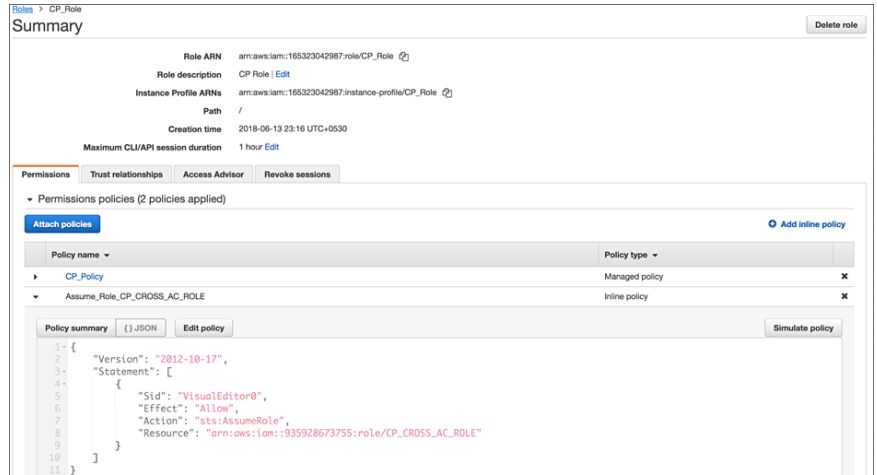
- Trusted entities:** `arn:aws:iam::165323042987:role/CP_Role`

The **Conditions** section indicates that there are no conditions associated with this role.

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 CloudPoint 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。

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ゾー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。

表 4-4 Google Cloud Platform プラグインの構成パラメータ

CloudPoint 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。JSON ファイルには project_id として記載されています。

CloudPoint の構成パラメータ	Google の同等の用語と説明
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。JSON ファイルには <code>client_email</code> として記載されています。
秘密鍵 (Private Key)	秘密鍵。JSON ファイルには <code>private_key</code> 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。
ゾーン (Zones)	プラグインが動作するゾーンのリスト。

CloudPoint は、次の GCP ゾーンをサポートします。

表 4-5 CloudPoint でサポートされる GCP ゾーン

GCP ゾーン
- asia-east1-a, asia-east1-b, asia-east1-c - asia-east2-a, asia-east2-b, asia-east2-c - asia-northeast1-a, asia-northeast1-b, asia-northeast1-c - asia-northeast2-a, asia-northeast2-b, asia-northeast2-c - asia-south1-a, asia-south1-b, asia-south1-c - asia-southeast1-a, asia-southeast1-b, asia-southeast1-c
australia-southeast1-a, australia-southeast1-b, australia-southeast1-c
- europa-north1-a, europa-north1-b, europa-north1-c - europa-west1-b, europa-west1-c, europa-west1-d - europa-west2-a, europa-west2-b, europa-west2-c - europa-west3-a, europa-west3-b, europa-west3-c - europa-west4-a, europa-west4-b, europa-west4-c - europa-west6-a, europa-west6-b, europa-west6-c
- northamerica-northeast1-a, northamerica-northeast1-b, northamerica-northeast1-c - southamerica-east1-a, southamerica-east1-b, southamerica-east1-c

GCP ゾーン

- us-central1-a, us-central1-b, us-central1-c, us-central1-f
- us-east1-b, us-east1-c, us-east1-d
- us-east4-a, us-east4-b, us-east4-c
- us-west1-a, us-west1-b, us-west1-c
- us-west2-a, us-west2-b, us-west2-c
- us-west3-a Utah, us-west3-b Utah, us-west3-c Utah
- us-west4-a Nevada, us-west4-b Nevada, us-west4-c Nevada

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ゾーンを削除すると、そのゾーンから検出されたすべての資産も、CloudPoint 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。
このゾーンをプラグイン構成に再び追加すると、CloudPoint 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。
- 同じプラグインに対して複数の構成を作成する場合は、それらが異なるゾーン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。

p.87 の「[CloudPoint で必要な Google Cloud Platform アクセス権](#)」を参照してください。

p.89 の「[CloudPoint の GCP サービスアカウントの構成](#)」を参照してください。

p.89 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。

CloudPoint で必要な Google Cloud Platform アクセス権

CloudPoint が 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。

```
compute.diskTypes.get
compute.diskTypes.list
compute.disks.create
compute.disks.createSnapshot
compute.disks.delete
compute.disks.get
compute.disks.list
compute.disks.setIamPolicy
```

```

compute.disks.setLabels
compute.disks.update
compute.disks.use
compute.globalOperations.get
compute.globalOperations.list
compute.images.get
compute.images.list
compute.instances.addAccessConfig
compute.instances.attachDisk
compute.instances.create
compute.instances.delete
compute.instances.detachDisk
compute.instances.get
compute.instances.list
compute.instances.setDiskAutoDelete
compute.instances.setMachineResources
compute.instances.setMetadata
compute.instances.setMinCpuPlatform
compute.instances.setServiceAccount
compute.instances.updateNetworkInterface
compute.instances.setLabels
compute.instances.setMachineType
compute.instances.setTags
compute.instances.start
compute.instances.stop
compute.instances.use
compute.machineTypes.get
compute.machineTypes.list
compute.networks.get
compute.networks.list
compute.projects.get
compute.regionOperations.get
compute.regionOperations.list
compute.regions.get
compute.regions.list
compute.snapshots.create
compute.snapshots.delete
compute.snapshots.get
compute.snapshots.list
compute.snapshots.setLabels
compute.snapshots.useReadOnly
compute.subnetworks.get
compute.subnetworks.list

```



```
compute.subnetworks.update
compute.subnetworks.use
compute.subnetworks.useExternalIp
compute.zoneOperations.get
compute.zoneOperations.list
compute.zones.get
compute.zones.list
```

CloudPoint 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 CloudPoint に必要です。カスタムロールを作成し、CloudPoint 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、CloudPoint 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、CloudPoint で必要なすべてのアクセス権を追加します。

p.87 の「CloudPoint で必要な Google Cloud Platform アクセス権」を参照してください。

詳しい手順については、次の GCP のマニュアルを参照してください。

<https://cloud.google.com/iam/docs/creating-custom-roles>

- 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 CloudPoint 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。

詳しい手順については、次の GCP のマニュアルを参照してください。

<https://cloud.google.com/iam/docs/creating-managing-service-accounts#iam-service-accounts-create-console>

プラグイン構成のための GCP サービスアカウントの準備

CloudPoint GCP プラグイン構成の準備をするには

- 1 CloudPoint で必要な GCP 構成パラメータを収集します。

p.85 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
N1lEvA18ADAN89kq4k199w08AQEFAA5C8KYw9951A9EAAo18AQCNvpuJ3oK974z4¥n
.
.
.
weT9odE4ryl81tNU¥nV3q1XNX4fK55Qtpd6CNU+f7QjEw5x8+5ft05DU8ayQcNkX¥n
4pXJoDol54N52+T4qV4WkoFD5uL4NLPz5wxfly¥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
¥
/o/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、CloudPoint 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
4pXJoDo154N52+T4qV4WkoFD5uL4NLPz5wxfl1y¥nNWcNfru8K8a2q1/9o0U+99==
-----END PRIVATE KEY-----
```

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。

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。

- 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のロールにサービスプリンシパルを割り当てます。

詳しくは、次の Azure のマニュアルに記載されている手順に従ってください。

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal>

表 4-6 Microsoft Azure プラグインの構成パラメータ

CloudPoint 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)	アプリケーションを作成した AAD 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。
地域 (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。

CloudPoint の構成パラメータ	Microsoft 製品の同等の用語と説明
リソースグループの接頭辞 (Resource Group prefix)	リソースグループ内のすべてのリソースを追加するために使用する文字列。
接頭辞が付いたリソースグループが見つからなくても資産を保護する (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かどうかによって、資産がどのリソースグループにも関連付けられていない場合に、その資産を保護するかどうかを決めます。接頭辞が付いたリソースグループは、ソースの資産のリソースグループと同じ地域に存在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。
- CloudPoint 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。
- CloudPoint では、Azure 環境での Ultra SSD ディスク形式のスナップショット操作はサポートされていません。CloudPoint で Ultra ディスクが正常に検出された場合でも、そのようなディスク資産でトリガされるスナップショット操作は次のエラーで失敗します。

Snapshots of UltraSSD_LRS disks are not supported.

- 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 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
- CloudPointAzure 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	■ 中国東部
CloudPoint 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 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)

- Microsoft Azure Gen2 形式の仮想マシンはサポートされません。Gen1 のイメージ形式を使用して VM を作成していることを確認します。
- CloudPoint 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。

Microsoft Azure でのアクセス権の設定

CloudPoint 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。CloudPoint 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 CloudPoint 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。

```
{ "Name": "CloudPoint Admin",
  "IsCustom": true,
  "Description": "Necessary permissions for
Azure plug-in operations in CloudPoint",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/beginGetAccess/action",
    "Microsoft.Compute/disks/endGetAccess/action",
    "Microsoft.Compute/images/write",
    "Microsoft.Compute/images/delete",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/beginGetAccess/action",
    "Microsoft.Compute/snapshots/endGetAccess/action",
    "Microsoft.Compute/virtualMachines/capture/action",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/generalize/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/runCommand/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Network/*/read",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/publicIPAddresses/join/action",
    "Microsoft.Network/publicIPAddresses/write",
```

```
"Microsoft.Network/routeTables/join/action",
"Microsoft.Network/virtualNetworks/delete",
"Microsoft.Network/virtualNetworks/subnets/delete",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/write",
"Microsoft.Resources/*/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/ ¥
validateMoveResources/action",
"Microsoft.Resources/subscriptions/tagNames/tagValues/write",
"Microsoft.Resources/subscriptions/tagNames/write",
"Microsoft.Subscription/*/read",
"Microsoft.Authorization/locks/*",
"Microsoft.Authorization/*/read" ],
"NotActions": [ ],
"AssignableScopes": [
"/subscriptions/subscription_GUID",
"/subscriptions/subscription_GUID/ ¥
resourceGroups/myCloudPointGroup" ] }
```

CloudPoint 拡張機能が Azure の管理対象 Kubernetes クラスタにインストールされている場合は、プラグインを構成する前に次の権限も追加できます。

```
"Microsoft.ContainerService/managedClusters/agentPools/read",
"Microsoft.ContainerService/managedClusters/read",
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSet
```

Powershell を使用してカスタム役割を作成するには、次の Azure マニュアルの手順に従ってください。

<https://docs.microsoft.com/ja-jp/azure/role-based-access-control/tutorial-custom-role-powershell>

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、次の Azure マニュアルの手順に従ってください。

<https://docs.microsoft.com/ja-jp/azure/role-based-access-control/tutorial-custom-role-cli>

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。
- CloudPoint 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.91 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 9.0 には、Azure の増分スナップショットが導入されています。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、次の Azure Stack のマニュアルを参照してください。

<https://docs.microsoft.com/ja-jp/azure-stack/operator/azure-stack-identity-overview?view=azs-2008>

- 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、次の 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。

<https://docs.microsoft.com/ja-jp/azure-stack/operator/azure-stack-create-service-principals>

表 4-7 AAD を使用した Azure Stack Hub プラグインの構成パラメータ

CloudPoint 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)	CloudPoint 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。
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。

表 4-8 AD FS を使用した Azure Stack Hub プラグインの構成パラメータ

CloudPoint 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)	CloudPoint 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>
ユーザー名 (User Name)	AzureStackAdmin ドメイン管理者アカウントのインストール時に指定されたユーザー名。次の形式で示されます。 <Azure Stack Hub domain>\<cloud admin user name>
パスワード (Password)	AzureStackAdmin ドメイン管理者アカウントのインストール時に指定されたパスワード。
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。
- CloudPoint 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。

- CloudPoint では現在、Azure Stack 管理対象ディスクと、Azure Stack Resource Manager 配備も出る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、CloudPoint 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。
- CloudPoint 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。
- CloudPoint 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

CloudPoint 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。CloudPoint 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 CloudPoint 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。

```
{ "Name": "CloudPoint Admin",
  "IsCustom": true,
  "Description": "Necessary permissions for
  Azure Stack Hub plug-in operations in CloudPoint",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Storage/storageAccounts/listKeys/action",
    "Microsoft.Storage/storageAccounts/ListAccountSas/action",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/images/write",
    "Microsoft.Compute/images/delete",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/beginGetAccess/action",
    "Microsoft.Compute/snapshots/endGetAccess/action",
    "Microsoft.Compute/virtualMachines/capture/action",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/generalize/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/runCommand/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/*/read",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkInterfaces/effectiveNetworkSecurityGroups/action",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/publicIPAddresses/join/action",
```

```
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/routeTables/join/action",
"Microsoft.Network/virtualNetworks/delete",
"Microsoft.Network/virtualNetworks/subnets/delete",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/write",
"Microsoft.Resources/*/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Resources/subscriptions/resourceGroups/ ¥
validateMoveResources/action",
"Microsoft.Resources/subscriptions/tagNames/tagValues/write",
"Microsoft.Resources/subscriptions/tagNames/write",
"Microsoft.Subscription/*/read",
"Microsoft.Authorization/*/read" ],
"NotActions": [ ],
"AssignableScopes": [
"/subscriptions/subscription_GUID",
"/subscriptions/subscription_GUID/ ¥
resourceGroups/myCloudPointGroup" ] }
```

Powershell を使用してカスタム役割を作成するには、次の **Azure Stack** マニュアルの手順に従ってください。

<https://docs.microsoft.com/ja-jp/azure-stack/operator/azure-stack-registration-role?view=azs-2008>

次に例を示します。

```
New-AzRoleDefinition -InputFile "C:¥CustomRoles¥registrationrole.json"
```

Azure CLI を使用してカスタム役割を作成するには、次の **Azure** マニュアルの手順に従ってください。

<https://docs.microsoft.com/ja-jp/azure/role-based-access-control/tutorial-custom-role-cli>

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。

- CloudPoint 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.96 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 2008 バージョンでは、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 CloudPoint サーバーで、

/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。

CloudPoint ストレージアレイプラグイン

この章では以下の項目について説明しています。

- [CloudPoint ストレージアレイのプラグインの構成方法](#)
- [NetApp プラグインの構成に関する注意事項](#)
- [NetApp アレイの ACL の構成](#)
- [Nutanix Files プラグインの構成に関する注意事項](#)
- [Nutanix アレイの ACL の構成](#)
- [Dell EMC Unity アレイプラグインの構成に関する注意事項](#)
- [Pure Storage FlashArray プラグインの構成に関する注意事項](#)
- [HPE RMC プラグインの構成に関する注意事項](#)
- [HPE XP プラグインの構成に関する注意事項](#)
- [Hitachi プラグインの構成に関する注意事項](#)
- [Hitachi \(HDS VSP 5000\) プラグインの構成に関する注意事項](#)
- [InfiniBox プラグインの構成に関する注意事項](#)
- [Dell EMC PowerScale \(Isilon\) プラグインの構成に関する注意事項](#)
- [Dell EMC PowerMax および VMax プラグインの構成に関する注意事項](#)
- [Qumulo プラグインの構成に関する注意事項](#)

CloudPoint ストレージアレイのプラグインの構成方法

CloudPoint プラグインは、クラウドまたはオンプレミス環境の資産の検出を可能にするソフトウェアモジュールです。NetBackup プライマリサーバーに CloudPoint サーバーを登録した後、NetBackup を使用して作業負荷を保護できるように CloudPoint プラグインを構成する必要があります。

プラグインをどのように構成するかは、資産タイプと CloudPoint の配備方法によって決まります。CloudPoint サーバーがオンプレミスで配備されていて、ストレージアレイを保護する場合は、NetBackup 管理コンソール (Java UI) を使用して CloudPoint サーバーを登録し、ストレージアレイプラグインを構成する必要があります。資産タイプに関係なく、プラグインを構成するための全体的な手順は類似しています。構成パラメータのみが異なります。

ストレージプラグインの構成方法について詳しくは、『NetBackup Snapshot Client 管理者ガイド』を参照してください。

NetApp プラグインの構成に関する注意事項

NetApp NAS および SAN 用の CloudPoint プラグインを使用すると、NetApp ストレージアレイ上の次の資産のスナップショットを作成、削除、リストア、エクスポート、およびデポートできます。

- SAN 環境の NetApp LUN (論理ユニット番号) ストレージユニット。
- NAS 環境の NetApp NFS ボリューム。
- NAS クライアントに NFS プロトコルを使用したストレージへのアクセスを許可する、NetApp SVM (ストレージ仮想マシン)。

NetApp プラグイン構成の前提条件

NetApp プラグインを構成する前に、次の点を確認します。

- NetApp ストレージアレイにスナップショット操作を実行するために必要な NetApp ライセンスがあることを確認します。
- サポート対象の ONTAP バージョンが NetApp アレイにインストールされていることを確認します。
CloudPoint は次をサポートします。
 - ONTAP バージョン 8.3 以降
- NAS ベースのストレージ配備の場合、NetApp の共有がアクティブな junction_path を使用して構成されていることを確認します。
- プラグインを構成するために使用する NetApp ユーザーアカウントに、NetApp アレイで次の操作を実行する権限があることを確認します。

- スナップショットの作成
- スナップショットの削除
- スナップショットのリストア
- プラグインを構成するために使用する NetApp ユーザーアカウントが、http および ontapi アクセス方式で構成されていることを確認します。
- プラグインを構成するために使用する NetApp ユーザーアカウントに、次のロールが割り当てられていることを確認します。
 - デフォルト: 読み取り専用
 - LUN: すべて
 - volume snapshot: すべて
 - vservers エクスポートポリシー: すべて
 ユーザーとロールを作成し、アクセス権を割り当てる方法については、NetApp のマニュアルを参照してください。

p.104 の「[NetApp プラグインの構成パラメータ](#)」を参照してください。

p.105 の「[NetApp ストレージでサポートされる CloudPoint 操作](#)」を参照してください。

NetApp プラグインの構成パラメータ

NetApp NAS および SAN プラグインを構成するには、次のパラメータが必要です。

表 5-1 NetApp プラグインの構成パラメータ

CloudPoint の構成パラメータ	説明
アレイの IP アドレスまたは FQDN	NetApp ストレージアレイまたはファイラのクラスタ管理 IP アドレスまたは FQDN (完全修飾ドメイン名)。
ユーザー名	NetApp ストレージアレイまたはファイラでスナップショット操作を実行するアクセス権を持つ NetApp ユーザーアカウント。
パスワード	NetApp ユーザーアカウントのパスワード。

NetBackup アクセスの専用 LIF の構成

NetApp NAS ベースの volume snapshot は、NAS プロトコルを経由して NetBackup に公開されます。NetBackup は、各 SVM (ストレージ仮想マシン) で利用可能な任意のデータ LIF を使用して、これらのスナップショットを読み込みます。必要に応じて、NetBackup アクセス専用のデータ LIF を構成できます。

データ LIF の構成時に、SVM のインターフェース名に接頭辞「`nbu_nas_`」を使用します。このようなデータ LIF が存在する場合、NetBackup は、その LIF のみを自動的に使用してスナップショットにアクセスします。

メモ: (これはオプションの手順です)。構成されている場合、バックアップの読み込みは専用の LIF に制限されます。構成されていない場合、ボリュームのスナップショットには、対応する SVM の利用可能なデータ LIF を介してアクセスします。

NetApp ストレージでサポートされる CloudPoint 操作

CloudPoint は、NetApp ストレージアレイに対して次の管理操作を実行します。

表 5-2 NetApp ストレージでの CloudPoint 操作

CloudPoint 操作	説明
資産の検出	- SAN の配備では、CloudPoint はストレージボリュームから作成された LUN を検出します。 状態がオンラインで、読み取り/書き込み操作が有効になっている、スナップショットの自動削除パラメータが <code>false</code> に設定されている LUN だけが検出されます。 <code>["state":"online","vol_type":"rw","is_snapshot_auto_delete_enabled": "false"]</code> メモ: SAN の配備で、CloudPoint は CloudPoint を使用して作成されたスナップショットのみを検出できます。 - NAS の配備で、CloudPoint は NetApp ストレージ上のすべての NFS 共有、およびセキュリティスタイルが UNIX で混合モードのボリュームを検出します。 CloudPoint で共有の検出を可能にするには、共有にアクティブな <code>junction_path</code> が構成されている必要があります。

CloudPoint 操作	説明
スナップショットの作成	■ SAN の配備では、CloudPoint は NetApp LUN のスナップショットを作成します。 CloudPoint が NetApp ストレージで LUN スナップショットをトリガすると、LUN が属しているボリューム全体に対して、ROW (リダイレクトオンライト) スナップショットを内部的にトリガします。ボリュームに複数の LUN が含まれる場合、スナップショットにはそのボリュームに存在するすべての LUN のデータが含まれます。 CloudPoint によって作成される一般的なスナップショットには、次の命名規則があります。 NB<unique_21digit_number> ■ NAS の配備では、CloudPoint は NetApp NFS 共有のスナップショットを作成します。
スナップショットの削除	■ SAN の配備では、LUN のスナップショットを削除するときに、CloudPoint は LUN が属する 1 つ以上のボリュームのスナップショットを内部的に削除します。 ■ NAS 配備では、CloudPoint は共有のスナップショットを削除します。
スナップショットのリストア	■ SAN の配備では、スナップショットから LUN をリストアするときに、CloudPoint はリストアがトリガされた特定の LUN のみをリストアします。LUN スナップショットは、基になるボリュームの ROW スナップショットであり、そのボリュームには複数の追加の LUN を含めることができます。スナップショットに複数の LUN のデータが含まれている場合でも、選択した LUN に対してのみリストアが実行されます。その他の LUN のデータは変更されないままです。 ■ NAS 配備では、CloudPoint は指定したスナップショットを使用してボリュームをリストアします。

CloudPoint 操作	説明
スナップショットのエクスポート	■ SAN の配備では、スナップショットのエクスポート操作がトリガされると、CloudPoint はスナップショットから LUN を作成してターゲットホストに接続します。ターゲットホストには、エクスポートされた LUN に対する読み取り/書き込み権限が割り当てられます。 エクスポート操作は、次のプロトコルを使用してサポートされます。 ■ FC (ファイバーチャネル) ■ iSCSI (Internet Small Computer Systems Interface) ■ NAS 配備では、スナップショットのエクスポート操作がトリガされると、新しいルールがエクスポートポリシーに作成され、ネットワーク共有として利用可能なエクスポートされたスナップショットに割り当てられます。ターゲットホストには、エクスポートされたスナップショット共有に対する読み取り専用権限が割り当てられます。 エクスポート操作は、NFS プロトコルを使用してサポートされます。 メモ: CloudPoint は SVM の「デフォルト」のエクスポートポリシーは変更しません。ボリュームが NetApp の「デフォルト」のエクスポートポリシーにのみ接続されている場合、エクスポート操作は失敗します。デフォルト以外のエクスポートポリシーに NAS ボリュームを割り当てる必要があります。
スナップショットのデポート	SAN 配備では、スナップショットのデポート操作がトリガされると、CloudPoint はターゲットホストから LUN マッピングを削除してから LUN を削除します。 NAS 配備では、スナップショットのデポート操作がトリガされると、NetBackup は、スナップショットがエクスポートされたときにエクスポートポリシーに作成された新しいルールを削除します。

スナップショットのエクスポート関連の必要条件と制限事項

NetApp 環境には、次の必要条件と制限事項が適用されます。

- スナップショットをエクスポートするホストはゾーン化し、そのスナップショットを接続またはエクスポートする **SVM** (ストレージ仮想マシン) に追加する必要があります。
- **CloudPoint** のスナップショットのエクスポート操作は、デフォルトのアレイエクスポートポリシーが割り当てられている共有に対して失敗します。エクスポート操作を実行する前に、(デフォルト以外の) 別のエクスポートポリシーを共有に割り当てていることを確認します。
- スナップショットは複数回エクスポートできません。
- エクスポートされたスナップショットは削除できません。

NetApp アレイの ACL の構成

NetApp アレイの ACL を構成するには:

- 1 OnCommand System Manager コンソールにログインします。
- 2 SMB ボリュームまたは共有を作成する各 SVM に移動します。
- 3 右ペインの[SVM 設定 (SVM setting)]をクリックします。
- 4 左のナビゲーションペインの[ホストユーザーとグループ (Host Users and Groups)]で[Windows]をクリックします。
- 5 右ペインで[グループ (Groups)]タブと[ユーザー (Users)]タブが開きます。
- 6 [グループ (Groups)]タブで BUILTIN\Backup Operators をクリックし、上部の[編集 (Edit)]オプションを選択します。
- 7 [変更 (Modify)]ダイアログの[メンバ (Members)]フレームで、ドメインユーザーを追加して、[SetBackupPrivilege]、[SetRestorePrivilege]、[SetSecurityPrivilege]の各権限を選択します。

Nutanix Files プラグインの構成に関する注意事項

Veritas NetBackup は、ネットワーク接続ストレージ (NAS) ストレージホストに設定される共有に、堅牢なデータ保護ソリューションを提供します。NetBackup は、この NAS サポートを拡張して、Nutanix Files 環境でホストされているファイルサービスを保護できるようにします。CloudPoint を構成し、NFS (Network File System) のエクスポートとして公開されている Nutanix Files 共有を検出してから、これらに対してバックアップ操作とリストア操作を実行するようにできます。

Nutanix Files 用の CloudPoint プラグインには、NetBackup が Nutanix Files サーバーの共有を検出し、それらの共有に対してスナップショットの作成、エクスポート、デポート、削除の各操作のトリガを可能にする、必要な関数ロジックが含まれています。NetBackup プライマリサーバーでこのプラグインを構成する必要があります。

CloudPoint は、Nutanix REST API を使用して、Nutanix Files ファイルサーバーと通信します。CloudPoint は、自身をバックアップアプリケーションとして登録して Nutanix Files ファイルサーバーとの接続を確立し、API エンドポイントを使用して、バックアップの作成が必要な共有とそのスナップショットを検出します。

Nutanix Files プラグイン構成の前提条件

プラグインを構成する前に、次の操作を実行します。

- サポートされているバージョンの Nutanix Files が、Nutanix アレイにインストールされていることを確認します。
CloudPoint は次をサポートします。

Nutanix Files バージョン 3.6.1.3 以降

- Nutanix Files クラスタについての次の情報を収集します。Nutanix Files プラグインを構成するときに、これらの詳細を使用します。

パラメータ	説明
Nutanix Files ファイルサーバー FQDN	Nutanix Files ファイルサーバーの FQDN (完全修飾ドメイン名)。
REST API ユーザー名	ファイルサーバー上の Nutanix Files REST API を呼び出す権限を持つユーザーアカウント。
REST API パスワード	前の手順で指定した Nutanix REST API ユーザーアカウントのパスワード。

NetBackup 管理コンソールを使用してプラグインを構成すると、次の画面が表示されます。

Configure Plugin @: 10.10.10.10.veritas.com

CloudPoint Server: 10.10.10.10.veritas.com

Selected Plugin: Nutanix Files

Credentials

Enter Plugin ID:
PUNE_NUTANIX_FILES_01

File Server FQDN:
10.10.10.10.veritas.com

REST API Username:
veritas

REST API Password:

OK Cancel Help

Nutanix Files プラグインの考慮事項および制限事項

次の考慮事項と制限事項が適用されます。

- スナップショット操作は、Nutanix Files ファイルサーバーのネストした共有ではサポートされません。
ネストした共有とは、その共有自体が、既存のファイル共有のサブディレクトリであるものです。NetBackup は、このようなネストした共有のスナップショットの作成をサポートしません。

- **Nutanix Files** ファイルサーバーは、スナップショットを使用した共有の指定した時点 (PIT) へのローカルバックリストアをサポートしません。共有のデータの **NetBackup** アシストリストアを使用できます。
- **Nutanix Files** 共有の最大スナップショット数は **20** です。
最大スナップショット数の制限によって、指定した共有に対して保持されるポリシートリガスナップショットの最大数が定義されます。最大数に達すると、ポリシーによって作成される次のスナップショット作成時に、最も古いスナップショットが削除されます。
Nutanix Files 共有を保護する **NetBackup** ポリシーのポリシースケジュールと保持を考慮する必要がある場合があります。

Nutanix Files ファイルサーバーでサポートされる CloudPoint 操作

CloudPoint は、Nutanix Files ファイルサーバー上で次の管理操作を実行します。

表 5-3 Nutanix Files ファイルサーバーでの CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint は、一部のメタデータとともにすべての共有とそのスナップショットを検出します。CFT_BACKUP 機能を備えた共有は、スナップショットの差分に基づいた増分バックアップに適しています。 メモ: スナップショット操作は、Nutanix Files ファイルサーバーのネストした共有ではサポートされません。
スナップショットの作成	スナップショットを作成するために、CloudPoint は必要な共有情報とスナップショット名を使用して、/mount_targets API で POST REST API 呼び出しをトリガします。API は、スナップショットの詳細を返します (マウントターゲットスナップショットとも呼ばれる)。 CloudPoint は、スナップショットの状態が成功 (または、失敗した場合はエラー) に変更されるまで、スナップショットの詳細をポーリングし続けます。
スナップショットの削除	スナップショットを削除するために、CloudPoint は、必要なスナップショットの詳細を使用して、次の形式で DELETE REST API 呼び出しをトリガします。 /mount_target_snapshot/:snapshot_uuid CloudPoint は、「404 Not Found」エラーコードが返されるまで、スナップショット UUID のポーリングを継続します。このコードは、スナップショットが正常に削除されたことを確認します。
スナップショットのリストア	CloudPoint では、この操作はサポートされていません。

CloudPoint 操作	説明
スナップショットのエクスポート	スナップショットのエクスポート操作がトリガされると、バックアップホストがプラグインの構成中に登録されたパートナーサーバーに追加されます。必要なマウントターゲットの詳細を指定して、パートナーサーバーに PUT REST API 呼び出しが行われます。 CloudPoint は、操作が正常に完了したことを確認するために、パートナーサーバーへのポーリングを維持します。
スナップショットのデポート	スナップショットのデポート操作がトリガされると、CloudPoint は、エクスポート操作中に追加されたマウントターゲットエントリを削除するために、パートナーサーバーに PUT REST API 呼び出しを行います。 CloudPoint は、操作が正常に完了したことを確認するために、パートナーサーバーへのポーリングを維持します。
スナップショットの差分の作成	Nutanix ファイルには、共有の 2 つのスナップショット間の差分を作成することを可能にする API が用意されています。このプロセスは、CFT (変更されたファイルの追跡) と呼ばれます。スナップショットの差分の作成要求が行われたときに、CloudPoint は、2 つのスナップショットの間に CFT を生成する REST API 呼び出しを行い、CFT データを取得して CloudPoint サーバーに格納します。 CFT ベースのバックアップは、トップレベルの共有でのみサポートされます。ネストした共有はサポートされません。

Nutanix Files の NetBackup 問題のトラブルシューティング

次を参照してください。

Nutanix Files のバックアップジョブが、スナップショットのインポート操作およびエクスポート操作の失敗のためにエラーになる

Nutanix Files のファイル共有にスケジュールされているバックアップジョブは、スナップショットのインポートおよびエクスポート操作で競合エラーが発生したために失敗することがあります。

ジョブログに次のエラーが含まれます。

```
Snapshot import failed (4213)
Backup from Snapshot job failed with error 4213
Snapshot import failed
(errMsg": "Failed to export Error: Edit conflict: please retry change)
```

```
WARNING: Snapshot export failed.
```

```
Failed to export. Error: Edit conflict: please retry change.  
Error vfms Snapshot export API failed for snapshot ID[snapID].
```

推奨処置:

この問題は、同じ **Nutanix Files** ファイルシステムが、複数の **CloudPoint** サーバーインスタンスで同時に設定されている場合に発生します。

NetBackup は、**Nutanix Files** プラットフォームでパートナーサーバーとして登録されます。**NetBackup CloudPoint** サーバーと **Nutanix Files** の間に、1 対 1 のマッピングが存在します。同じ **Nutanix Files** ファイルシステムが複数の **CloudPoint** インスタンスで構成されると、リソースの競合が発生します。各 **CloudPoint** サーバーは、バックアップジョブ情報を使用して構成を更新しようとします。この単一のパートナーサーバー登録に対する同時の構成の更新は失敗し、競合エラーが発生します。

NetBackup はこのような複合構成をサポートしていません。**NetBackup** ドメイン内の **CloudPoint** サーバーの 1 つのインスタンスを使用して **Nutanix Files** を設定していることを確認します。

Nutanix Files のバージョンがサポートされていない場合にプラグインの構成が失敗することがある

Nutanix Files プラグインの構成が **http 500** 状態コードで失敗し、次のエラーメッセージが表示されることがあります。

サポートされる最小 AFS バージョン 3.6.1.3 (Minimum supported AFS version 3.6.1.3)

この問題は、使用中の **Nutanix Files** のバージョンが **CloudPoint** でサポートされていない場合に発生します。プラグインを構成する前に、サポート対象バージョンの **Nutanix Files** がインストールされていることを確認します。

p.108 の「[Nutanix Files プラグイン構成の前提条件](#)」を参照してください。

Nutanix アレイの ACL の構成

Nutanix アレイの ACL を構成するには:

- 1 Prism コンソールにログオンします。
- 2 ファイルサーバーリストを開き、SMB 共有を作成するファイルサーバーをクリックします。
- 3 右隅の[プロトコル管理 (Protocol Management)]リンクで[ユーザーマッピング (User Mapping)]を選択します。
- 4 [明示的マッピング (Explicit Mapping)]ダイアログが表示されるまで、[次へ (Next)]を複数回クリックします。

- 5 [1 対 1 マッピングの追加 (Add One to One Mapping)]をクリックし、ドメインユーザーと NFS ID を追加し、保存して[次へ (Next)]をクリックします。
- 6 1 人のドメインユーザーをデフォルトのマッピングに追加する必要があります。詳細を保存します。
- 7 選択したファイルサーバーの右ペインで[ロールの管理 (Manage Roles)]をクリックします。
- 8 [管理者の追加 (Add Admins)]セクションでドメインユーザーを追加し、[ロール (Role)]で[バックアップ管理者: バックアップへのアクセスのみ (Backup admin: Backup access only)]を選択します。
- 9 保存してダイアログを閉じます。

Dell EMC Unity アレイプラグインの構成に関する注意事項

Dell EMC Unity アレイプラグイン用の CloudPoint プラグインは、ネットワーク接続ストレージ (NAS) ストレージホストもサポートしており、EMC Unity アレイ環境でホスティングされている NFS (Network File System) およびサーバーメッセージブロック (SMB) のエクスポートを保護できます。NFS および SMB のエクスポートで検出を行い、その後バックアップ操作とリストア操作を実行するように CloudPoint を構成できます。

このプラグインを使用して、NetBackup は EMC Unity アレイで NFS のエクスポートを検出し、それらのエクスポートに対してスナップショットの作成、エクスポート、デポート、削除の各操作をトリガできます。NetBackup プライマリサーバーでこのプラグインを構成する必要があります。

CloudPoint は、Storops バージョン 1.2.8 の REST API SDK を使用して EMC Unity 資産と通信します。CloudPoint は、SDK によって公開された RestClient ライブラリを使用して EMC Unity アレイとの接続を確立し、SDK メソッドを使用して、バックアップの作成が必要な NFS のエクスポートとそのスナップショットを検出します。

Dell EMC Unity アレイプラグインの構成パラメータ

Dell EMC Unity アレイプラグインを構成するには、次のパラメータが必要です。

表 5-4 Dell EMC Unity アレイプラグインの構成パラメータ

NetBackup の構成パラメータ	説明
アレイの IP アドレス	保護するアレイの IP アドレス。IPv6 と IPv4 の両方の設定がサポートされています。

NetBackup の構成パラメータ	説明
ユーザー名	EMC Unity アレイでスナップショット操作を実行する権限を持つユーザーアカウント名。 指定したユーザーアカウントがアレイでスナップショットを作成、削除、およびリストアする権限を持っていることを確認します。
パスワード	前の手順で指定した EMC Unity アレイのユーザーアカウントのパスワード。

NetBackup 管理コンソールを使用してプラグインを構成すると、次の画面が表示されます。

Dell EMC Unity プラグインの考慮事項および制限事項

- このアレイは共有レベルのスナップショットをサポートしません。そのため、スナップショットはファイルレベルで作成され、互いに 1 対 1 のマッピングを行います。
- NetBackup でバックアップ操作がトリガされるたびに、スナップショット形式の新しい共有がアレイに作成され、デポート操作 (期限切れ) がトリガされると、共有は自動的に消去されます。

サポートされる Dell EMC Unity アレイ

CloudPoint を使用して、次の Dell EMC Unity アレイモデルを検出して保護できます。

表 5-5 サポートされる EMC アレイ

カテゴリ	サポート対象
アレイモデル	Unity 600 理論的には、CloudPoint にはモデル固有のコーディングは含まれていないため、他のモデルも機能します。その他のモデルには次のものがあります。 ■ Unity 300 と Unity 300F (「F」はフラッシュアレイであることを示します) ■ Unity 400 および Unity 400F ■ Unity 500 および Unity 500F ■ Unity 600F
ソフトウェア	UnityOS
ファームウェアのバージョン	4.2.1.9535982 以降 ファームウェアのバージョンと、アレイの現在のファームウェアを確認する方法について詳しくは、アレイ固有のマニュアルを参照してください。
ライブラリ	storops メモ: インストール時に、CloudPoint は必要なすべてのライブラリを自動的にインストールします。

Dell EMC Unity アレイでサポートされる CloudPoint 操作

CloudPoint は Dell EMC Unity アレイで次の管理操作を実行します。

表 5-6 Dell EMC Unity プラグインでの CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint はストレージグループとともにすべてのボリュームとそのスナップショットを検出します。 メモ: CloudPoint は、深さが 2 の資産のみを検出します。
スナップショットの作成	スナップショットを作成するために、CloudPoint は必要な情報とスナップショット名を使用して、ボリュームが存在するストレージグループで SDK メソッドをトリガします。 CloudPoint によって作成される一般的なスナップショットには、次の命名規則があります。 NB<unique_21digit_number>

CloudPoint 操作	説明
スナップショットの削除	スナップショットを削除するために、CloudPoint は必要なスナップショットの詳細を使用して SDK メソッドをトリガし、アレイでスナップショットが正常に削除されたことを確認します。
スナップショットのリストア	CloudPoint は、さまざまなリストアパスで SDK メソッドを活用してリストアする機能を提供します。
スナップショットのエクスポート	スナップショットのエクスポート操作がトリガされると、NFS の新しいエクスポートが同じファイルシステムパスに作成され、バックアップホストが読み取り専用アクセス権を持つクライアントとして追加されます。
スナップショットのデポート	スナップショットのデポート操作がトリガされると、スナップショットのパスに作成済みのエクスポートされたストレージグループ、その中のボリューム、およびソースとして使用される一時ストレージグループが CloudPoint によって削除されます。基本的に、スナップショットのエクスポート操作を元に戻します。

サポート対象の DELL EMC Unity アレイに対して、次の CloudPoint 操作も実行できます。

- すべてのディスクの一覧を出力します。
- LUN の COW (コピーオンライト) スナップショットを作成します。

メモ: スナップショット名には小文字または大文字を使用でき、任意の ASCII 文字と特殊文字を含められます。

- LUN の COW スナップショットを削除します。
- COW スナップショットを使用して LUN をリストアします。スナップショットは元のオブジェクトを上書きします。

メモ: 一貫性のあるグループに含まれる LUN のスナップショットは作成できません。この制限の理由は、単一の LUN スナップショットのリストアによって一貫性のあるグループ全体がリストアされるためです。

スナップショットのエクスポート関連の必要条件と制限事項

Dell EMC Unity アレイ環境には、次の必要条件と制限事項が適用されます。

- スナップショットをエクスポートするホストは、アレイに接続されている必要があります。

メモ: エクスポートされたスナップショットはホストに接続され、アレイによって割り当てられた WWN (ワールドワイドネーム) を使用してアクセスできます。

- スナップショットのエクスポートは、次のプロトコルを使用してサポートされます。
 - FC (ファイバーチャネル)
 - iSCSI (Internet Small Computer Systems Interface)
- スナップショットは複数回エクスポートできません。
- エクスポートされたスナップショットは削除できません。

Pure Storage FlashArray プラグインの構成に関する注意事項

Pure Storage FlashArray プラグインを構成するときは、次のパラメータを指定します。

表 5-7 Pure Storage FlashArray プラグインの構成パラメータ

CloudPoint の構成パラメータ	説明
IP アドレス	アレイの IP アドレス
ユーザー名	アレイにアクセスするために使用するユーザー名
パスワード	アレイにアクセスするために使用するパスワード

プラグインを構成する前に、指定したユーザーアカウントがアレイでスナップショットを作成、削除、およびリストアする権限を持っていることを確認します。

サポート対象の Pure Storage FlashArray モデル

CloudPoint を使用して、次の Pure Storage FlashArray モデルを検出して保護できます。

表 5-8 サポート対象の Pure Storage FlashArray モデル

カテゴリ	サポート対象
アレイモデル	FA-405

カテゴリ	サポート対象
ファームウェアのバージョン	■ ソフトウェア: Purity OS ■ Purity OS のバージョン: 5.1.4 ■ Rest バージョン: 1.11 ファームウェアのバージョンと、アレイの現在のファームウェアを確認する方法について詳しくは、アレイ固有のマニュアルを参照してください。

Pure Storage FlashArray モデルでサポートされている CloudPoint 操作

サポート対象の Pure Storage FlashArray モデルで次の CloudPoint 操作を実行できます。

- すべてのボリュームを検出して一覧表示します。
- ボリュームのクローンスナップショットを作成します。

メモ: スナップショット名は、「<Diskname> + <snapshotname>」で構成されます。スナップショットの接尾辞は、1 から 63 文字の長さで指定する必要があり、英数字にできます。スナップショット名の先頭と末尾は英字または数字である必要があります。接尾辞には、少なくとも 1 文字または「-」を含める必要があります。

- クローンのスナップショットを削除します。
- スナップショットから元のボリュームをリストアします。スナップショットは元のボリュームを上書きします。
- スナップショットをエクスポートします。
スナップショットのエクスポート操作がトリガされると、CloudPoint はスナップショットから新しいボリュームを作成し、FC (ファイバーチャネル) プロトコルを使用してターゲットホストに接続します。ターゲットホストには、エクスポートされたスナップショットボリュームに対する読み取り/書き込み権限が割り当てられます。
- スナップショットをデポートします。
スナップショットのデポート操作がトリガされると、CloudPoint はエクスポートされたスナップショットボリュームをターゲットホストから切断し、その後、そのボリュームを削除します。

スナップショットのエクスポート関連の必要条件と制限事項

次の必要条件と制限事項は、Pure Storage アレイ環境でのスナップショットのエクスポートとデポートの操作に適用されます。

- スナップショットは複数回エクスポートできません。
- エクスポートされたスナップショットは削除できません。

HPE RMC プラグインの構成に関する注意事項

HPE (Hewlett Packard Enterprise) RMC (Recovery Manager Central) 用の CloudPoint プラグインを使用すると、RMC でサポートされているすべての HPE ストレージシステムでディスクのスナップショットを作成、削除、リストアできます。プラグインは、クローンと COW (コピーオンライト) スナップショット形式をサポートします。

メモ: COW スナップショットはリストアできますが、クローンスナップショットはリストアできません。

p.119 の「[RMC プラグインの構成パラメータ](#)」を参照してください。

p.120 の「[サポート対象の HPE ストレージシステム](#)」を参照してください。

p.120 の「[HPE ストレージアレイでサポートされている CloudPoint 操作](#)」を参照してください。

RMC プラグインの構成パラメータ

CloudPoint プラグインを構成するには、次のパラメータが必要です。

表 5-9 RMC プラグインの構成パラメータ

CloudPoint の構成パラメータ	説明
IP アドレス	RMC サーバーの IP アドレス
ユーザー名	RMC 管理者ユーザーアカウント
パスワード	RMC 管理者ユーザーアカウントのパスワード

プラグインを構成する前に、CloudPoint に指定するユーザーアカウントに、RMC サーバーの管理者ロールが割り当てられていることを確認します。

サポート対象の HPE ストレージシステム

表 5-10 サポート対象の RMC バージョン

カテゴリ	サポート対象
RMC ソフトウェアのバージョン	■ 6.0 以降 ■ 6.2 以降 (HPE Nimble の場合)

表 5-11 サポート対象の RMC 管理下のストレージシステム

カテゴリ	サポート対象
アレイ	■ HPE 3PAR StoreServ ■ HPE Nimble Storage

HPE ストレージアレイでサポートされている CloudPoint 操作

CloudPoint では、HPE RMC によって管理されている資産に対して、次の操作をサポートします。

表 5-12 HPE RMC で管理される資産に対する CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint は、アレイ上で作成されたすべてのボリュームを検出します。ボリュームがマルチボリュームのボリュームセットの一部である場合、CloudPoint はボリュームセットをスキャンし、個々のボリューム情報を抽出して、ボリュームセットに含まれる一意のボリュームすべてのリストを作成します。 スナップショットの場合、CloudPoint はすべてのスナップショットセットをスキャンして、各スナップショットを元の親ボリュームにリンクします。

CloudPoint 操作	説明
スナップショットの作成	CloudPoint は、アレイ上のすべてのボリュームのスナップショットを取得します。 CloudPoint は、スナップショットを作成するときに、ボリューム全体の COW (コピーオンライト) スナップショットを内部的にトリガします。ボリュームがマルチボリュームのボリュームセットの一部である場合、CloudPoint はボリュームセット全体のスナップショットを取得し、スナップショットセットを作成します。スナップショットセットには、そのボリュームセットの一部であるすべてのボリュームのスナップショットが含まれています。ただし、CloudPoint は、スナップショット操作のために選択されたボリュームだけにそのスナップショットセットを関連付けます。ボリュームセットに追加のボリュームが含まれている場合でも、スナップショットセットは選択されたボリュームだけに関連付けられます。 たとえば、vol-1、vol-2、vol-3 という 3 つのボリュームを含むボリュームセットを想定します。vol-1 のスナップショットを作成するために CloudPoint を使用すると、CloudPoint はそのボリュームセット内のすべてのボリュームのスナップショットを含むスナップショットセットを作成します。しかし、他のボリューム vol-2、vol-3 に属する追加のスナップショットがスナップショットセットに含まれている場合でも、スナップショットセットは vol-1 (選択したボリューム) のスナップショットとしてマーク付けされます。
スナップショットの削除	CloudPoint は、スナップショットまたはスナップショットセットを削除します (親ボリュームがボリュームセットの一部である場合)。 CloudPoint を使用して削除できるのは、CloudPoint を使用して作成されたスナップショットのみです。RMC 環境に他のスナップショットが含まれている場合、CloudPoint はそれらのスナップショットを検出できますが、それらのスナップショットに対する削除操作は許可されません。
スナップショットのリストア	スナップショットをリストアするときに、CloudPoint は、選択したボリュームに対応する特定のスナップショットのみをリストアします。スナップショットセットは COW スナップショットで、ボリュームセット内の追加ボリュームに属する他のスナップショットを含めることができます。ただし、CloudPoint は、選択したボリュームのスナップショットのみをリストアします。その他のスナップショットは、リストア操作中には使用されません。 スナップショットリストアを開始する前に、親ボリュームがターゲットホストからマウント解除されていることを確認します。

CloudPoint 操作	説明
スナップショットのエクスポート	スナップショットのエクスポート操作がトリガされると、CloudPoint はスナップショットから新しいボリュームを作成し、その後、ターゲットホストに新しいボリュームを接続します。 選択したスナップショットがスナップショットセットの場合は、新しいボリュームを作成するときに、CloudPoint はスナップショットセットから新しいボリュームセットを作成します。新しいボリュームセットに複数のボリュームが含まれている場合でも、CloudPoint はエクスポート対象として選択されたスナップショットに対応するボリュームのみを接続します。その他のボリュームはエクスポート操作では使用されません。 エクスポート操作は、次のプロトコルを使用してサポートされます。 - FC (ファイバーチャネル) - iSCSI (Internet Small Computer Systems Interface)
スナップショットのデポート	スナップショットのデポート操作がトリガされると、CloudPoint はターゲットホストからボリュームを切断し、その後、そのボリュームを削除します。ボリュームがマルチボリュームのボリュームセットの一部である場合、ボリュームセット全体が切断されてホストから削除されます。

メモ: ボリュームセットのスナップショットの場合は、スナップショットボリューム名を形成するために使用される名前パターンを使用します。HPE のストレージ情報ライブラリから利用可能な HPE 3PAR コマンドラインインターフェースリファレンスの **VV** 名のパターンを参照してください。

HPE RMC プラグインの考慮事項および制限事項

HPE EMC プラグインを構成する際は、次の点を考慮します。

- CloudPoint を使用してスナップショットを削除するときに、CloudPoint によって管理されているスナップショットのみを削除できます。CloudPoint を使用して作成されていないスナップショットは、NetBackup を使用して削除できません。
- NetBackup 操作は、ディスクとボリュームでのみサポートされます。ボリュームがボリュームセットとしてグループ化されている場合でも、CloudPoint はボリュームセットの一部である個々のボリュームの形式でボリュームセットを検出して表示します。マルチボリュームのボリュームセットに属するボリュームのスナップショットを作成する場合、CloudPoint は、そのボリュームセット内のすべてのボリュームのスナップショットを含むスナップショットセットを作成します。そのため、スナップショット操作によって追加のスナップショットが作成されます。これらは、CloudPoint によって追跡されません。

ボリュームセットの保護に CloudPoint を使用する場合、Veritas は、ボリュームセットに 1 つのボリュームを構成することをお勧めします。

HPE XP プラグインの構成に関する注意事項

HPE XP (XP7 and XP8) 用の CloudPoint プラグインを使用して、NetBackup で HPE XP アレイの SAN ボリュームを検出し、それらに対してスナップショットの作成、エクスポート、デポート、削除、リストアの各操作をトリガできます。NetBackup プライマリサーバーでこのプラグインを構成する必要があります。

CloudPoint は、HPE XP Configuration Manager でホスティングされている REST API を使用して、HPE XP ストレージアレイと通信します。HPE XP Configuration Manager でセッションを作成して HPE XP ストレージアレイとの接続を確立し、REST API を使用して、バックアップする必要がある SAN ボリュームとそのスナップショットを検出します。

p.119 の「[RMC プラグインの構成パラメータ](#)」を参照してください。

p.120 の「[サポート対象の HPE ストレージシステム](#)」を参照してください。

p.120 の「[HPE ストレージアレイでサポートされている CloudPoint 操作](#)」を参照してください。

HPE XP プラグインの構成パラメータ

プラグインを構成する前に、スナップショットを格納するためのストレージアレイで flexsnap_pool という接頭辞が付く名前のプールを作成してください。

HPE XP アレイに関する次の情報を収集します。プラグインを構成するときに、これらの情報を使用する必要があります。

表 5-13 HPE XP プラグインの構成パラメータ

CloudPoint の構成パラメータ	説明
HPE XP Configuration Manager サーバーの IP	使用するストレージアレイで構成される HPE XP Configuration Manager REST サーバーの IP
HPE XP Configuration Manager サーバーのポート	HPE XP Configuration Manager REST サーバーがホスティングされているポート
アレイのユーザー名	スナップショット操作の権限を持つ HPE XP ストレージアレイのユーザーアカウント
アレイパスワード	アレイのユーザー名に関連付けられているパスワード
アレイストレージデバイス ID	HPE XP Configuration Manager にすでに登録されているアレイのストレージデバイス ID

NetBackup 管理コンソールを使用してプラグインを構成すると、次の画面が表示されます。

Configure Plugin

CloudPoint Server:

Selected Plugin: HPE XP Storage Array

Credentials

Enter Plugin ID:

HPE XP Configuration Manager Server IP:

HPE XP Configuration Manager Server Port:

Array Username:

Array Password:

Array storage Device Id:

OK

Cancel

Help

HPE XP プラグインの考慮事項および制限事項

- CloudPoint はスナップショットの作成時にスナップショットグループを使用し、1 つのアレイに対する CloudPoint のスナップショットの最大数は 8192 です。
- 作成したプールには、すべてのスナップショットのニーズに対応できる十分なサイズが必要です。

HPE XP ストレージアレイでサポートされている CloudPoint 操作

CloudPoint は HPE XP ストレージアレイで次の管理操作を実行します。

表 5-14 HPE XP で管理される資産に対する CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint は、ストレージアレイで作成された論理デバイス (LDEV) と、flexsnap_snap_group に類似した名前のスナップショットグループ内のスナップショットおよびそのメタデータの一部を検出します。 属性に「CMD」が含まれている LDEV と、論理ユニット番号 (LUN) がマッピングされていない LDEV は検出されません。

CloudPoint 操作	説明
スナップショットの作成	スナップショットの場合、CloudPoint は HPE XP Fast Snap ペアを使用して、必要な情報とスナップショット名を指定して一連の REST API 要求をトリガします。API によって、スナップショットの詳細が戻されます。 CloudPoint によって作成される一般的なスナップショットの命名規則は NB<unique_21digit_number> です。
スナップショットの削除	スナップショットを削除するために、CloudPoint は必要なスナップショットの詳細を使用して REST API 要求をトリガし、クラスターでスナップショットが正常に削除されたことを確認します。
スナップショットのリストア	スナップショットをリストアするために、CloudPoint は Fast Snap が親ボリュームにリストアされる REST API 要求をトリガします。
スナップショットのエクスポート	CloudPoint では、iSCSI および FC を使用したエクスポートがサポートされています。Cloudpoint は REST API を使用して、スナップショットの LUN パスを設定します。
スナップショットのデポート	スナップショットのデポート操作がトリガされると、CloudPoint はエクスポート操作時にスナップショットパスに作成されたエクスポートを削除します。基本的に、エクスポート操作を元に戻します。

Hitachi プラグインの構成に関する注意事項

Hitachi 用 CloudPoint プラグインを使用すると、HCM (Hitachi Configuration Manager) に登録されているサポート対象の Hitachi ストレージレイのストレージスナップショットを作成、削除、エクスポート、デポート、リストアできます。プラグインは、COW (コピーオンライト) スナップショット形式をサポートします。

Hitachi プラグイン構成の前提条件

Hitachi プラグインを構成する前に、ストレージシステムで次の手順を実行します。

- Hitachi ストレージレイに flexsnap_pool という名前のプールを作成していることを確認します。これは、CloudPoint プラグインを動作させるために必要です。
- ストレージレイ上に flexsnap_default_group という名前のスナップショットグループを作成します。

メモ: これは前提条件ではありません。このスナップショットグループを作成しないと、プラグインは構成中にこのグループを自動的に作成します。

- Hitachi ストレージアレイが HCM (Hitachi Configuration Manager) に登録されていることを確認します。CloudPoint は HCM REST API を使用して、ストレージアレイと通信します。
- Hitachi ストレージアレイにスナップショット操作を実行するために必要なライセンスがあることを確認します。
- CloudPoint に提供するユーザーアカウントには、ストレージアレイのスナップショットを作成、削除、エクスポート、デポート、およびリストアするためのアクセス権とともに、一般的な読み取り権限が付与されていることを確認します。

p.126 の「[Hitachi プラグインの構成パラメータ](#)」を参照してください。

p.126 の「[サポート対象の Hitachi ストレージアレイ](#)」を参照してください。

p.127 の「[Hitachi アレイでサポートされる CloudPoint 操作](#)」を参照してください。

Hitachi プラグインの構成パラメータ

CloudPoint Hitachi アレイプラグインを構成するには、次のパラメータが必要です。

表 5-15 Hitachi プラグインの構成パラメータ

CloudPoint の構成パラメータ	説明
Hitachi Configuration Manager サーバーの URL	HCM (Hitachi Configuration Manager) サーバーにアクセスするためのベース URL。 URL の形式は次のとおりです。 <code>protocol://host-name:port-number/ConfigurationManager</code>
アレイの IP アドレス	Hitachi ストレージアレイの IP アドレス。
アレイのユーザー名	Hitachi ストレージアレイへのアクセス権を持つユーザーアカウントの名前。 一般的な読み取り権限のほかに、ユーザーアカウントには、ストレージアレイのスナップショットを作成、削除、エクスポート、デポート、およびリストアするためのアクセス権が必要です。
アレイパスワード	Hitachi ストレージアレイへのアクセスに使用するユーザーアカウントのパスワード。

サポート対象の Hitachi ストレージアレイ

CloudPoint を使用して、次の Hitachi G シリーズアレイモデルを検出して保護できます。

表 5-16 サポート対象の Hitachi アレイ

カテゴリ	サポート対象
アレイモデル	VSP G1000 VSP G1500
ファームウェアのバージョン	80-01-21-XX/XX 以降
必要な SDK (ソフトウェア開発キット)	HCM (Hitachi Configuration Manager)

ハードウェアサポートの最新の情報については、CloudPoint ハードウェア互換性リスト (HCL) を参照してください。

p.17 の「[システム要件への準拠](#)」を参照してください。

Hitachi アレイでサポートされる CloudPoint 操作

HCM (Hitachi Configuration Manager) に登録されている、サポート対象の Hitachi ストレージアレイに対して次の CloudPoint 操作を実行できます。

表 5-17 Hitachi アレイでサポートされる CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint はストレージアレイで作成されたすべての LDEV (論理デバイス) を検出します。プライマリ LDEV オブジェクトは、ディスク資産として表示されます。TI (シンイメージ) ペアの一部であるセカンダリ LDEV オブジェクトは、スナップショットの下に表示されます。 1 つ以上の LDEV オブジェクトは、プールと呼ばれる論理エンティティにグループ化されます。CloudPoint Hitachi プラグインが機能するためには、ストレージアレイに flexsnap_pool という名前のプールを作成する必要があります。

CloudPoint 操作	説明
スナップショットの作成	NetBackup は、ホストグループに接続されているすべての LDEV オブジェクトのスナップショットを取得します。 CloudPoint は、スナップショットを取得するときに次の処理を実行します。 ■ 元の (基本) LDEV と同じサイズの新しい LDEV オブジェクトを作成します。 ■ 基本 LDEV と新しい LDEV を TI (シンイメージ) ペアに配置します。基本 LDEV はプライマリ LDEV で、新しい LDEV はセカンダリ LDEV です。 ■ TI ペアを分割して基本 LDEV の特定時点のスナップショットを作成し、次にスナップショット LUN パスを更新してセカンダリ LDEV を指すようにします。 ■ 基本 LDEV が接続されているのと同じホストグループにスナップショットを接続します。
スナップショットの削除	CloudPoint は、スナップショットを削除すると次の処理を実行します。 ■ スナップショットを削除します。 ■ スナップショットに関連付けられているセカンダリ LDEV への LUN パスを削除します。 ■ セカンダリシン LDEV を削除します。
スナップショットのリストア	CloudPoint は、LDEV のシンイメージスナップショットでリストア操作を実行します。プライマリ LDEV のすべてのデータは、セカンダリ LDEV のデータによって上書きされます。
スナップショットのエクスポート	スナップショットのエクスポート操作がトリガされると、CloudPoint は、エクスポート要求で指定された WWN (ワールドワイドネーム) または IQN (iSCSI 修飾名) に基づいてターゲットホストを検索します。ホストがストレージアレイで識別された後、CloudPoint は、スナップショットをエクスポートするターゲットホストでセカンダリ LDEV のパス属性を更新します。ターゲットホストがセカンダリ LDEV ホストポートに追加されると、エクスポートされたスナップショットがターゲットホストにすぐに表示されます。
スナップショットのデポート	スナップショットのデポート操作がトリガされると、CloudPoint はターゲットホストをセカンダリ LDEV パス属性から削除します。ターゲットホストエントリがセカンダリ LDEV ホストポートから削除されると、エクスポートされたスナップショットはターゲットホストに表示されなくなり、デポート操作は完了します。

スナップショット関連の必要条件と制限事項

Hitachi プラグインを構成する際は、次の点を考慮します。

- CloudPoint を使用してスナップショットを削除するときに、CloudPoint によって管理されているスナップショットのみを削除できます。CloudPoint を使用して作成されていないスナップショットは、CloudPoint を使用して削除できません。
- エクスポート操作は、次のプロトコルを使用してサポートされます。
 - FC (ファイバーチャネル)
 - iSCSI (Internet Small Computer Systems Interface)

Hitachi (HDS VSP 5000) プラグインの構成に関する注意事項

Hitachi (HDS VSP 5000) 用の CloudPoint プラグインを使用して、Hitachi HDS VSP 5000 で SAN ボリュームを検出し、それらのエクスポートに対してスナップショットの作成、エクスポート、デポート、削除、リストアの各操作をトリガできます。NetBackup プライマリサーバーでこのプラグインを構成する必要があります。

CloudPoint は、Hitachi Configuration Manager でホスティングされている REST API SDK を使用して、Hitachi ストレージアレイと通信します。CloudPoint は Hitachi Configuration Manager でセッションを作成して Hitachi ストレージアレイとの接続を確立し、REST API を使用して、バックアップする必要がある SAN ボリュームとそのスナップショットを検出します。

Hitachi (HDS VSP 5000) プラグインの構成パラメータ

- スナップショットを保存するため、1 つの HTI (Hitachi Thin Image) プールを作成し、その名前に接頭辞 `flexsnap_pool` を付けます。
- Hitachi (HDS VSP 5000) に関する次の情報を収集します。プラグインを構成するときに、これらの情報を使用します。

表 5-18 Hitachi (HDS VSP 5000) プラグインの構成パラメータ

CloudPoint の構成パラメータ	説明
Hitachi Configuration Manager サーバーの IP	使用するストレージアレイで構成される Hitachi Configuration Manager REST サーバーの IP。
Hitachi Configuration Manager サーバーのポート	Hitachi Configuration Manager REST サーバーがホスティングされているポート。

CloudPoint の構成パラメータ	説明
アレイのユーザー名	Hitachi ストレージアレイへのアクセス権を持つユーザーアカウントの名前。 一般的な読み取り権限のほかに、ユーザーアカウントには、ストレージアレイのスナップショットを作成、削除、エクスポート、デポート、およびリストアするためのアクセス権が必要です。
アレイパスワード	Hitachi ストレージアレイへのアクセスに使用するユーザーアカウントのパスワード。
アレイストレージデバイス ID	Hitachi Configuration Manager にすでに登録されているストレージアレイデバイスの ID。

NetBackup 管理コンソールを使用してプラグインを構成すると、次の画面が表示されます。

Configure Plugin

CloudPoint Server:

Selected Plugin: Hitachi Storage Array

Credentials

Enter Plugin ID:

Hitachi Configuration Manager Server IP:

Hitachi Configuration Manager Server Port:

Array Username:

Array Password:

Array storage Device Id:

OK

Cancel

Help

Hitachi (HDS VSP 5000) プラグインの考慮事項および制限事項

- CloudPoint はスナップショットの作成時にスナップショットグループを使用し、1 つのアレイに対する CloudPoint のスナップショットの最大数は 8192 です。
- シンイメージプールには、すべてのスナップショットのニーズに対応できる十分な大きさが必要です。

Hitachi (HDS VSP 5000) アレイでサポートされる CloudPoint 操作

CloudPoint は Hitachi (HDS VSP 5000) ストレージアレイで次の管理操作を実行します。

表 5-19 Hitachi (HDS VSP 5000) アレイでサポートされる CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint は、ストレージアレイで作成された論理デバイス (LDEV) と、flexsnap_snap_group に類似した名前のスナップショットグループ内のスナップショットおよびそのメタデータの一部を検出します。 属性に「CMD」が含まれている LDEV と、論理ユニット番号 (LUN) がマッピングされていない LDEV は検出されません。
スナップショットの作成	スナップショットの場合、CloudPoint は Hitachi シンイメージペアを使用して、必要な情報とスナップショット名を指定して一連の REST API 要求をトリガします。API によって、スナップショットの詳細が戻されます。 CloudPoint によって作成される一般的なスナップショットには、次の命名規則があります。 NB<unique_21digit_number>
スナップショットの削除	スナップショットを削除するために、CloudPoint は必要なスナップショットの詳細を使用して REST API 要求をトリガし、クラスターでスナップショットが正常に削除されたことを確認します。
スナップショットのリストア	スナップショットをリストアするために、CloudPoint はシンイメージが親ボリュームにリストアされる REST API 要求をトリガします。
スナップショットのエクスポート	CloudPoint では、iSCSI および FC を使用したエクスポートがサポートされています。Cloudpoint は REST API を使用して、スナップショットの LUN パスを設定します。
スナップショットのデポート	スナップショットのデポート操作がトリガされると、CloudPoint はエクスポート操作時にスナップショットパスに作成されたエクスポートを削除します。基本的に、エクスポート操作を元に戻します。

InfiniBox プラグインの構成に関する注意事項

InfiniBox 用の CloudPoint プラグインを使用すると、INFINIDAT InfiniBox ストレージアレイのストレージプールの一部である SAN ボリューム (仮想ディスク) のスナップショットを作成、削除、リストア、エクスポート、およびデポートできます。

CloudPoint は、InfiniSDK と互換性があるすべての InfiniBox ストレージアレイをサポートします。

InfiniBox プラグイン構成の前提条件

InfiniBox プラグインを構成する前に、ストレージシステムで次の手順を実行します。

- InfiniBox ストレージアレイにスナップショット操作を実行するために必要なライセンスがあることを確認します。
- CloudPoint に提供するユーザーアカウントに、CloudPoint を使用して保護するすべてのストレージプールに対する管理者権限があることを確認します。

p.132 の「[InfiniBox プラグインの構成パラメータ](#)」を参照してください。

p.132 の「[InfiniBox アレイでサポートされる CloudPoint 操作](#)」を参照してください。

InfiniBox プラグインの構成パラメータ

CloudPoint InfiniBox アレイプラグインを構成するには、次のパラメータが必要です。

表 5-20 InfiniBox プラグインの構成パラメータ

CloudPoint の構成パラメータ	説明
InfiniBox システムの IP アドレス	InfiniBox ストレージアレイの IP アドレス。
ユーザー名	InfiniBox ストレージアレイへのアクセス権を持つユーザーアカウントの名前。 ユーザーアカウントには、アレイのストレージプールに対する管理者権限 (POOL_ADMIN ロール) が必要です。
パスワード	InfiniBox ストレージアレイへのアクセスに使用するユーザーアカウントのパスワード。

InfiniBox アレイでサポートされる CloudPoint 操作

CloudPoint は、InfiniBox ストレージアレイに対して次の操作をサポートします。

表 5-21 InfiniBox アレイでサポートされる CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint は、InfiniBox ストレージアレイで作成されるストレージプールの一部であるすべての SAN ボリューム (仮想ディスク) を検出します。プラグインは、タイプが PRIMARY に設定されているすべてのボリュームのリストを返すように、アレイに要求を送信します。このようなボリュームはベースボリュームと見なされ、ディスク資産として表示されます。 スナップショットオブジェクトを検出するために、プラグインは、タイプが SNAPSHOT として設定されていて、深度の属性が 1 に設定されているすべてのボリュームのリストを返すように、アレイに要求を送信します。このようなボリュームはスナップショットと見なされます。 InfiniBox アレイは、スナップショットのスナップショットの作成をサポートします。深度の属性は、スナップショットの種類を識別します。スナップショットの深度値が 1 より大きい場合は、それが既存のスナップショットのスナップショットであることを示します。 CloudPoint では、1 以外の深度値を持つスナップショットボリュームの検出と操作をサポートしません。
スナップショットの作成	CloudPoint は、ストレージプールの一部であるすべての SAN ボリュームのスナップショットを取得します。スナップショットが作成されると、CloudPoint プラグインは InfiniSDK を使用して、選択したボリュームで create_snapshot 方式の要求を送信し、スナップショット名をその要求の引数として渡します。 InfiniBox アレイは、スナップショットボリュームを作成し、そのタイプを SNAPSHOT として設定し、深度属性の値を 1 に設定して、その情報を CloudPoint に返します。
スナップショットの削除	スナップショットが削除されると、CloudPoint プラグインは、スナップショットに関連付けられた親ボリュームで delete_snapshot 方式の要求を送信し、スナップショットボリューム名をその要求の引数として渡します。InfiniBox アレイは、親ボリュームに関連付けられている指定されたスナップショットを削除します。
スナップショットのリストア	スナップショットのリストア操作がトリガされると、CloudPoint は、最初に、リストアされているスナップショットに関連付けられている親ボリュームについての詳細を取得します。CloudPoint プラグインは、次に、親ボリュームで restore_snapshot 方式の要求を送信し、選択したスナップショットをその要求の引数として渡します。 アレイは、選択したスナップショットを使用して、親ボリュームでリストアを実行します。親ボリュームのすべてのデータは、スナップショットボリュームのデータによって上書きされます。

CloudPoint 操作	説明
スナップショットのエクスポート	スナップショットのエクスポート操作がトリガされると、CloudPoint は、エクスポート要求で指定された WWN (ワールドワイドネーム) または IQN (iSCSI 修飾名) に基づいてターゲットホストを検索します。ホストが識別されると、CloudPoint プラグインは、ターゲットホストで map_volume 方式の要求を送信し、選択したスナップショット ID をその要求の引数として渡します。 InfiniBox アレイは、リストア要求に対する応答として LUN ID を返します。CloudPoint は、LUN ID とターゲットホスト ID のマッピング情報を CloudPoint データベース内に内部的に格納します。エクスポート操作では、disk:snapshot:export というタイプの新しい仮想資産も作成されて、CloudPoint データベースに保存されます。
スナップショットのデポート	スナップショットのデポート操作がトリガされると、CloudPoint は、最初にデータベースからターゲットホスト ID を取得します。CloudPoint プラグインは、次に、ターゲットホストで unmap_volume 方式の要求を送信し、選択したスナップショット ID をその要求の引数として渡します。InfiniBox アレイは、指定されたターゲットホストからスナップショットボリュームマッピングを削除します。

InfiniBox プラグインとスナップショット関連の必要条件と制限事項

InfiniBox プラグインを構成するときは、次の点を考慮します。

- InfiniBox プラグインは、深度属性の値が 1 に設定されている volume snapshot のみの、検出操作とスナップショット操作をサポートします。1 以外の深度属性値がある volume snapshot はサポートされません。
- InfiniBox アレイ上のすべての親ボリュームオブジェクトとスナップショットオブジェクトは一意です。ボリュームのスナップショットを作成するときに、同じ名前のオブジェクトがアレイにすでに存在する場合、作成操作は失敗します。スナップショット名が一意であることを確認する必要があります。
- CloudPoint を使用してスナップショットを削除するときに、CloudPoint によって管理されているスナップショットのみを削除できます。CloudPoint を使用して作成されていないスナップショットは、CloudPoint を使用して削除できません。
- スナップショットのエクスポート操作は、次のプロトコルを使用してサポートされます。
 - FC (ファイバーチャネル)
 - iSCSI (Internet Small Computer Systems Interface)

Dell EMC PowerScale (Isilon) プラグインの構成に関する注意事項

Veritas NetBackup は、ネットワーク接続ストレージ (NAS) ストレージホストに設定される共有に、堅ろうなデータ保護ソリューションを提供します。NetBackup は、NAS サポートを拡張し、Dell EMC PowerScale (Isilon) 環境でホストされている NFS のエクスポートを保護できるようにします。NFS (Network File System) のエクスポートで検出を行い、その後バックアップおよびリストア操作を行うように CloudPoint を設定できます。

Dell EMC PowerScale 用の CloudPoint プラグインには、NetBackup が PowerScale (Isilon) で NFS のエクスポートを検出し、それらのエクスポートに対してスナップショットの作成、エクスポート、デポート、スナップショットの差分 (変更リスト)、削除の各操作のトリガを可能にする、必要な関数ロジックが含まれています。NetBackup プライマリサーバーでこのプラグインを構成する必要があります。

CloudPoint は、PowerScale (Isilon) (isilon_sdk_python) によって提供される REST API SDK を使用して、PowerScale (Isilon) NFS のエクスポートとスナップショットと通信します。CloudPoint は、自身をバックアップアプリケーションとして登録して PowerScale (Isilon) との接続を確立し、API エンドポイントを使用して、バックアップの作成が必要な NFS のエクスポートとそのスナップショットを検出します。

Dell EMC PowerScale (Isilon) プラグインの構成の前提条件

プラグインを構成する前に、次の操作を実行します。

- Dell EMC PowerScale (Isilon) の OneFS バージョンがサポートされていることを確認します。
CloudPoint のサポート対象は次のとおりです。
 - OneFS バージョン 8.0 以降
 - ベンダー変更追跡を使用する場合は、OneFS バージョン 8.2.1 以降
- Dell EMC PowerScale (Isilon) に関する次の情報を収集します。PowerScale プラグインを構成するときに、これらの情報を使用します。

パラメータ	説明
クラスタアドレス (Cluster Address)	Isilon クラスタは 3 つ以上のハードウェアノードで構成されます。 ノードの管理 IP アドレスまたは完全修飾ドメイン名 (FQDN) を追加できます。
ユーザー名 (Username)	PowerScale クラスタでスナップショット操作を実行する権限を持つユーザーアカウント。

表 5-22 Dell EMC PowerScale (Isilon) プラグインでの CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint は、すべての NFS のエクスポートとそのスナップショット、およびその一部のメタデータを検出します。 メモ: CloudPoint は、深さが 2 の資産のみを検出します。 たとえば、NFS のエクスポートの資産が <code>["/ifs", "/ifs/test_fs1", "/ifs/test_fs2", "/ifs/test_fs1/test_data", "/ifs/smb_03/test_data/dir01"]</code> の場合、クラウドポイントで検出される NFS のエクスポートは <code>["/ifs/test_fs1", "/ifs/test_fs2"]</code> です。
スナップショットの作成	スナップショットを作成するために、CloudPoint は必要な情報とスナップショット名を使用して、<code>nfs_export</code> で POST REST API 呼び出しをトリガします。API によって、スナップショットの詳細が戻されます。 CloudPoint によって作成される一般的なスナップショットには、次の命名規則があります。 <code>NB<unique_21digit_number></code>
スナップショットの削除	スナップショットを削除するために、CloudPoint は必要なスナップショットの詳細を使用して <code>DELETE REST API</code> 呼び出しをトリガし、クラスターでスナップショットが正常に削除されたことを確認します。
スナップショットのリストア	CloudPoint は、JobAPI を使用してスナップショットを元に戻します。 ディレクトリを含むスナップショットを元に戻すには、ディレクトリ用に <code>SnapRevert</code> ドメインを作成することをお勧めします。 スナップショットを元に戻すには、次の手順を実行します。 1 ディレクトリ用に <code>SnapRevert</code> ドメインを作成します。 2 スナップショットの復元ジョブを作成します。
スナップショットのエクスポート	スナップショットのエクスポート処理がトリガされると、新しい NFS のエクスポートがスナップショットパス (<code>/ifs/test_fs/.snapshot/NB15985918570166499611/</code>) に作成され、バックアップホストが読み取り専用アクセス権を持つルートクライアントとして追加されます。
スナップショットのデポート	スナップショットのデポート処理がトリガされると、CloudPoint はエクスポート操作時にスナップショットパスに作成された NFS のエクスポートを削除します。

CloudPoint 操作	説明
スナップショットの差分の作成	CloudPoint は、JobAPI を使用してスナップショット間の変更リストを作成します。変更リストを作成するには、次の手順を実行します。 1 JobAPI を使用して、スナップショット間の変更リストを作成するジョブを作成します。 2 <code>get_changelist_entries</code> API を使用して、スナップショット間の変更リストのエントリをフェッチします。 メモ: 以下に重要な点を挙げます。 ■ <code>get_changelist_entries</code> API は、OneFS バージョン 8.2.1 以降でのみ利用できます。 ■ 変更リストの作成には、JobAPI を使用します。ジョブエンジンでは、3 種類のジョブのみを同時に実行できます。変更リストの複数のインスタンスを許可するには、次の CLI を実行します。 ■ <code>isi_gconfig -t job-config jobs.types.changelistcreate.allow_multiple_instances=true'</code> (デフォルトは <code>false</code>) ■ <code>isi_gconfig -t job-config jobs.types.changelistcreate.allow_multiple_instances'</code>

Dell EMC PowerMax および VMax プラグインの構成に関する注意事項

Dell EMC PowerMax および VMax 用の CloudPoint プラグインを使用すると、NetBackup は PowerMax または VMax にマウントされている SAN ボリュームを検出し、それらのボリュームに対してスナップショットの作成、エクスポート、デポート、リストア、削除の各操作をトリガできます。NetBackup プライマリサーバーでこのプラグインを構成する必要があります。

CloudPoint は、PowerMax/VMax (PyU4V) が提供する REST API SDK を使用して、PowerMax/VMax 資産と通信します。CloudPoint は、自身をバックアップアプリケーションとして登録して PowerMax/VMax アレイとの接続を確立し、API エンドポイントを使用して、バックアップの作成が必要な SAN ボリュームとそのスナップショットを検出します。

Dell EMC PowerMax および VMax プラグインの構成の前提条件

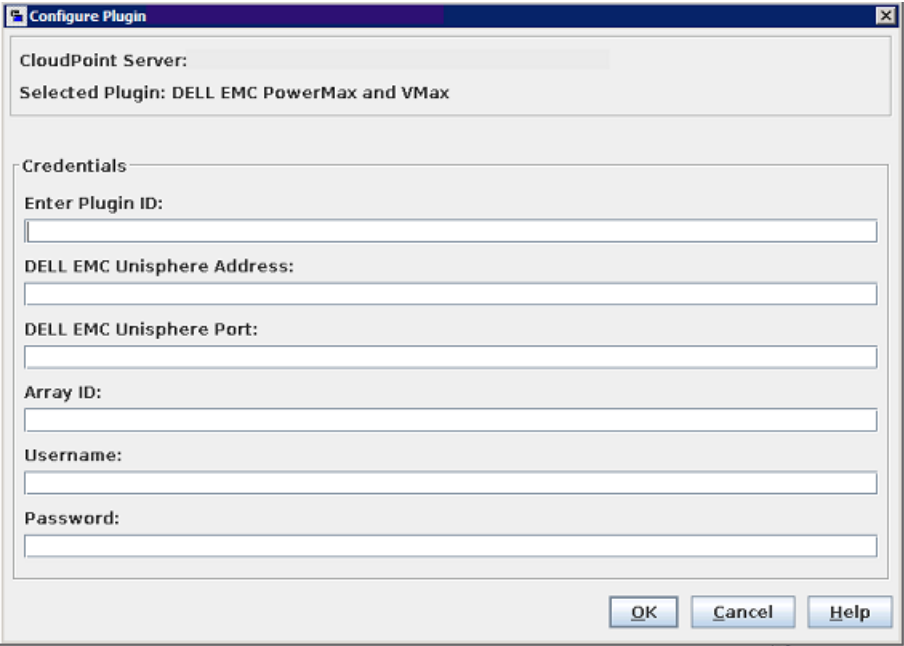
プラグインを構成する前に:

- 次の点に注意してください。

- 必要な Unisphere の最小バージョンは、Unisphere Management Console 9.2.0.1 です。
- サポート対象のアレイモデルは、PowerMax、VMAX-3、VMAX-AFA です。
- PowerMax OS、HyperMax OS で「SnapSet Id」をサポートするには、アレイの uCode が 5978.669.669 より大きい必要があります。
- Dell EMC PowerMax/VMax に関する次の情報を収集します。プラグインを構成するときに、これらの情報を使用します。

パラメータ	説明
Unisphere アドレス	すべてのアレイの管理に使用する Unisphere Management Console。 Unisphere Management Console の管理 IP アドレスまたは完全修飾ドメイン名 (FQDN) を追加できます。
Unisphere ポート	コンソールへのアクセスに使用される Unisphere 管理ポート (Dell EMC 社は 8443 を推奨)。 Unisphere コンソールにアクセスできる任意のポートを構成できます。
アレイ ID	保護対象となる 12 桁の一意のアレイ ID。
ユーザー名	PowerMax/VMax アレイでスナップショット操作を実行する権限を持つ Unisphere コンソールのユーザーアカウント。
パスワード	前の手順で指定した Unisphere ユーザーアカウントのパスワード。

NetBackup 管理コンソールを使用してプラグインを構成すると、次の画面が表示されます。



Dell EMC PowerMax および VMax のサポート対象の CloudPoint 操作

CloudPoint は Dell EMC PowerMax および VMax アレイで次の管理操作を実行します。

表 5-23 Dell EMC PowerMax/VMax プラグインでの CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint はストレージグループとともにすべてのボリュームとそのスナップショットを検出します。 メモ: CloudPoint は、深さが 2 の資産のみを検出します。
スナップショットの作成	スナップショットを作成するために、CloudPoint は必要な情報とスナップショット名を使用して、ボリュームが存在するストレージグループで POST API 呼び出しをトリガします。 CloudPoint によって作成される一般的なスナップショットには、次の命名規則があります。 NB<unique_21digit_number>

CloudPoint 操作	説明
スナップショットの削除	スナップショットを削除するために、CloudPoint は必要なスナップショットの詳細を使用して DELETE REST API 呼び出しをトリガし、アレイでスナップショットが正常に削除されたことを確認します。
スナップショットのリストア	CloudPoint は、ストレージグループのスナップショットリストアを行う Unisphere の API を使用します。 ボリューム上の指定した時点のイメージにスナップショットをリストアするには 1 空の一時ストレージグループを作成します。 2 そのストレージグループにリストアされるボリュームを追加します。 3 一時ストレージグループをリストアします。 4 一時ストレージグループを削除します。
スナップショットのエクスポート	スナップショットのエクスポート操作がトリガされると、ボリュームはスナップショットから切り出され、エクスポートされるホストに接続されます。 次の手順を実行します。 1 エクスポートを実行するイニシエータをフェッチします。 2 空の一時ストレージグループを作成します。 3 スナップショットをストレージグループにエクスポートするソースボリュームを追加します。 4 ここで、一時ストレージをソースストレージグループと見なして、スナップショットからエクスポートストレージグループを作成し、エクスポートされたストレージグループにスナップショットをリンクします。 5 ホスト ID とポートグループ ID をフェッチします。 6 エクスポートストレージグループ、ホスト ID、ポートグループ ID を使用し、エクスポートされたストレージグループをホストに接続するマスク表示グループを作成します。
スナップショットのデポート	スナップショットのデポート操作がトリガされると、エクスポートされたストレージグループ、その中のボリューム、ソースとして使用される一時ストレージグループが CloudPoint によって削除されます。基本的に、スナップショットのエクスポート操作を元に戻します。

Qumulo プラグインの構成に関する注意事項

NetBackup は、ネットワーク接続ストレージ (NAS) ストレージホストに設定される共有に、堅ろうなデータ保護ソリューションを提供します。NetBackup は、この NAS サポートを拡張し、Qumulo 環境でホストされている NFS のエクスポートを保護できるようにします。

NFS (Network File System) のエクスポートで検出を行い、その後バックアップ操作とリストア操作を実行するように CloudPoint を設定できます。

Qumulo 用の CloudPoint プラグインには、NetBackup が Qumulo クラスタで NFS のエクスポートを検出し、それらのエクスポートに対してスナップショットの作成、エクスポート、デポート、削除の各操作のトリガを可能にする、必要な関数ロジックが含まれています。NetBackup プライマリサーバーでこのプラグインを構成する必要があります。

CloudPoint は、REST API SDK Qumulo (qumulo-api) を使用して Qumulo 資産と通信します。CloudPoint は、SDK によって公開された RestClient ライブラリを使用して Qumulo との接続を確立し、SDK メソッドを使用して、バックアップの作成が必要な NFS のエクスポートとそのスナップショットを検出します。

Qumulo プラグインの構成の前提条件

プラグインを構成する前に、次の操作を実行します。

- Qumulo Core バージョンがサポートされていることを確認します。
CloudPoint はバージョン 3.0.5 以降をサポートします。
- Qumulo クラスタに関する次の情報を収集します。プラグインを設定するときに、これらの情報を使用します。

パラメータ	説明
クラスタアドレス (Cluster Address)	ノードの管理 IP アドレスまたは完全修飾ドメイン名 (FQDN) を追加できます。Qumulo DNS ラウンドロビンの FQDN も使用できます。
ユーザー名 (Username)	Qumulo クラスタでスナップショット操作を実行する権限を持つユーザーアカウント。
パスワード (Password)	前の手順で指定した Qumulo ユーザーアカウントのパスワード。

NetBackup 管理コンソールを使用してプラグインを構成すると、次の画面が表示されます。

Configure Plugin [redacted] eritas.com

CloudPoint Server: [redacted] india.veritas.com

Selected Plugin: Qumulo

Credentials

Enter Plugin ID:

Qumulo Cluster FQDN/ IP address:

Username:

Password:

OK Cancel Help

Qumulo プラグインの考慮事項および制限事項

次の考慮事項と制限事項が適用されます。

- スナップショット操作は、Qumulo ファイルサーバーのネストした共有ではサポートされません。ネストした共有とは、その共有自体が、既存のファイル共有のサブディレクトリであるものです。NetBackup は、このようなネストした共有のスナップショットの作成をサポートしません。
- Qumulo ファイルサーバーは、スナップショットを使用した共有の指定した時点 (PIT) へのロールバックリストアをサポートしません。NetBackup を利用して共有のデータをリストアできます。
- NFSv4 は、Qumulo プラグインではサポートされません。NetBackup では、NAS ポリシーで明示的なオプションを使用して、バックアップジョブに NFS マウントバージョン NFSv3 と NFSv4 を設定できますが、NAS ポリシーにはデフォルトで NFSv3 が設定されています。

Qumulo プラグインのサポート対象の CloudPoint 操作

CloudPoint は、Qumulo プラグインで次の管理操作を実行します。

表 5-24 Qumulo プラグインでの CloudPoint 操作

CloudPoint 操作	説明
資産の検出	CloudPoint は、すべての Qumulo とファイルシステムそのスナップショット、およびその一部のメタデータを検出します。深さ 1 の検出がサポートされます。 たとえば、ファイルシステムディレクトリが [/home, /home/user1, /home/user2, /user1] の場合、検出されるファイルシステムは [/home,/user1] です。
スナップショットの作成	スナップショットを作成するために、CloudPoint は必要な情報とスナップショット名を使用して、SDK メソッドをトリガします。API によって、スナップショットの詳細が戻されます。 CloudPoint によって作成される一般的なスナップショットには、次の命名規則があります。 NB<unique_21digit_number>
スナップショットの削除	スナップショットを削除するために、CloudPoint は必要なスナップショットの詳細を使用して、SDK メソッドをトリガします。次に、CloudPoint はクラスタでスナップショットが正常に削除されたことを確認します。
スナップショットのリストア	CloudPoint では、この操作はサポートされていません。
スナップショットのエクスポート	スナップショットのエクスポート操作がトリガされると、NFS の新しいエクスポートが同じファイルシステムパスに作成され、バックアップホストが読み取り専用アクセス権を持つルートクライアントとして追加されます。
スナップショットのデポート	スナップショットのデポート処理がトリガされると、CloudPoint はエクスポート操作時にスナップショットパスに作成された NFS のエクスポートを削除します。
スナップショットの差分の作成	CloudPoint では、この操作はサポートされていません。

CloudPoint アプリケーションエージェントとプラグイン

この章では以下の項目について説明しています。

- [Microsoft SQL プラグインの構成に関する注意事項](#)
- [Oracle プラグインの構成に関する注意事項](#)
- [MongoDB プラグインの構成に関する注意事項](#)
- [インストールと構成の処理について](#)
- [Linux ベースエージェントのインストールの準備](#)
- [Windows ベースエージェントのインストールの準備](#)
- [CloudPoint エージェントのダウンロードとインストール](#)
- [Linux ベースのエージェントの登録](#)
- [Windows ベースのエージェントの登録](#)
- [CloudPoint アプリケーションプラグインの構成](#)
- [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](#)
- [クラウド資産に対する NetBackup 保護計画の作成](#)
- [NetBackup 保護計画へのクラウド資産のサブスクリプション](#)
- [スナップショットのリストアについて](#)
- [Microsoft SQL Server のリストアの要件および制限事項](#)
- [Oracle のリストアの要件および制限事項](#)

- **Oracle** スナップショットのリストア後に必要な追加手順
- **MongoDB** のリストアの要件および制限事項
- **MongoDB** スナップショットのリストア後に必要な追加手順
- **SQL AG** データベースをリストアする前に必要な手順
- **SQL** データベースの同じ場所へのリカバリ
- 代替の場所への **SQL** データベースのリカバリ
- **SQL Server** スナップショットのリストア後に必要な追加手順
- **SQL AG** データベースをリストアした後に必要な追加手順
- **Windows** インスタンスが **CloudPoint** 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
- 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
- **AWS RDS** データベースインスタンスをリストアした後に必要な追加手順

Microsoft SQL プラグインの構成に関する注意事項

Microsoft SQL 用 CloudPoint 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保護できます。プラグインを構成した後、CloudPoint 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 と Amazon AWS 環境でのみサポートされます。
- 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.17 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。
CloudPoint 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。

- CloudPoint 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.160 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。

メモ: CloudPoint 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。

<https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa>

Oracle プラグインの構成に関する注意事項

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。

- サポート対象のバージョンの Oracle が、サポート対象の RHEL (Red Hat Enterprise Linux) ホスト環境にインストールされています。
p.17 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 社のマニュアルを参照してください。
https://docs.oracle.com/cd/B19306_01/backup.102/b14192/setup005.htm
- 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。
- CloudPoint 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。CloudPoint 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

Veritas 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。

Veritas 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。

https://docs.oracle.com/cd/B10500_01/server.920/a96521/control.htm#3545

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。

MongoDB プラグインの構成に関する注意事項

MongoDB 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 MongoDB プラグインを構成できます。

MongoDB 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。

- MongoDB Enterprise 3.6 または 4.0 を実行している必要があります。
- MongoDB スタンドアロンインスタンスの検出がサポートされています。
- データベースとジャーナルは、同じボリュームに格納する必要があります。
- アプリケーションの整合性スナップショットを作成する場合は、ジャーナリングを有効にする必要があります。
- プラグインを構成するときに、次の情報を用意する必要があります。

表 6-1 MongoDB プラグインの構成パラメータ

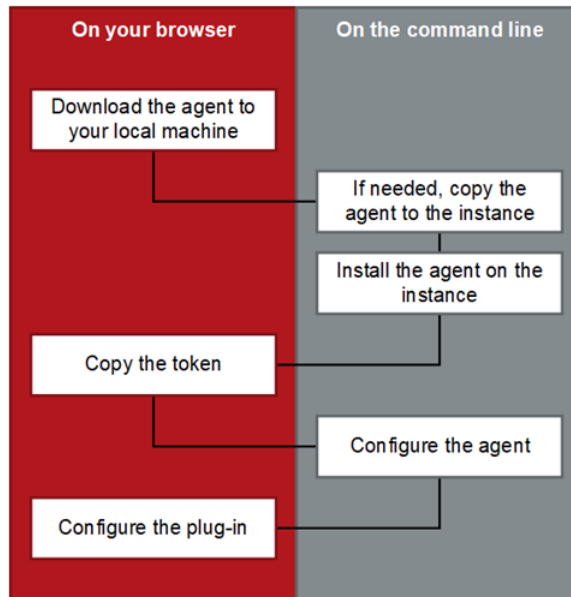
CloudPoint の構成パラメータ	説明
MongoDB 構成ファイルのパス	MongoDB conf ファイルの場所。
MongoDB 管理者ユーザー名	管理者権限を持つ MongoDB ユーザー名。
MongoDB 管理者ユーザーパスワード	MongoDB 管理者ユーザーアカウントのパスワード。

インストールと構成の処理について

CloudPoint 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からタスクを実行します。

エージェントレス接続機構を使用してもエージェント接続を確立できます。p.184 の「[エージェントレス機能について](#)」を参照してください。

図 6-1 CloudPoint エージェントのインストールと構成の処理



p.150 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.150 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.150 の「[CloudPoint 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 ベースエージェントのインストールの準備

アプリケーションホストに Linux ベースのエージェントをインストールする前に、次の操作を実行していることを確認してください。

- 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ます。
p.148 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.149 の「[インストールと構成の処理について](#)」を参照してください。

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 CloudPoint ホストで有効になっていることを確認します。
p.34 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。
- CloudPoint 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。

CloudPoint 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 CloudPoint 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.150 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。

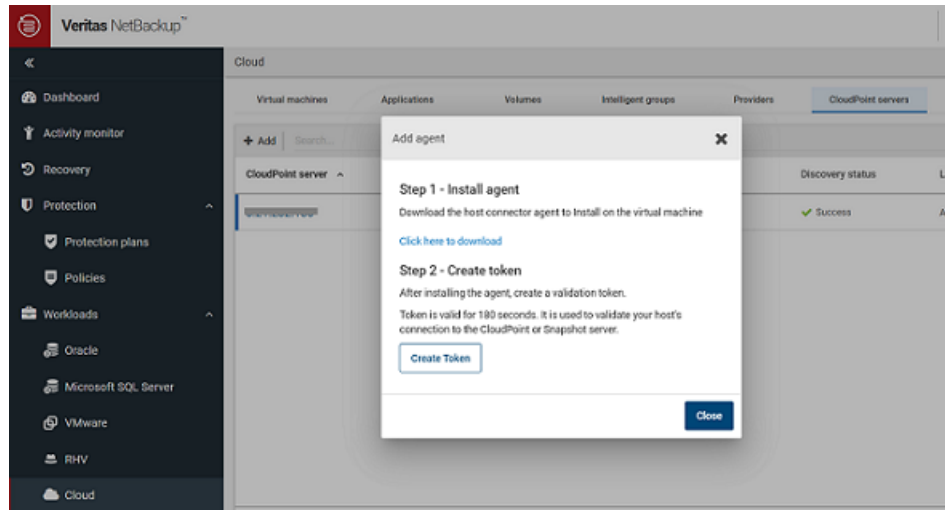
p.150 の「[Windows ベースエージェントのインストールの準備](#)」を参照してください。

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、[クラウド (Cloud)]をクリックし、次に[CloudPoint サーバー (CloudPoint servers)]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 CloudPoint サーバーが表示されます。

- 3 目的の CloudPoint 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り、認証トークンを取得します。

- 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 CloudPoint 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** ベースのエージェントの場合は、**Linux** ホスト上で次のコマンドを入力します。

```
# sudo yum -y install <cloudpoint_agent_rpm_name>
```

ここで、<cloudpoint_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
```

```
VRTScloudpoint-agent-8.3.0.8549-RHEL7.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。

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\VRTScloudpoint-agent-8.3.0.8549-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。

- 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.153 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.156 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.150 の「[CloudPoint 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。
- CloudPoint Linux ベースエージェントがすでにホストで設定されていて、同じ CloudPoint 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/VRTScloudpoint/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/VRTScloudpoint/keys
```

- CloudPoint Linux ベースエージェントがすでにホストで設定されていて、別の CloudPoint 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.240 の「[CloudPoint 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/VRTScloudpoint/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/VRTScloudpoint/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.150 の「[CloudPoint 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 CloudPoint instance <instance>.
```

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開いている場合は、NetBackup Web UI に再びサインインして、次の操作を行います。

- 左側のナビゲーションメニューで[クラウド (Cloud)]をクリックし、[CloudPoint サーバー (CloudPoint servers)]タブを選択します。
 - 目的の CloudPoint 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 CloudPoint 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、CloudPoint 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。

Add agent

×

Step 1 - Install agent

Download the host connector agent to install on the virtual machine

[Click here to download](#)

Step 2 - Create token

After installing the agent, create a validation token.

Token is valid for 180 seconds. It is used to validate your host's connection to the CloudPoint or Snapshot server.

Token

```
agent-2c9xc9o19fcklgffwzz3rp0h8vwxxtf9v9wmiv8o3vzfpbjwp-  
jzls5s5442vqy831ptlgqsswa3jw9jshk6k5ccm21fcdj59cxho6xnxydj1h9  
gf1vffwi8mmcdmcqmf37rixngl4384f2azw80fsmt3knelqfy7i0cmr4ky8xh  
gs442nqpvmzmsft4u8luiv4c53euc8lgu3lkm06g7yyauue9hcbh4bibhk74on  
4nulspnz4jpflb
```

167 seconds remaining.

Copy Token

Close

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 <cloudpoint_host_FQDN_or_IP> --token  
<authtoken>
```

ここで、<cloudpoint_host_FQDN_or_IP> は、CloudPoint 構成中に指定された CloudPoint 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、CloudPoint は次の処理を行います。

- Linux ベースのエージェントの登録
- Linux インスタンスでの /etc/flexsnap.conf 構成ファイルの作成と、CloudPoint ホスト情報を使用したファイルの更新
- Linux ホストでのエージェントサービスの有効化と起動

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、CloudPoint 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、CloudPoint 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.159 の「[CloudPoint 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.150 の「[CloudPoint 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。

- 左側のナビゲーションメニューで[クラウド (Cloud)]をクリックし、[CloudPoint サーバー (CloudPoint servers)]タブを選択します。
目的の CloudPoint 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 CloudPoint 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、CloudPoint 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。

Add agent

×

Step 1 - Install agent

Download the host connector agent to install on the virtual machine

[Click here to download](#)

Step 2 - Create token

After installing the agent, create a validation token.

Token is valid for 180 seconds. It is used to validate your host's connection to the CloudPoint or Snapshot server.

Token

agent-2c9xc9o19fcklgffwzz3rp0h8vwxxtf9v9wmiv8o3vzfpbjwp-jzls5s5442vqy831ptlgqsswa3jw9jshk6k5ccm21fcdj59cxho6xnxuydj1h9gf1vffwi8mmcdmcqmf37rixngl4384f2azw80fsm3knelqfy7i0cmr4ky8xhgs442nqpvmzmsft4u8luiv4c53euc8lgu3lkm06g7yyauue9hcbh4b1bhk74on4nulspmz4jplb

167 seconds remaining.

Copy Token

Close

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 <cloudpoint_host_FQDN_or_IP> --token  
<authtoken>
```

エージェントのインストール先ディレクトリは、以前にインストールウィザードを使用して **Windows** エージェントをインストールするときに指定したパスです。デフォルトのパスは `C:\Program Files\Veritas\CloudPoint\` です。

ここで、`<cloudpoint_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
`C:\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。

- 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、**CloudPoint** 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、**CloudPoint** 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.159 の「[CloudPoint 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。

CloudPoint アプリケーションプラグインの構成

CloudPoint 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。

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.153 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.156 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.147 の「[Oracle 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.148 の「[MongoDB 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.146 の「[Microsoft SQL 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。

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、[クラウド (Cloud)] をクリックしてから[仮想マシン (Virtual machines)] タブを選択します。
- 2 資産のリストから、CloudPoint 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 CloudPoint 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。
[CloudPoint サーバー (CloudPoint servers)] タブをクリックして、目的の CloudPoint 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。

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。

- CloudPoint 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。
- CloudPoint 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。

<https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa>

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. **CloudPoint** 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
```

クラウド資産に対する NetBackup 保護計画の作成

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。

保護計画を作成するには

- 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、[保護計画 (Protection plans)]をクリックし、右側の[追加 (Add)]をクリックします。
- 3 [基本プロパティ (Basic properties)]パネルで、次の操作を実行します。
 - 計画の[名前 (Name)]と[説明 (Description)]を入力します。
 - [作業負荷 (Workload)]ドロップダウンから、[クラウド (Cloud)]を選択します。

- [クラウドプロバイダ (Cloud Provider)] ドロップダウンから、クラウドプロバイダを選択します。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リブする際、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。
 - [次へ (Next)] をクリックします。
- 4 [スケジュールと保持 (Schedules and retention)] パネルで、目的のバックアップスケジュールを指定して[次へ (Next)] をクリックします。
 - 5 必要に応じて残りのオプションを構成し、[完了 (Finish)] をクリックして保護計画を作成します。
作成した計画が[保護計画 (Protection plans)] ペインに表示されます。
 - 6 この保護計画に資産を割り当てることができるようになりました。

p.162 の「[NetBackup 保護計画へのクラウド資産のサブスクリブ](#)」を参照してください。

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リブ

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リブできます。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リブする際、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リブするには

- 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、[クラウド (Cloud)] をクリックし、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まれます。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。

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。

スナップショットのリストアについて

リストアできるスナップショットの種類とリストアできる場所は、資産タイプによって異なります。

スナップショットをリストアするときは、次の点に注意してください。

- 暗号化された AWS スナップショットをリストアできます。暗号化されたスナップショットのリストアを有効にするには、KMS (Key Management Service) ポリシーを追加し、KMS キーへのアクセス権を NetBackup ユーザーに付与して暗号化されたスナップショットをリストアできるようにします。
- レプリケートされたホストのスナップショットをソースの領域とは別の場所にリストアする場合、ターゲットの場所でキーが利用できないため、リストアが失敗する可能性があります。
前提条件として、スナップショットのソースと同じ名前のキーペアを作成するか、ソースからターゲット領域にキーペアをインポートします。
次に、リストアが正常に完了したら、インスタンスのネットワーク設定からインスタンスのセキュリティグループを変更します。
- ファイルシステムを作成してマウントしているサポート対象のストレージアレイディスクのスナップショットを作成したら、そのファイルシステムを使用しているアプリケーション

を最初に停止してから、ファイルシステムをマウント解除してリストアを実行する必要があります。

- **LVM (Logical Volume Manager) および LDM (Logical Disk Manager)** ベースのストレージ領域上のアプリケーションスナップショットのリストアはサポートされていません。
- リストア操作後、リストアされたインスタンスのインバウンドポート規則を更新して、インスタンスへのリモートアクセスを取得します。
- **AWS/Azure/GCP** クラウドのディスクスナップショットと **volume snapshot** の場合は、最初にインスタンスからディスクを切断してから、元の場所にスナップショットをリストアする必要があります。
- **(AWS のみに該当)** ホストレベルのアプリケーションスナップショットをリストアする場合、作成される新しい仮想マシンの名前は、アプリケーションのスナップショットに対応するホストレベルのスナップショットの名前と同じになります。
たとえば、OracleAppSnap という名前のアプリケーションスナップショットを作成すると、**NetBackup** で OracleAppSnap-<number> という名前の対応するホストレベルのスナップショットが自動的に作成されます。たとえば、スナップショットの名前は OracleAppSnap-15 のようになります。
ここで、アプリケーションのスナップショット (OracleAppSnap) をリストアすると、新しい **VM** の名前は OracleAppSnap-<number> (timestamp) になります。
前述の例では、新しい **VM** の名前は OracleAppSnap-15 (restored Nov 20 2018 09:24) のようになります。
VM 名には、ホストレベルのスナップショットの名前である「Oracle-AppSnap-15」が含まれることに注意してください。
- **(AWS のみに該当)** ディスクレベルのアプリケーションスナップショットまたはディスクスナップショットをリストアするときに作成される新しいディスクには、名前が表示されません。ディスク名は空白で表示されます。
リストア後にディスクを識別して使用できるようにするには、ディスクに名前を手動で割り当てる必要があります。
- **Windows** インスタンスのスナップショットをリストアするときは、元のインスタンスのユーザー名、パスワード、または **pem** ファイルを使用して、新しくリストアされたインスタンスにログインできます。
デフォルトでは、**AWS** は **AMI** からインスタンスを起動した後、暗号化されたパスワードのランダムな生成を無効にします。毎回新しいパスワードを生成するには、**config.xml** で **Ec2SetPassword** を有効に設定する必要があります。パスワードを設定する方法について詳しくは、次のリンクを参照してください。
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2config-service.html#UsingConfigXML_WinAMI
- **CloudPoint 9.0** では、2019 年 6 月より前に作成された **Amazon EC2** インスタンスのリストアには、**AWS** の制限により製品の請求コードがありません。

- レプリケートされたスナップショット用に新しく作成されたボリュームのボリューム形式は、リージョンのデフォルトのボリューム形式に従います。
ボリューム形式が指定されていない場合は、次のデフォルト値が使用されます。

表 6-2 デフォルトのボリューム形式

リージョン	デフォルトのボリューム形式
us-east-1, eu-west-1, eu-central-1, us-west-1, us-west-2 ap-northeast-1, ap-northeast-2, ap-southeast-1, ap-southeast-2, ap-south-1 sa-east-1, us-gov-west-1, cn-north-1	標準
その他すべてのリージョン	gp2

- 同じ場所へのディスクレベルのスナップショットリストアを実行する場合は、リストアをトリガする前に、元のディスクがインスタンスに接続されていることを確認します。
既存の元のディスクがインスタンスから切断されている場合、リストア操作が失敗することがあります。
[p.180 の「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」](#)を参照してください。
- 1 つのスナップショットに一度に実行できるリストア操作は、1 つのみです。複数の操作が同じ資産に送信された場合、最初の操作のみがトリガされ、残りの操作は失敗します。
これは、一般的にすべての **CloudPoint** 操作に適用されます。**CloudPoint** では、同じ資産で同時に複数のジョブを実行することはサポートされていません。
- 複数のファイルシステムまたはデータベースを同じインスタンスにリストアする場合、**Veritas**では、これらの操作を 1 つずつ順番に実行することをお勧めします。
複数のリストア操作を並列して実行すると、インスタンスレベルで一貫性が失われる可能性があり、最終的に操作が失敗する場合があります。共有資産に相互にアクセスする必要がある複数のリストアジョブは許可されません。リストアジョブに参加している資産はロックされ、そのようなロックされた資産を必要とする他のジョブは失敗します。

次の種類の **SQL Server** 配備がサポートされています。

- スタンドアロンデータベースを含む **SQL** インスタンスとデータベース
インスタンスレベルでスナップショット操作とリストア操作を実行できます。**SQL** インスタンスのスナップショットを作成すると、そのインスタンスで構成されているすべてのオンラインデータベースがスナップショットに含まれます。
NetBackup 8.3 リリース以降は、同じ一連の操作を 1 つのデータベースレベルでも実行できます。オンライン状態にある個々のスタンドアロン **SQL** データベースのバックアップを作成し、同じ場所または代替の場所にリストアできます。既存のデータベースを上書きするオプションが用意されています。既存のものを上書きするオプションが

選択されていない場合は、同じ場所または代替の場所へのリストアは失敗します。ディスクレベルのスナップショットのリストア操作は、ターゲットホストのデータベースをリストアします。新しいデータベースは次の検出サイクルで検出され、UI に自動的に表示されます。

- AG (可用性グループ) に配備された SQL データベース
NetBackup 8.3 リリース以降、AG の一部である SQL データベースに対してバックアップ操作とリストア操作を実行できます。SQL AG のデータベースのスナップショットを取得すると、SQL データベース管理者が構成したレプリカからスナップショットが取得されます。AG 構成でレプリカとして構成されている SQL インスタンスに、単一の AG データベースをリストアできます。AG データベースは、AG 構成に含まれていない SQL インスタンスにもリストアできます。AG 環境にリストアする場合、リストアを実行する前に、データベースを AG から削除する必要があります。

p.166 の「[Microsoft SQL Server のリストアの要件および制限事項](#)」を参照してください。

p.167 の「[Oracle のリストアの要件および制限事項](#)」を参照してください。

p.169 の「[MongoDB のリストアの要件および制限事項](#)」を参照してください。

SQL AG データベースをリストアするためのプロセス

SQL AG (可用性グループ) データベースのスナップショットを複数のレプリカにリストアすることを計画している場合、Veritas では、次の順序に従って、各レプリカに対して順次リストアを実行することをお勧めします。

- プライマリレプリカのリストア前の手順を最初に実行します。
p.171 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。
- 次に、プライマリレプリカの AG データベースをリストアします。
p.172 の「[SQL データベースの同じ場所へのリカバリ](#)」を参照してください。
- リストアが完了した後、プライマリレプリカでリストア後の手順を実行します。
p.179 の「[SQL AG データベースをリストアした後に必要な追加手順](#)」を参照してください。
- プライマリレプリカの処理全体が完了した後、追加のセカンダリレプリカごとに同じプロセスを繰り返します。

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.172 の「**SQL データベースの同じ場所へのリカバリ**」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.176 の「**SQL Server 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。
- **CloudPoint** 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。
<https://support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa>
- **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.171 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。

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.168 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、ベリタスでは、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、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 **CloudPoint** ホストに接続されている
- **CloudPoint 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** `listener.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
```

MongoDB のリストアの要件および制限事項

MongoDB 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。

- ターゲットホストが接続または構成されている場合、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 MongoDB 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、MongoDB 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。

MongoDB 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、MongoDB 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.170 の「[MongoDB 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。

MongoDB スナップショットのリストア後に必要な追加手順

MongoDB 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。

メモ: これらの手動の手順は、同じ場所への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。

実行する手順

- 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接続されていること(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 アプリケーションホストに接続します。

- 3 次のコマンドを使用して、接続されたディスクをアプリケーションホストにマウントします。

```
# sudo mount /dev/<diskname> /<mountdir>
```

ここで **<diskname>** は、リストア後に作成された新しいディスクの名前で、**<mountdir>** はディスクをマウントするパスです。

- 4 MongoDB 構成ファイル `/etc/mongod.conf` を編集し、前の手順で指定した `<mountdir>` パスに `dbPath` パラメータ値を設定します。

- 5 アプリケーションホストで MongoDB サービスを起動し、サービスが実行中であることを確認します。

次のコマンドを使用します。

```
# sudo systemctl start mongod.service  
  
# sudo systemctl status mongod.service
```

メモ: 新しいホストへのディスクレベルのリストアの場合は、mongo がそのホストにインストールされていることを確認します。

- 6 MongoDB クライアントを使用して MongoDB サーバーにログオンし、データベースが実行されていることを確認します。

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 データベースの同じ場所へのリカバリ

次の手順を実行して、SQL Server スナップショットを資産と同じ場所にリストアします。続行する前に、次の点に注意してください。

- SQL AG データベースは同じ場所へのリカバリをサポートしません。
- RECOVERY と NORECOVERY リストアオプションは、SQL データベースにのみ適用されます。

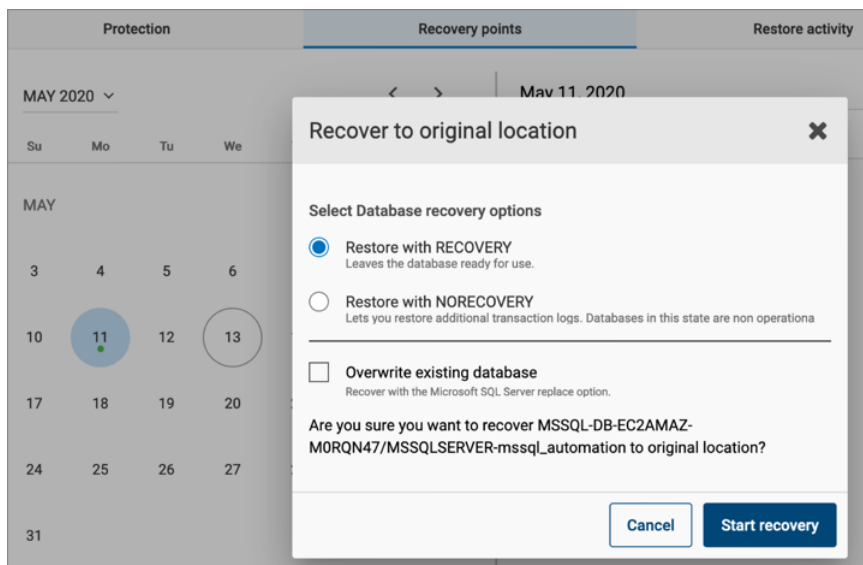
SQL スナップショットを同じ場所にリストアするには

- 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。
- 3 リカバリする SQL 資産を選択して、[詳細の表示 (View details)] をクリックし、[リカバリポイント (Recovery points)] タブを選択します。

このペインには、リストアに利用可能なすべてのリカバリポイントのスナップショットが表示されます。

- 4 リストアに使用するリカバリポイントのスナップショットをクリックして選択します。
- 5 右側の [リカバリ (Recover)] をクリックし、ドロップダウンメニューから [元の場所 (Original location)] を選択します。

- 6 [元の場所にリカバリする (Recover to original location)] ダイアログボックスで、データベースのリカバリオプションを選択し、[リカバリの開始 (Start recovery)] をクリックしてリカバリジョブをトリガします。



利用可能なオプションは次のとおりです。

リカバリオプション

説明

RECOVERY を指定してリストア (Restore with RECOVERY)

データベースで単一のリストアを実行し、一貫性がある動作状態に戻す場合は、このオプションを選択します。

データベースは、リストアの完了後すぐにアクセスできるようになります。

NORECOVERY を指定してリストア (Restore with NORECOVERY)

バックアップのグループから複数のデータベースのリストアを実行する場合は、このオプションを選択します。たとえば、完全バックアップスナップショットを使用してリストアを実行し、次にトランザクションログをリストアする場合です。

データベースはリストア状態のままで、アクセスできないままです。**RECOVERY** オプションを使用してトランザクションログをリストアした後にはのみ、データベースを操作できます。

既存のデータベースを上書き (Overwrite existing database)

リストア操作で元のデータベースを置換する場合は、このオプションを選択します。

- 7 [アクティビティモニター (Activity monitor)] ペインからリカバリジョブを監視できます。

状態コード 0 は、リカバリジョブが成功したことを示します。SQL データベースがリカバリされたことを確認できるようになりました。

代替の場所への SQL データベースのリカバリ

SQL データベースを新しい場所にリストアするには、次の手順を実行します。続行する前に、次の点に注意してください。

- SQL AG データベースは、代替の場所へのリカバリのみをサポートします。
- RECOVERY と NORECOVERY リストアオプションは、SQL データベースにのみ適用されます。
- AG データベースの場合、プライマリレプリカにリカバリする場合は、リストア時に RECOVERY オプションを選択する必要があります。セカンダリレプリカにリカバリする場合は、リストア時に NORECOVERY オプションを選択します。
- 同じ名前のデータベースを新しい場所にリストアする場合も同じ手順が適用されます。同じ名前のデータベースが新しい場所にすでに存在する場合、リストアを正常に実行するには、既存の上書きオプションを選択する必要があります。

SQL データベースを代替の場所にリストアするには

- 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。
- 3 リカバリする SQL 資産を選択して、[詳細の表示 (View details)] をクリックし、[リカバリポイント (Recovery points)] タブを選択します。

このペインには、リストアに利用可能なすべてのリカバリポイントのスナップショットが表示されます。
- 4 リストアに使用するリカバリポイントのスナップショットをクリックして選択します。
- 5 右側の [リカバリ (Recover)] をクリックし、ドロップダウンメニューから [代替の場所 (Alternate location)] を選択します。

- 6 [代替の場所にリカバリする (Recover to alternate location)]ダイアログボックスで、データベースのリカバリオプションを選択し、[リカバリの開始 (Start recovery)]をクリックしてリカバリジョブをトリガします。

利用可能なオプションは次のとおりです。

リカバリオプション	説明
RECOVERY を指定してリストア (Restore with RECOVERY)	データベースで単一のリストアを実行し、一貫性がある動作状態に戻す場合は、このオプションを選択します。 データベースは、リストアの完了後すぐにアクセスできるようになります。 メモ: AG データベースをプライマリレプリカにリカバリする場合は、このオプションを選択します。
NORECOVERY を指定してリストア (Restore with NORECOVERY)	バックアップのグループから複数のデータベースのリストアを実行する場合は、このオプションを選択します。たとえば、完全バックアップスナップショットを使用してリストアを実行し、次にトランザクションログをリストアする場合です。 データベースはリストア状態のままで、アクセスできないままです。RECOVERY オプションを使用してトランザクションログをリストアした後のみ、データベースを操作できます。 メモ: AG データベースをセカンダリレプリカにリカバリする場合は、このオプションを選択します。
既存のデータベースを上書き (Overwrite existing database)	ターゲットの場所に同じ名前のデータベースが存在する場合、このオプションは、リストア操作でそのデータベースを置換する場合に選択します。

- 7 [アクティビティモニター (Activity monitor)]ペインからリカバリジョブを監視できます。
- 状態コード 0 は、リカバリジョブが成功したことを示します。SQL データベースがリカバリされたことを確認できるようになりました。
- 8 リストアモードで SQL データベースをリカバリする場合にリカバリ操作が完了したら、SQL ホストのデータベースの状態が[リストア中... (Restoring...)]であることを確認します。
 - 9 必要な場合は、リカバリされたデータベースのトランザクションログを手動でリストアできます。

SQL Server 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 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 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 にログインします。
- 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。

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。

Windows インスタンスが CloudPoint 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

Windows インスタンスが CloudPoint 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 CloudPoint エージェントが、CloudPoint 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 CloudPoint 操作が、Windows インスタンスで失敗し始めます。

CloudPoint 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、CloudPoint 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
```

CloudPoint が Veritas 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 Veritas CloudPoint 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。

AWS RDS データベースインスタンスをリストアした後に必要な追加手順

AWS RDS データベースインスタンスの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。リストア操作が正常に実行された場合でも、これらの手動による手順は、通常の用途でインスタンスを利用できるようにするために必要です。

AWS RDS データベースのインスタンスを正常にリストアした後、リストアされたインスタンスの特定のプロパティを手動で確認して再割り当てする必要があります。これは、リストア操作自体が正常に実行された場合でも、1 つ以上のインスタンスプロパティが完全にはリストアされないために必要です。場合によっては、**NetBackup** はプロパティ値をデフォルト設定にリセットします。

次の RDS データベースインスタンスまたはクラスタプロパティは完全にはリストアされず、変更が必要になります。

- [VPC セキュリティグループ (VPC security groups)] の値 (AWS 管理コンソール、[RDS データベースインスタンス (RDS Database instance)]、[接続性とセキュリティ (Connectivity & security)] タブ)
- [削除の保護 (Deletion protection)] の設定 (AWS 管理コンソール、[RDS データベースインスタンス (RDS Database instance)]、[構成 (Configuration)] タブ)
- [スナップショットへのタグのコピー (Copy tags to snapshots)] の設定 (AWS 管理コンソール、[RDS データベースインスタンス (RDS Database instance)]、[保守とバックアップ (Maintenance & backups)] タブ)

次の手順を実行します。

- 1 RDS データベースインスタンスのスナップショットが正常にリストアされたことを確認します。
- 2 AWS 管理コンソールにログインし、右上隅から RDS インスタンスをリストアしたリージョンを選択します。
- 3 [サービス (Services)] メニューの [データベース (Database)] で、[RDS] をクリックします。
- 4 左側のダッシュボードメニューから、[データベース (Databases)] をクリックします。
- 5 [データベース (Databases)] パネルで、リストアされた RDS データベースインスタンスを選択し、右上のメニューバーから [変更 (Modify)] をクリックします。

- 6 [DB の変更 (Modify DB)] パネルで、次のプロパティを確認し、属性値が元のインスタンスと一致することを確認します。
 - [ネットワークとセキュリティ (Network & Security)] で、[セキュリティグループ (Security group)] の属性に正しいセキュリティグループ名が割り当てられていることを確認します。
 - [バックアップ (Backup)] で、[タグをスナップショットにコピー (Copy tags to snapshots)] オプションが元のインスタンスに従って設定されていることを確認します。
 - [削除の保護 (Deletion protection)] で、[削除を有効にする (Enable deletion protection)] オプションが元のインスタンスに従って設定されていることを確認します。
 - 必要に応じて、他のすべてのパラメータ値を確認し、設定します。
- 7 必要な RDS インスタンスのプロパティを変更したら、[続行 (Continue)] をクリックします。
- 8 [変更のスケジュール設定 (Scheduling of modifications)] で、インスタンスに変更を適用するタイミングに応じて適切なオプションを選択し、[DB インスタンスを変更 (Modify DB instance)] をクリックします。
- 9 RDS インスタンスのプロパティを確認し、変更が有効になっていることを確認します。

CloudPoint のエージェントレス機能を使用した資産の保護

この章では以下の項目について説明しています。

- [エージェントレス機能について](#)
- [エージェントレス構成の前提条件](#)
- [エージェントレス機能の構成](#)
- [CloudPoint のアップグレード後のエージェントレス機能の構成](#)

エージェントレス機能について

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、CloudPoint 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。

- CloudPoint ソフトウェアは、Linux では SSH、Windows の場合は WMI および SMB を介してホストにアクセスします。
- CloudPoint 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、CloudPoint ソフトウェアによってプロセスが停止されます。

現在、CloudPoint 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、MS SQL および MongoDB データベース資産を検出して動作します。

p.185 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.187 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 キー
- この機能を構成するホストで、CloudPoint 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。

CloudPoint 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。

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

CloudPoint 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。CloudPoint 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. CloudPoint 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、CloudPoint 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インします。
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. CloudPoint 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、CloudPoint 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

- リモートインスタンスへの接続に使用するユーザーアカウントでは、以下が可能である必要があります。
 - リモート管理共有 (ADMIN\$) へのアクセス。デフォルトで有効。
 - root¥cimv2 へのアクセス
- 次のポートを構成します。
 - セキュリティグループを変更して、ポート 135 と 445、WMI 用の動的ポートまたは固定ポートで受信トラフィックを許可します。
 - ファイアウォールで、ポート 135 と 445、Windows ホストの動的または固定 WMI-IN ポートに対して受信ルールを有効にします。

メモ: ポートの動的範囲は 49152 から 65535 です。

- 固定または動的 WMI-IN ポートを使用できます。固定 WMI-IN ポートを構成する場合は、
<https://docs.microsoft.com/ja-jp/windows/win32/wmisdk/setting-up-a-fixed-port-for-wmi>
 を参照してください。
- エージェントレス機能にアクセスするユーザーグループのユーザーアカウント制御を無効にします。
- SQL アプリケーションを保護するには、SQL Server にアクセスするために必要な管理者権限が、クラウドホストへの接続に使用するユーザーアカウントに必要です。

Windows での SMB の構成 (省略可能)

Windows でエージェントレス機能を構成する前に、次の SMB (Server Message Block) 構成を実行します。

- 値を True に設定して、SMB 共有への暗号化されていないアクセスを制限します。
`RejectUnencryptedAccess: True`
- Windows PowerShell で次のコマンドを実行して、SMB 1.0 を無効にします。
`Set-SmbServerConfiguration -EnableSMB1Protocol $false`
 詳しくは、
<https://docs.microsoft.com/ja-jp/windows-server/storage/file-server/smb-security#disabling-smb-10>
 を参照してください。

SMB のセキュリティについて詳しくは、
<https://docs.microsoft.com/ja-jp/windows-server/storage/file-server/smb-security> を
 参照してください。

Windows における WMI のセキュリティの構成 (省略可能)

WMI (Windows Management Instrumentation) のセキュリティは、名前空間データへのアクセスを保護します。CloudPoint は `root\cimv2` 名前空間を使用します。この名前空間は、接続オプションを使用して構成されているユーザーのみアクセス可能である必要があります。詳しくは、
<https://docs.microsoft.com/ja-jp/windows/win32/wmisdk/maintaining-wmi-security?redirectedfrom=MSDN>
 を参照してください。

エージェントレス機能の構成

CloudPoint 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.185 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、[クラウド (Cloud)] をクリックしてから [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、CloudPoint 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、MS SQL および MongoDB データベース資産を検出して動作します。

- 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 にクレデンシヤ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ヤ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「クレデンシヤルの管理」セクションを参照してください。

CloudPoint のアップグレード後のエージェントレス機能の構成

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ヤルを変更する場合は、クレデンシヤル管理から資産のクレデンシヤルを関連付け、更新する必要があります。

NetBackup CloudPoint 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。

- [CloudPoint](#) でのボリュームの暗号化のサポートについて
- [Azure](#) でのボリュームの暗号化
- [GCP](#) でのボリュームの暗号化
- [AWS](#) でのボリュームの暗号化

CloudPoint でのボリュームの暗号化のサポートについて

NetBackup CloudPoint は、AWS、Azure、および Google Cloud プラットフォーム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。

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)

Azure での暗号化について詳しくは、次のサイトを参照してください。

<https://docs.microsoft.com/ja-jp/azure/security/fundamentals/encryption-models>

表 8-1 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。

表 8-2 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。

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、次のサイトを参照してください。

<https://cloud.google.com/security/encryption-at-rest>

表 8-3 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 8-4 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	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。

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 での暗号化について詳しくは、次のサイトを参照してください。
<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

表 8-5 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。
CMEK	ソースディスクと同じ CMEK を使用します。

表 8-6 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。
CMEK	スナップショットと同じ CMEK を使用します。

CloudPoint 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 および Azure Stack のセキュリティの構成](#)
- [Azure および Azure Stack 用クラウドコネクタの構成](#)
- [Azure Stack の CA 構成](#)
- [CloudPoint への接続の保護](#)

Azure および Azure Stack のセキュリティの構成

Azure または Azure Stack の作業負荷には 2 つの方法で接続できます。

- CloudPoint サーバーは、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。
- CloudPoint サーバー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 と 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。

Azure および 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、CloudPoint サーバーの
`/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、パブリックルート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、CloudPoint サーバーの
`/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

CRL の検証は、**NetBackup** プライマリサーバーまたはメディアサーバーが CloudPoint
サーバーに接続したときに実行されます。また、CloudPoint サーバーがクラウド作業負
荷に接続したとき、および CloudPoint サーバーのデータムーバーコンテナが NetBackup
メディアサーバーに接続したときにも実行されます。

NetBackup プライマリサーバーまたはメディアサーバーが CloudPoint サーバーに接続
したとき、および CloudPoint サーバーが作業負荷に接続したとき、デフォルトでは証明
書失効リスト (CRL) の検証は無効です。

CloudPoint サーバーのデータムーバーコンテナと NetBackup メディアサーバー間の
CRL の検証は、デフォルトで有効です。

CloudPoint サーバーの `/cloudpoint/openv/netbackup/bp.conf` ファイルの
`VIRTUALIZATION_CRL_CHECK` パラメータで、次の値のいずれかを指定できます。

- **`DISABLE`** (または **`0`**): 失効の確認を無効にします。ホストとの通信時に、CRL で証
明書の失効状態は検証されません。これはデフォルト値です。
- **`LEAF`** (または **`1`**): CRL でリーフ証明書の失効状態が検証されます。
- **`CHAIN`** (または **`2`**): CRL で証明書チェーンの証明書すべての失効状態が検証され
ます。

CRL パスの指定

CRL の検証を有効にした場合は、外部 CA の失効した証明書を含むディレクトリへのパス
を指定する必要があります。

CloudPoint サーバーの `/cloudpoint/openv/netbackup/bp.conf` ファイルの
`ECA_CRL_PATH` パラメータで、外部 CA の証明書失効リスト (CRL) があるディレクトリ
のパスを指定します。パスは `/cloudpoint/eca/crl` にする必要があります。

`ECA_CRL_PATH` オプションが指定されていない場合、NetBackup は CRL 配布ポイント (CDP) で指定されている URL から CRL をダウンロードし、それら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。

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. ECA-1 で NetBackup と CloudPoint を構成し、ECA-1 または ECA-2 で Azure Stack を構成
 - `/cloudpoint/opensv/netbackup/bp.conf` ファイルで `ECA_TRUST_STORE_PATH` パラメータを構成する必要があります。
 - トラストストアファイルは `/cloudpoint/eca/trusted/cacerts.pem` にあり、PEM 形式です。
 - このファイルには、NetBackup と Azure Stack の両方のアプライアンスのパブリックルート証明書が含まれています。このファイルに、NetBackup のルート CA 証明書と Azure Stack アプライアンスのルートパブリック証明書を手動で追加します。
2. NBCA、CPCA (CloudPoint CA)、および ECA で構成した Azure Stack: Azure Stack アプライアンスのパブリックルート証明書のみ
`/cloudpoint/eca/trusted/cacerts.pem` ファイルに含める必要があります。
3. NBUCA、CPCA、Azure Stack クラウドをバックアップする ECA
 - ピアとホストの検証にデータムーバーコンテナで利用可能な `/usr/opensv/var/global/wmc/cloud/cacert.pem` ファイルを使用します。
 - CloudPoint サーバーで `ECA_TRUST_STORE_PATH` を構成します。
`ECA_TRUST_STORE_PATH` は、NetBackup ルート CA 証明書を含むファイルを指す必要があります。これにより `vnetd` が NetBackup サーバーに接続できるようになります。

CloudPoint への接続の保護

CloudPoint サーバーでは外部 CA の CRL を `/cloudpoint/eca/crl` 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/opensv/netbackup/bp.conf` ファイルの `ECA_CRL_PATH` パラメータに対してこ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 9-1 ECA パラメータ

パラメータ	デフォルト	値	注釈
eca_crl_check	0 (無効)	0 (無効) 1 (リーフ) 2 (チェーン)	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 CloudPoint 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 (無効): 検証時に CRL/OCSP は実行されません。 ■ 1 (リーフ): リーフにのみ CRL/OCSP 検証が実行されます。 ■ 2 (チェーン): チェーン全体に CRL/OCSP 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 CloudPoint CRL キャッシュを更新する間隔 (時間)。/cloudpoint/eca/crl 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 の CloudPoint CRL キャッシュを更新する時間間隔 (時間)。/cloudpoint/eca/crl 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。

メモ: /cloudpoint/flexsnap.conf 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、キャッシュは無効になります。

メモ: CRL の確認の範囲は、Azure と Azure Stack 限定です。

CloudPoint のメンテナンス

- [第10章 CloudPoint のログ](#)
- [第11章 CloudPoint のアップグレード](#)
- [第12章 CloudPoint のアンインストール](#)
- [第13章 CloudPoint のトラブルシューティング](#)

CloudPoint のログ

この章では以下の項目について説明しています。

- [CloudPoint のログ記録のしくみについて](#)
- [Fluentd ベースの CloudPoint ログ記録のしくみ](#)
- [CloudPoint ログ](#)
- [エージェントレスログ](#)
- [CloudPoint ログ記録のトラブルシューティング](#)

CloudPoint のログ記録のしくみについて

CloudPoint 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、次を参照してください。

<https://www.fluentd.org/>

すべての **CloudPoint** 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、**CloudPoint** 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。**MongoDB** コレクションと **flexsnap-fluentd** コンテナのログは、デフォルトで設定されている 2 つの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 **CloudPoint** 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 **CloudPoint** 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
- CloudPoint 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 CloudPoint ログ記録のしくみ

CloudPoint をインストールまたはアップグレードすると、CloudPoint 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、CloudPoint ホスト上で開始されます。このサービスは、他のすべての CloudPoint 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 CloudPoint 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、CloudPoint 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 CloudPoint 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、CloudPoint 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。

CloudPoint 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。

CloudPoint ホスト上で稼働する fluentd デーモンは、さまざまな宛先に CloudPoint 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。

CloudPoint の場合、これらのプラグイン構成は、CloudPoint 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、CloudPoint 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設定ファイルに追加されます。

- STDOUT
これは、CloudPoint 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、CloudPoint 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。

- MongoDB
- 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 MongoDB、Splunk または ElasticSearch ターゲットを設定するには、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、fluentd.conf 構成ファイルを変更します。

fluentd.conf ファイルを変更するには

- 1 CloudPoint ホスト上で、任意のテキストエディタを使用して
/cloudpoint/fluentd/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。

CloudPoint ログ

CloudPoint は、CloudPoint 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、CloudPoint ホストの `<install_path>/cloudpoint/logs` に格納されます。

表 10-1 CloudPoint ログファイル

ログ	説明
<code>/cloudpoint/logs/flexsnap.log</code>	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。
<code>/cloudpoint/logs/flexsnap-cloudpoint.log</code>	このログファイルには、CloudPoint のインストール関連のすべてのログが含まれています。
<code>/cloudpoint/logs/flexsnap-ipv6config</code>	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。
- `VRTSpxb` のログは、`opt` ディレクトリ内にあります。
- `bpbkar`、`bpcd`、`bpcIntcmd`、`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、CloudPoint サーバーの `/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 CloudPoint サーバーの 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
```

CloudPoint 拡張機能の場合、プライマリサーバーの構成が使用されます。プライマリ CloudPoint サーバーで構成を変更すると、1 時間以内に各 CloudPoint 拡張機能で構成が更新されます。プライマリ CloudPoint や CloudPoint 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 CloudPoint サーバーでのみ変更する必要があります。プライマリと CloudPoint 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、各プライマリまたは CloudPoint 拡張機能にマウントされた /cloudpoint に基づいて計算されます。

CloudPoint 拡張機能ログ

各 CloudPoint 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: /cloudpoint/logs ディレクトリ
- 管理対象 Kubernetes のクラスターベースの拡張機能ログ: ファイル共有に属する /cloudpoint/logs ディレクトリ

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: /tmp/ directory
- Windows: C:\¥¥ProgramData¥¥Veritas¥¥CloudPoint¥¥logs¥¥

CloudPoint 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 CloudPoint 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。

Docker 環境の場合: # `sudo cat /cloudpoint/logs/flexsnap.log | grep <flexsnap-service name>`

Podman 環境の場合: # `tail /cloudpoint/logs/flexsnap.log | grep <flexsnap-service name>`

CloudPoint 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。

- [CloudPoint のアップグレードについて](#)
- [サポート対象のアップグレードパス](#)
- [アップグレードのシナリオ](#)
- [CloudPoint のアップグレードの準備](#)
- [CloudPoint のアップグレード](#)
- [パッチまたは Hotfix を使用した CloudPoint のアップグレード](#)
- [CloudPoint の移行とアップグレード](#)
- [アップグレード後のタスク](#)

CloudPoint のアップグレードについて

2 つのバージョンの **CloudPoint** 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。

CloudPoint 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。**Veritas** では、同じホスト、または以前のバージョンの **CloudPoint** データボリュームが接続されている別のホストで **CloudPoint** 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 11-1 CloudPoint 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
8.3	9.0、9.1
9.0	9.1

注意:

- CloudPoint 2.2.x から 9.1 への直接のアップグレードはサポートされていません。
- OS のバージョンを超える CloudPoint のアップグレードはサポートされていません。RHEL 7.x ホストで CloudPoint を使用している場合は、RHEL 8.3 ホストにのみ移行できます。その後、RHEL 8.3 ホスト上の CloudPoint をアップグレードするには、上記の表に記載されているアップグレードパスに従います。

アップグレードのシナリオ

次の表に、CloudPoint のアップグレードのシナリオを示します。

メモ: NetBackup プライマリサーバーを 9.1 にアップグレードした後で 9.1 バージョンにアップグレードされていない CloudPoint サーバーは、互換性の問題を引き起こす可能性があります。

表 11-2 アップグレードのシナリオ

シナリオ	説明	処理
NetBackup 8.3 または 9.0 から NetBackup 9.1 への完全アップグレード	NetBackup を 9.1 にアップグレードする場合 (すべての CloudPoint サーバーのアップグレードを含む)	■ CloudPoint サーバーを無効にします。 ■ CloudPoint サーバーをアップグレードします。 ■ NetBackup プライマリサーバーをアップグレードします。 ■ 次に、CloudPoint サーバーを有効にします。 p.206 の「CloudPoint のアップグレード」を参照してください。 メモ: 1 台以上の CloudPoint 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 CloudPoint 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。

シナリオ	説明	処理
CloudPoint のみをバージョン 9.1 にアップグレードする	CloudPoint サーバーのみを 9.1 にアップグレードし、NetBackup は 9.1 にアップグレードしない場合	■ CloudPoint と NetBackup のバージョン間の互換性をサポートする EEB (緊急エンジニアリングバイナリ) を入手するには、ベリタステクニカルサポートにお問い合わせください。 ■ CloudPoint 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。 ■ CloudPoint サーバーをアップグレードします。 ■ 次に、CloudPoint サーバーを有効にします。 p.221 の「パッチまたは Hotfix を使用した CloudPoint のアップグレード」を参照してください。

CloudPoint 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。

- CloudPoint インスタンス、仮想マシン、または物理ホストが CloudPoint バージョン 9.1 の要件を満たしていることを確認します。
p.17 の「[システム要件への準拠](#)」を参照してください。
- CloudPoint 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 CloudPoint 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.235 の「[CloudPoint のバックアップ](#)」を参照してください。
- CloudPoint で実行されているジョブがないことを確認します。
 - NetBackup Web UI を使用している場合は CloudPoint サーバーを無効にし、進行中のすべてのジョブが完了するまで待機します。nbstlutil コマンドを使用して、保留中のすべての SLP 操作をキャンセルします。次のいずれかのコマンドを使用します。
 - 特定のイメージに対する保留中の SLP 操作をキャンセルする場合は、
nbstlutil cancel -backupid <value> を使用します。
 - 特定のライフサイクルに属するイメージに対する保留中の SLP 操作をキャンセルする場合は、nbstlutil cancel -lifecycle <name> を使用します。
 - NetBackup 管理コンソール (Java UI) を使用している場合は、NetBackup プライマリサーバーで、次のコマンドを実行してすべての NetBackup プロセスを停止します。
 - UNIX の場合: /usr/opensv/netbackup/bin/bp.kill_all

- Windows の場合: `install_path¥NetBackup¥bin¥bpdwn -f`
- CloudPoint 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 CloudPoint サーバーを有効にする必要があります。
- アップグレード後、スナップショットからのバックアップまたはバックアップジョブからのリストアに使用する CloudPoint サーバーはすべて、トークンを指定して再編集し、NetBackup 証明書が CloudPoint サーバーで生成されるようにする必要があります。詳しくは、『NetBackup Web UI クラウド管理者ガイド』の「CloudPoint サーバーの編集」セクションを参照してください。

CloudPoint のアップグレード

次の手順では、CloudPoint 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 CloudPoint 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。

Docker 環境でのアップグレード

Docker 環境で CloudPoint サーバーをアップグレードするには

- 1 CloudPoint アップグレードインストーラをダウンロードします。

CloudPoint 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 CloudPoint インストーラをダウンロードします。

CloudPoint ソフトウェアコンポーネントは Docker イメージの形式で利用可能で、これらのイメージは圧縮ファイルにパッケージ化されます。ファイル名の形式を次に示します。

`Veritas_CloudPoint_9.x.x.x.img.gz`

ファイル名の数値シーケンスは、製品のバージョンを表します。

- 2 CloudPoint 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 次のコマンドを使用して、イメージファイルをロードします。

```
# sudo docker load -i <imagefilename>
```

たとえば、バージョンが 9.1.0.0.9349 の場合、コマンド構文は次のようになります。

```
# sudo docker load -i  
Veritas_CloudPoint_9.1.0.0.9349.img.gz
```

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。

```
Load -i VRTScloudpoint-docker-9.1.0.0.9349.img.gz  
  
3b48714f4630: Loading layer [=====>]  
26.62kB/26.62kB  
e2be05255641: Loading layer [=====>]  
1.022GB/1.022GB  
f4019e787431: Loading layer [=====>]  
71.16MB/71.16MB  
8fa41882618d: Loading layer [=====>]  
2.56kB/2.56kB  
2eb7b5f07188: Loading layer [=====>]  
433.6MB/433.6MB  
9a80f5e55187: Loading layer [=====>]  
3.072kB/3.072kB  
Loaded image: veritas/flexsnap-policy:9.1.0.0.9349  
4610240a3245: Loading layer [=====>]  
2.56kB/2.56kB  
009536fb1f1f: Loading layer [=====>]  
4.096kB/4.096kB  
e281e184c054: Loading layer [=====>]  
51.31MB/51.31MB  
01455a2a7aca: Loading layer [=====>]  
38.89MB/38.89MB  
0cd7f5d9561b: Loading layer [=====>]  
803.8kB/803.8kB  
cbe0c1de2aeb: Loading layer [=====>]  
3.072kB/3.072kB  
bf3c086d3dc8: Loading layer [=====>]  
99.56MB/99.56MB  
Loaded image: veritas/flexsnap-api-gateway:9.1.0.0.9349
```

```
0c5d3de7e49e: Loading layer [=====>]
38.26MB/38.26MB
ecc5f9d1a612: Loading layer [=====>]
57.34kB/57.34kB
02b122e862b3: Loading layer [=====>]
4.327MB/4.327MB
Loaded image: veritas/flexsnap-cloudpoint:9.1.0.0.9349
Loaded image: veritas/flexsnap-fluentd:9.1.0.0.9349
60b2acb680f6: Loading layer [=====>]
3.584kB/3.584kB
f595300c08bc: Loading layer [=====>]
3.584kB/3.584kB
Loaded image: veritas/flexsnap-mongodb:9.1.0.0.9349
Loaded image: veritas/flexsnap-agent:9.1.0.0.9349
Loaded image: veritas/flexsnap-scheduler:9.1.0.0.9349
8df81d5ea017: Loading layer [=====>]
7.68kB/7.68kB
7d0351be3c82: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-nginx:9.1.0.0.9349
2ab7b82b7b67: Loading layer [=====>]
433.6MB/433.6MB
cb5786a5d4da: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-coordinator:9.1.0.0.9349
82845be8152d: Loading layer [=====>]
2.56kB/2.56kB
4335a9dd8761: Loading layer [=====>]
433.6MB/433.6MB
7726c32b0a94: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-onhostagent:9.1.0.0.9349
ee9829847a2f: Loading layer [=====>]
10.12MB/10.12MB
e821f4ed533d: Loading layer [=====>]
2.56kB/2.56kB
b2ca6971711b: Loading layer [=====>]
17.92kB/17.92kB
ac4489fdf0fb: Loading layer [=====>]
38.26MB/38.26MB
7a3246be4423: Loading layer [=====>]
12.92MB/12.92MB
663007ab9b7a: Loading layer [=====>]
```



```
31.74kB/31.74kB
Loaded image: veritas/flexsnap-config:9.1.0.0.9349
7eb7d2ecf33a: Loading layer [=====>]
12.92MB/12.92MB
4cbef47218cf: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-certauth:9.1.0.0.9349
44ed763d4f00: Loading layer [=====>]
38.29MB/38.29MB
a6d54a76196f: Loading layer [=====>]
4.096kB/4.096kB
e0340c5d3b40: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-rabbitmq:9.1.0.0.9349
Loaded image: veritas/flexsnap-notification:9.1.0.0.9349
45358ab4ca0b: Loading layer [=====>]
42.52MB/42.52MB
31b87f996cd9: Loading layer [=====>]
3.072kB/3.072kB
fe498c617335: Loading layer [=====>]
48.66MB/48.66MB
Loaded image: veritas/flexsnap-idm:9.1.0.0.9349

Loaded image: veritas/flexsnap-cloudpoint:9.1.0.0.9349
```

コマンドプロンプトで、状態メッセージの最後に表示される、ロードされたイメージ名とバージョンを書き留めます。これはアップグレード後の新しい **CloudPoint** のバージョンを表します。以降の手順で、この情報が必要になります。

メモ:ここに示すバージョンは、表示にのみ使用されます。実際のバージョンは、インストールする製品のリリースによって異なります。

- 4 インストールされている現在の **CloudPoint** のバージョンを書き留めておきます。次の手順ではバージョン番号を使用します。

- 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 **CloudPoint** を停止します。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<current_version> stop
```

ここで、**current_version** は、現在インストールされている **CloudPoint** のバージョンを表します。前の手順でメモしたバージョン番号を使用します。

たとえば、インストールした **CloudPoint** のバージョンが **9.0.0.0.9234** の場合、コマンドは次のようになります。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:9.0.0.0.9234 stop
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

CloudPoint 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.8a51aac1848c404ab61e4625d7b88703 ...done
Stopping container: flexsnap-workflow-long-15 ...done
Stopping container: flexsnap-workflow-long-14 ...done
Stopping container: flexsnap-workflow-long-13 ...done
Stopping container: flexsnap-workflow-long-12 ...done
Stopping container: flexsnap-workflow-long-11 ...done
Stopping container: flexsnap-workflow-long-10 ...done
Stopping container: flexsnap-workflow-long-9 ...done
Stopping container: flexsnap-workflow-long-8 ...done
Stopping container: flexsnap-workflow-long-7 ...done
Stopping container: flexsnap-workflow-long-6 ...done
Stopping container: flexsnap-workflow-long-5 ...done
Stopping container: flexsnap-workflow-long-4 ...done
Stopping container: flexsnap-workflow-long-3 ...done
Stopping container: flexsnap-workflow-long-2 ...done
```

```
Stopping container: flexsnap-workflow-long-1 ...done
Stopping container: flexsnap-workflow-long-0 ...done
Stopping container: flexsnap-workflow-15 ...done
Stopping container: flexsnap-workflow-14 ...done
Stopping container: flexsnap-workflow-13 ...done
Stopping container: flexsnap-workflow-12 ...done
Stopping container: flexsnap-workflow-11 ...done
Stopping container: flexsnap-workflow-10 ...done
Stopping container: flexsnap-workflow-9 ...done
Stopping container: flexsnap-workflow-8 ...done
Stopping container: flexsnap-workflow-7 ...done
Stopping container: flexsnap-workflow-6 ...done
Stopping container: flexsnap-workflow-5 ...done
Stopping container: flexsnap-workflow-4 ...done
Stopping container: flexsnap-workflow-3 ...done
Stopping container: flexsnap-workflow-2 ...done
Stopping container: flexsnap-workflow-1 ...done
Stopping container: flexsnap-workflow-0 ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-idm ...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
```

すべての **CloudPoint** 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、CloudPoint をアップグレードします。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<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 -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<new_version> install -y
```

ここで、**new_version** はアップグレード後の CloudPoint のバージョンを表します。

-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に対して承認が渡され、インストーラを非対話モードで進められます。

たとえば、以前に指定したバージョン番号を使用すると、コマンドは次のようになります。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:9.1.0.0.9349 install -y
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

- 7 新しい CloudPoint インストーラによって、実行中の既存の CloudPoint コンテナが検出され、それらの削除の確認を求められます。

Y キーを押して古い CloudPoint コンテナの削除を確定します。

メモ: インストーラが非対話モードで実行されている場合、入力はありません。

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。

インストーラに次のようなメッセージが表示されるまで待機してから、次の手順に進みます。

```
Installing the services
Configuration started at time: Sat May 1 17:27:49 UTC 2021
docker server version: 19.03.12 Supported: true
This is an upgrade to NetBackup CloudPoint 9.1.0.0.9349
Previous CloudPoint version: 9.0.0.0.9234
Removing exited container flexsnap-ipv6config ...done
The containers flexsnap-agent.9eb4362a2aff43f885be984467faa230
flexsnap-agent.0ae95311f7f74be89659e62746389bb7
flexsnap-workflow-system-0-min flexsnap-workflow-general-0-min
flexsnap-listener flexsnap-nginx flexsnap-notification
flexsnap-policy flexsnap-scheduler flexsnap-idm
flexsnap-onhostagent flexsnap-agent flexsnap-coordinator
flexsnap-api-gateway flexsnap-certauth flexsnap-rabbitmq
flexsnap-mongodb flexsnap-fluentd are running.
Do you wish to remove them ? (y/n): y
Removing container flexsnap-agent.9eb4362a2aff43f885be984467faa230
...done
Removing container flexsnap-agent.0ae95311f7f74be89659e62746389bb7
...done
Removing container flexsnap-workflow-system-0-min ...done
Removing container flexsnap-workflow-general-0-min ...done
Removing container flexsnap-listener ...done
Removing container flexsnap-nginx ...done
Removing container flexsnap-notification ...done
Removing container flexsnap-policy ...done
Removing container flexsnap-scheduler ...done
Removing container flexsnap-idm ...done
Removing container flexsnap-onhostagent ...done
Removing container flexsnap-agent ...done
Removing container flexsnap-coordinator ...done
Removing container flexsnap-api-gateway ...done
```

```
Removing container flexsnap-certauth ...done
Removing container flexsnap-rabbitmq ...done
Removing container flexsnap-mongodb ...done
Removing container flexsnap-fluentd ...done
Deleting network : flexsnap-network ...done
Do you want to take a backup of the CloudPoint metadata prior to
upgrade?
(y/n): y
Taking backup of CloudPoint metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_9.0.0.0.9234.tar.gz.
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-ipv6config ...done
Starting container: flexsnap-mongodb ...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-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-idm ...done
Starting container: flexsnap-config ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Sat May 1 17:28:53 UTC 2021
Before using backups from cloud snapshots, re-register CloudPoint
with the
NetBackup primary server
```

- 8 (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>
```

- 9 新しい CloudPoint 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.47 の「[CloudPoint 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。

- 10 これによりアップグレードプロセスは終了します。CloudPoint 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。
- 11 CloudPoint が NetBackup プライマリサーバーに登録されていない場合は、すぐに登録する必要があります。
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。

Podman 環境でのアップグレード

Podman 環境で CloudPoint サーバーをアップグレードするには

- 1 CloudPoint アップグレードインストーラをダウンロードします。
CloudPoint 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 CloudPoint インストーラをダウンロードします。
CloudPoint ソフトウェアコンポーネントは圧縮ファイルにパッケージ化されたイメージの形式で利用可能です。ファイル名の形式を次に示します。
`Veritas_CloudPoint_9.x.x.x.tar.gz`
例: `Veritas_CloudPoint_9.1.0.0.9349.tar.gz`
- 2 CloudPoint 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 イメージファイルを解凍して tar を解凍し、内容を一覧表示します。

```
# gunzip VRTScloudpoint-podman-9.1.0.0.9349.tar.gz  
# tar -xvf VRTScloudpoint-podman-9.1.0.0.9349.tar
```

出力は次のようになります。

```
flexsnap-cloudpoint-9.x.x.x.x.img  
flexsnap-coordinator-9.x.x.x.x.img  
flexsnap-agent-9.x.x.x.x.img  
flexsnap-onhostagent-9.x.x.x.x.img  
flexsnap-policy-9.x.x.x.x.img  
flexsnap-scheduler-9.x.x.x.x.img  
flexsnap-config-9.x.x.x.x.img  
flexsnap-certauth-9.x.x.x.x.img  
flexsnap-rabbitmq-9.x.x.x.x.img  
flexsnap-api-gateway-9.x.x.x.x.img  
flexsnap-notification-9.x.x.x.x.img  
flexsnap-fluentd-9.x.x.x.x.img  
flexsnap-nginx-9.x.x.x.x.img  
flexsnap-idm-9.x.x.x.x.img  
flexsnap-workflow-9.x.x.x.x.img  
flexsnap-listener-9.x.x.x.x.img  
flexsnap-datamover-9.x.x.x.x.img  
flexsnap-mongodb-9.x.x.x.x.img  
flexsnap-podman-api.service  
flexsnap-podman-containers.service  
flexsnap_preinstall.sh  
dnsname
```


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

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

出力は次のようになります。

```
Executing the following changes on this node to prepare the  
CloudPoint
```

```
server for installation:
```

- 1) Loading CloudPoint service images.
- 2) Copying dnsname plugin to the /usr/libexec/cni folder.
- 3) Check if dnsmasq rpm is installed on the host, if not,
installation is done automatically.
- 4) Creating and starting the systemd service for the Podman

```
API server.
```

```
Do you want to continue? (Yes/No): Yes
```

```
Loaded image(s): localhost/veritas/flexsnap-agent:9.1.0.0.9349
```

```
Loaded image(s):
```

```
localhost/veritas/flexsnap-api-gateway:9.1.0.0.9349
```

```
Loaded image(s): localhost/veritas/flexsnap-certauth:9.1.0.0.9349
```

```
.....
```

```
.....
```

```
Loaded image(s): localhost/veritas/flexsnap-workflow:9.1.0.0.9349
```

```
Copying dnsname plugin...done
```

```
Starting Podman API service...done
```

メモ: 出力はページに合わせて切り捨てられます。

- 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 **CloudPoint** を停止します。

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<current_version> stop
```

ここで、**current_version** は、現在インストールされている **CloudPoint** のバージョン (たとえば 9.0.0.0.9234) 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。

CloudPoint 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-workflow-system-0-0 ...done
Stopping container: flexsnap-workflow-indexing-0-0 ...done
Stopping container: flexsnap-workflow-general-0-0 ...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-idm ...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
```

すべての **CloudPoint** 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、CloudPoint をアップグレードします。

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<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 --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<new_version> install -y
```

ここで、**new_version** はアップグレード後の CloudPoint のバージョン (たとえば 9.1.0.0.9349) 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に対して承認が渡され、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。

- 7** 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。

```
Installing the services
Configuration started at time: Mon May  3 11:57:33 UTC 2021
podman server version: 2.0.5 Supported: true
This is an upgrade to NetBackup CloudPoint 9.1.0.0.9349
Previous CloudPoint version: 9.0.0.0.9234
Do you want to take a backup of the CloudPoint metadata prior to
upgrade?
(y/n): y
Taking backup of CloudPoint metadata...done
Backup completed successfully.
Backup file located at
/cloudpoint/backup/cloudpoint_9.0.0.0.9234.tar.gz.
[Storing /cloudpoint/keys/idm_store]
[Storing /cloudpoint/keys/flexsnap-idm_store]
Creating network: flexsnap-network ...done
Starting container: flexsnap-fluentd ...done
Starting container: flexsnap-mongodb ...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-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-idm ...done
Starting container: flexsnap-config ...done
Starting container: flexsnap-nginx ...done
Upgrade finished at time: Mon May  3 11:58:51 UTC 2021
Before using backups from cloud snapshots, re-register CloudPoint
with the
NetBackup primary server
```

- 8** (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 rmi -f <imagename>:<oldimage_tagid>
```

- 9 新しい CloudPoint 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.47 の「CloudPoint 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。
- 10 これによりアップグレードプロセスは終了します。CloudPoint 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。
- 11 CloudPoint が NetBackup プライマリサーバーに登録されていない場合は、すぐに登録する必要があります。
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。

パッチまたは Hotfix を使用した CloudPoint のアップグレード

パッチまたは Hotfix を使用しても現在の CloudPoint 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 CloudPoint 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、ベリタステクニカルサポート (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.206 の「CloudPoint 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 CloudPoint 9.1.0.0.9344 で、Podman 環境の RHEL 8.3 システムで CloudPoint パッチバージョン 9.1.0.0.9349 にアップグレードする場合を考えます。Docker 環境には、適切な Docker コマンドを使用して同じ手順が適用されます。

パッチまたは Hotfix を使用して CloudPoint をアップグレードするには

- 1 ベリタステクニカルサポートから入手できる CloudPoint EEB をダウンロードします。

例: Veritas_CloudPoint_9.1.0.0.9349.img.gz

- 2 バイナリを解凍して tar を解凍し、内容を一覧表示します。

```
# gunzip VRTScloudpoint-podman-9.1.0.0.9349.tar.gz
```

```
# tar -xvf VRTScloudpoint-podman-9.1.0.0.9349.tar
```

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

```
# ./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 **CloudPoint** を停止します。

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<current_version> stop
```

- 5 次のコマンドを実行して、**CloudPoint** をアップグレードします。

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<EEB_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 --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<EEB_version>install -y
```

ここで、*EEB_version* はアップグレード後の **CloudPoint** パッチまたは **Hotfix** のバージョン (たとえば **9.1.0.0.9349**) 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に対して承認が渡され、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。

- 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 rmi -f <imagename>:<oldimage_tagid>
```

- 7 新しい **CloudPoint** 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.47 の「**CloudPoint 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 CloudPoint のアップグレードプロセスが完了しました。CloudPoint 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。
- 9 CloudPoint が NetBackup プライマリサーバーに登録されていない場合は、すぐに登録する必要があります。
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。

CloudPoint の移行とアップグレード

CloudPoint の移行を開始する前に

CloudPoint をインストールする前に、次の手順を完了していることを確認してください。

- 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.17 の「[システム要件への準拠](#)」を参照してください。
- CloudPoint 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.30 の「[CloudPoint 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 8.3 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 8.3 OS にアップグレードするか、RHEL 8.3 で新しいシステムを作成できます。
 - システムを RHEL 7.x から RHEL 8.3 に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。
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/single/upgrading_from_rhel_7_to_rhel_8/index
- RHEL 8.3 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.31 の [表 1-13](#) 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
```


オンプレミスの場合はサブスクリプションを有効にします。

```
# sudo subscription-manager register --auto-attach  
--username=<username> --password=<password>
```
 - 必要に応じて Podman をインストールします。

```
# sudo yum install -y podman
```

- SELinux が有効になっている場合は、モードを **permissive** モードに変更してシステムを再起動します。
`/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。
- 次のコマンドを実行して、必要なパッケージ (`lvm2`、`udev`、`dnsmasq`) を Podman がインストールされている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 python3-pyudev-<version>  
#yum install -y systemd-udev-<version>  
#yum install -y dnsmasq-<version>
```
- 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.34 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 8.3 ホストに CloudPoint を移行します。

p.224 の「[RHEL 8.3 での CloudPoint の移行とアップグレード](#)」を参照してください。

RHEL 8.3 での CloudPoint の移行とアップグレード

RHEL 7.x ホストから新しい RHEL 8.3 ホストに CloudPoint 8.3 または 9.0 を移行するには、次の手順を実行します。

CloudPoint 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 **CloudPoint** を停止します。

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<current_version> stop
```

ここで、**current_version** は、現在インストールされている **CloudPoint** のバージョンを表します。

例:

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:9.0.0.0.9234 stop
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

CloudPoint 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.8a51aac1848c404ab61e4625d7b88703 ...done
Stopping container: flexsnap-workflow-long-15 ...done
Stopping container: flexsnap-workflow-long-14 ...done
Stopping container: flexsnap-workflow-long-13 ...done
Stopping container: flexsnap-workflow-long-12 ...done
Stopping container: flexsnap-workflow-long-11 ...done
Stopping container: flexsnap-workflow-long-10 ...done
Stopping container: flexsnap-workflow-long-9 ...done
Stopping container: flexsnap-workflow-long-8 ...done
Stopping container: flexsnap-workflow-long-7 ...done
Stopping container: flexsnap-workflow-long-6 ...done
Stopping container: flexsnap-workflow-long-5 ...done
Stopping container: flexsnap-workflow-long-4 ...done
Stopping container: flexsnap-workflow-long-3 ...done
Stopping container: flexsnap-workflow-long-2 ...done
```

```
Stopping container: flexsnap-workflow-long-1 ...done
Stopping container: flexsnap-workflow-long-0 ...done
Stopping container: flexsnap-workflow-15 ...done
Stopping container: flexsnap-workflow-14 ...done
Stopping container: flexsnap-workflow-13 ...done
Stopping container: flexsnap-workflow-12 ...done
Stopping container: flexsnap-workflow-11 ...done
Stopping container: flexsnap-workflow-10 ...done
Stopping container: flexsnap-workflow-9 ...done
Stopping container: flexsnap-workflow-8 ...done
Stopping container: flexsnap-workflow-7 ...done
Stopping container: flexsnap-workflow-6 ...done
Stopping container: flexsnap-workflow-5 ...done
Stopping container: flexsnap-workflow-4 ...done
Stopping container: flexsnap-workflow-3 ...done
Stopping container: flexsnap-workflow-2 ...done
Stopping container: flexsnap-workflow-1 ...done
Stopping container: flexsnap-workflow-0 ...done
Stopping container: flexsnap-nginx ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-idm ...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
```

すべての CloudPoint 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 8.3 ホストに CloudPoint 構成データを移行します。

- RHEL 7.x から RHEL 8.3 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 8.3 システムの /cloudpoint に移動します。
- RHEL 8.3 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 8.3 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.32 の「[CloudPoint 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。

これにより、CloudPoint の移行プロセスが完了します。

- 3 CloudPoint を RHEL 8.3 ホストに移行した後、次の手順を実行して CloudPoint を 9.1 にアップグレードします。

詳しい手順については、「Podman 環境で CloudPoint サーバーをアップグレードするには」を参照してください。

p.206 の「[CloudPoint のアップグレード](#)」を参照してください。

Podman 環境で CloudPoint をアップグレードするための簡単な手順

- 1 CloudPoint アップグレードインストーラをダウンロードします。

例: Veritas_CloudPoint_9.1.0.0.9349.img.gz

- 2 イメージファイルを解凍して tar を解凍し、内容を一覧表示します。

```
# gunzip VRTScloudpoint-podman-9.1.0.0.9349.tar.gz
# tar -xvf VRTScloudpoint-podman-9.1.0.0.9349.tar
```

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

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

- 4 次のコマンドを実行して、CloudPoint をアップグレードします。

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<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 --privileged
-v /cloudpoint:/cloudpoint
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<new_version> install -y
```

ここで、**new_version** はアップグレード後の CloudPoint のバージョン (たとえば 9.1.0.0.9349) 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に対して承認が渡され、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。

- 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。

```
# podman rmi -f <imagename>:<oldimage_tagid>
```

- 6 新しい CloudPoint 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.47 の「[CloudPoint 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。

- 7 これにより CloudPoint の移行とアップグレードのプロセスが完了します。CloudPoint 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。

- 8 CloudPoint が NetBackup プライマリサーバーに登録されていない場合は、すぐに登録する必要があります。

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。

アップグレード後のタスク

CloudPoint 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 CloudPoint エージェントをアップグレードします。

メモ: CloudPoint 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。CloudPoint 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)]、[CloudPoint サーバー (CloudPoint servers)]、[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-agent.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 cloudpoint_agent_rpm_name
```

ここで、**cloudpoint_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。
- 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)]、[CloudPoint サーバー (CloudPoint Servers)]、[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。
- Linux ホストで flexsnap エージェントサービスを起動します。
Linux ホストで次のコマンドを実行します。

```
# sudo systemctl start flexsnap-agent.service --renew --token <auth_token>
```
- 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。

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)]、[CloudPoint サーバー (CloudPoint servers)]、[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 Veritas CloudPoint 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)]、[CloudPoint サーバー (CloudPoint Servers)]、[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。
- エージェントを再びホストに登録します。
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 (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>
```
- 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.150 の「[CloudPoint 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 アップグレード後に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実行する場合は、アップグレードされた CloudPoint 構成の詳細が NetBackup で利用できるようにするため、NetBackup の構成を更新する必要があります。アップグレード後、スナップショットからのバックアップまたはバックアップジョブからのリストアに使用する CloudPoint サーバーはすべて、トークンを指定して再編集し、NetBackup 証明書が生成されるようにする必要があります。詳しくは、『NetBackup Web UI クラウド管理者ガイド』の「CloudPoint サーバーの編集」セクションを参照してください。

次のいずれかの操作を実行します。

- NetBackup Web UI から、CloudPoint サーバーの情報を編集します。

- Web UI で、左側のナビゲーションペインを[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックし、[CloudPoint サーバー (CloudPoint servers)]タブをクリックします。
- アップグレードした CloudPoint サーバーを選択し、右の省略記号のアクションボタンの[編集 (Edit)]をクリックします。
- [CloudPoint サーバーを編集 (Edit CloudPoint server)]ダイアログで、要求されたすべての詳細を指定します。
- [検証 (Validate)]をクリックして、CloudPoint サーバーの証明書を検証します。
- [トークン (Token)]フィールドに、標準ホストトークンを入力します。
- [保存 (Save)]をクリックして、CloudPoint サーバーの構成を更新します。
- または、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 -cloudpoint_server  
cp-hostname=cloudpoint_server_user_id admin -manage_workload  
<manage_workload>
```

メモ: クラウドの作業負荷を管理している CloudPoint 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、CloudPoint 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/opensv/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、『Veritas 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/qp-hostname>

tpconfig コマンドとそのオプションについて詳しくは、『Veritas NetBackup コマンドリファレンスガイド』を参照してください。

CloudPoint 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。

- [CloudPoint のアンインストールの準備](#)
- [CloudPoint のバックアップ](#)
- [CloudPoint プラグインの構成解除](#)
- [CloudPoint エージェントの構成解除](#)
- [CloudPoint エージェントの削除](#)
- [CloudPoint のスタンドアロン Docker ホスト環境からの削除](#)
- [CloudPoint 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](#)
- [CloudPoint のリストア](#)

CloudPoint のアンインストールの準備

CloudPoint 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 **CloudPoint** 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 **CloudPoint** 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、**CloudPoint** 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.240 の「[CloudPoint エージェントの削除](#)」を参照してください。

- CloudPoint サーバーを NetBackup から無効にすることを確認します。CloudPoint サーバーをどのように設定したか (オンプレミスまたはクラウド) に応じて、CloudPoint サーバーは、NetBackup Web UI または NetBackup 管理コンソール (Java UI) のいずれかから無効にできます。

手順については、『NetBackup Web UI バックアップ管理者ガイド』または『NetBackup Snapshot Client 管理者ガイド』を参照してください。

- 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 CloudPoint 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.235 の「[CloudPoint のバックアップ](#)」を参照してください。

CloudPoint のバックアップ

CloudPoint 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 **CloudPoint** をバックアップするには

1 CloudPoint サービスを停止します。

次のコマンドを使用します。

```
# sudo docker run -it --rm -v  
/full_path_to_volume_name:/full_path_to_volume_name -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:version stop
```

ここで、**version** は、現在インストールされている **CloudPoint** 製品のバージョンを表します。次のコマンドを使用して、バージョンを取得できます。

```
# cat /cloudpoint/version
```

次に例を示します。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:8.3.0.8549 stop
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

2 すべての CloudPoint コンテナが停止していることを確認してください。CloudPoint の一貫したバックアップを取得するために、CloudPoint 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。

```
# sudo docker ps | grep veritas
```

このコマンドでは、アクティブに実行されている **CloudPoint** 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。

```
# sudo docker kill container_name
```

次に例を示します。

```
# sudo docker kill flexsnap-api
```

- 4 すべてのコンテナが停止した後、**CloudPoint** 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、**CloudPoint** サービスを再起動します。

次のコマンドを使用します。

```
# sudo docker run -it --rm -v  
/full_path_to_volume_name:/full_path_to_volume_name-v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:version start
```

ここで、**version** は、現在インストールされている **CloudPoint** 製品のバージョンを表します。

次に例を示します。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:8.3.0.8549 start
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

CloudPoint がオンプレミスに配備されている場合

オンプレミスに配備されている **CloudPoint** をバックアップするには

1 CloudPoint サービスを停止します。

次のコマンドを使用します。

```
# sudo docker run -it --rm -v  
/full_path_to_volume_name:/full_path_to_volume_name -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:version stop
```

ここで、**version** は、現在インストールされている **CloudPoint** 製品のバージョンを表します。

次に例を示します。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v  
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:8.3.0.8549 stop
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

2 すべての **CloudPoint** コンテナが停止していることを確認してください。CloudPoint の一貫したバックアップを取得するために、**CloudPoint** 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。

```
# sudo docker ps | grep veritas
```

このコマンドでは、アクティブに実行されている **CloudPoint** 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。

```
# sudo docker kill container_name
```

次に例を示します。

```
# sudo docker kill flexsnap-api
```

- 4 フォルダ /cloudpoint をバックアップします。希望するバックアップ方式を使用します。

次に例を示します。

```
# tar -czvf cloudpoint_dr.tar.gz /cloudpoint
```

このコマンドは、/cloudpoint ディレクトリのデータを含む cloudpoint_dr という名前の圧縮されたアーカイブファイルを作成します。

CloudPoint プラグインの構成解除

CloudPoint 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、CloudPoint 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 CloudPoint 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 CloudPoint 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。

CloudPoint 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。

CloudPoint 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 CloudPoint で有効にするには、まず CloudPoint 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、CloudPoint 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 CloudPoint サーバーの CloudPoint 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、CloudPoint 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 CloudPoint 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 CloudPoint 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 CloudPoint 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 CloudPoint プラグインを構成解除する必要があります。CloudPoint 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。
- CloudPoint 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 CloudPoint 構成から削除されます。

CloudPoint 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 CloudPoint プラグイン構成を削除します。
p.238 の「[CloudPoint 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。

CloudPoint 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。

エージェントの登録とそのホストについてのすべての資産情報が、データベースから完全に削除されます。

- 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 CloudPoint 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.240 の「[CloudPoint エージェントの削除](#)」を参照してください。

CloudPoint エージェントの削除

CloudPoint エージェントを削除する前に、まず CloudPoint 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。CloudPoint 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 CloudPoint プラグインを管理します。

CloudPoint 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 CloudPoint 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 <cloudpoint_agent_package>
```

ここで、<cloudpoint_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

VRTScloudpoint-agent-2.2-RHEL7.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 VRTScloudpoint-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、CloudPoint エージェントのエントリ (Veritas CloudPoint 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、CloudPoint のアンインストールに進めます。

p.241 の「[CloudPoint 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。

CloudPoint のスタンドアロン Docker ホスト環境からの削除

CloudPoint 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 CloudPoint ホストで次のタスクが実行されます。

- 稼働中のすべての CloudPoint コンテナの停止
- CloudPoint コンテナの削除
- CloudPoint イメージのロード解除と削除

CloudPoint をアンインストールする方法

1. CloudPoint エージェントを CloudPoint 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.240 の「[CloudPoint 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 CloudPoint をアンインストールします。

```
# sudo docker run -it --rm
-v /full_path_to_volume:/full_path_to_volume
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> uninstall
```

環境に応じて、次のパラメータを置き換えます。

パラメータ	説明
<version>	ホストにインストールされている CloudPoint 製品のバージョンを表します。
<full_path_to_volume>	CloudPoint データボリュームへのパスを表します。通常は /cloudpoint です。

たとえば、製品バージョンが 8.3.0.8549 の場合、コマンド構文は次のようになります。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.0.8549 uninstall
```

プロキシサーバーを使用している場合、前の表に示した例を使用すると、コマンドの構文は次のようになります。

```
# sudo docker run -it --rm -v /cloudpoint:/cloudpoint -e
VX_HTTP_PROXY="http://proxy.mycompany.com:8080/" -e
VX_HTTPS_PROXY="https://proxy.mycompany.com:8080/" -e
VX_NO_PROXY="localhost,mycompany.com,192.168.0.10:80" -v
```

```
/var/run/docker.sock:/var/run/docker.sock  
veritas/flexsnap-cloudpoint:8.3.0.8549 uninstall
```

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

インストーラによって、ホストから関連する **CloudPoint** 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 Veritas CloudPoint  
-----  
Stopping flexsnap-mongodb ... done  
Stopping flexsnap-rabbitmq ... done  
Stopping flexsnap-auth ... done  
Stopping flexsnap-coordinator ... done  
Removing flexsnap-mongodb ... done  
Removing flexsnap-rabbitmq ... done  
Removing flexsnap-auth ... done  
Removing flexsnap-coordinator ... done  
Unloading flexsnap-mongodb ... done  
Unloading flexsnap-rabbitmq ... done  
Unloading flexsnap-auth ... done  
Unloading flexsnap-coordinator ... done
```

3. **CloudPoint** 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。

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

4. 必要に応じて、ホストから **CloudPoint** 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** イメージを表示するには、次の **docker** コマンドを使用します。

```
# sudo docker images -a
```

次の **docker** コマンドを使用して、ホストから **CloudPoint** コンテナイメージを削除します。

```
# sudo docker rmi <image ID>
```

5. これにより、ホストで **CloudPoint** のアンインストールが完了します。

次の手順は、**CloudPoint** を再配備することです。

p.36 の「[Docker 環境への CloudPoint のインストール](#)」を参照してください。

CloudPoint 拡張機能の削除 - VM ベースまたは管理対象 Kubernetes クラスターベース

アンインストール中に、インストーラにより CloudPoint 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 CloudPoint コンテナの停止
- CloudPoint 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。

```
# sudo docker run -it --rm
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<version> uninstall
```

例:

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint -v
/var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:<9.1.x.x.xxx> uninstall
```

メモ: これは改行のない 1 つのコマンドです。

Podman 環境の場合:

次のコマンドを実行します。

```
# podman run -it --rm --privileged
-v /<full_path_to_volume_name>:/<full_path_to_volume_name>
-v /run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<version> uninstall
```

例:

```
# podman run -it --rm --privileged
-v /cloudpoint:/cloudpoint -v
/run/podman/podman.sock:/run/podman/podman.sock
veritas/flexsnap-cloudpoint:<9.1.x.x.xxx> uninstall
```

メモ: これは改行のない 1 つのコマンドです。

環境に応じて、次のパラメータを置き換えます。

パラメータ

説明

<version>

ホストにインストールされている CloudPoint 製品のバージョンを表します。

<full_path_to_volume>

CloudPoint データボリュームへのパスを表します。通常は /cloudpoint です。

- 2 必要に応じて、拡張機能ホストから CloudPoint 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 CloudPoint 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 CloudPoint 拡張機能のアンインストールが完了します。

管理対象 Kubernetes クラスター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 **kubect1** がインストールされているホストからダウンロードした、拡張機能スクリプト **cp_extension_start.sh** を実行します。

次のコマンドを実行します。

```
bash cp_extension_start.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。

CloudPoint のリストア

次のいずれかの方法を使用して CloudPoint 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 CloudPoint のリカバリ
- オンプレミスのバックアップを使用した CloudPoint のリカバリ

クラウドにある CloudPoint 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 CloudPoint 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 CloudPoint 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** をインストールします。

p.31 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 CloudPoint サーバーインスタンスに接続します。

- 5** このサーバーに **CloudPoint** 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 **CloudPoint** 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** **CloudPoint** 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 CloudPoint をインストールします。

次のコマンドを使用します。

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.1.5300 install
```

ここで、8.3.1.5300 は、CloudPoint のバージョンを表します。現在インストールされている製品のバージョンに応じて、この値を置換します。

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

インストールプログラムは、CloudPoint 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 CloudPoint 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 CloudPoint での作業を再開できます。

オンプレミスの CloudPoint バックアップの使用

オンプレミスのバックアップを使用して CloudPoint をリカバリするには

- 1 新しい CloudPoint サーバーに既存の CloudPoint バックアップをコピーし、それを CloudPoint のインストールディレクトリに抽出します。

次の例では、/cloudpoint がバックアップされたため、コマンドで新しい /cloudpoint ディレクトリを作成します。

```
# tar -zxvf cloudpoint_dr.tar.gz -C /cloudpoint/
```

- 2 CloudPoint 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。

3 CloudPoint をインストールします。

次のコマンドを使用します。

```
# sudo docker run -it --rm
-v /cloudpoint:/cloudpoint
-v /var/run/docker.sock:/var/run/docker.sock
veritas/flexsnap-cloudpoint:8.3.1.5300 install
```

ここで、8.3.1.5300 は、**CloudPoint** のバージョンを表します。現在インストールされている製品のバージョンに応じて、この値を置換します。

メモ: これは 1 つのコマンドです。改行なしでコマンドを入力していることを確認します。

インストールプログラムは、**CloudPoint** 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 **CloudPoint** 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。

4 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 **CloudPoint** での作業を再開できます。

CloudPoint 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。

- [CloudPoint のトラブルシューティング](#)

CloudPoint 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。

- エージェントホストが突然再起動された場合に **CloudPoint** エージェントが **CloudPoint** サーバーへの接続に失敗する。

この問題は、**CloudPoint** 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 **CloudPoint** 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.alf2ac945cd844e393c9876f347bd817' 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 **CloudPoint** 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、**CloudPoint** 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 **CloudPoint** 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 Veritas CloudPoint 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 Veritas CloudPoint™ Agent サービスを再起動します。

- Windows ホストでの CloudPoint 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 CloudPoint 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、CloudPoint サーバーで CloudPoint 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.156 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.48 の「[CloudPoint 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 CloudPoint 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、CloudPoint 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 CloudPoint 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インします。

```
/usr/opensv/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/opensv/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/opensv/netbackup/bin/admincmd/bpgetconfig -g <primary Sserver  
host name> -L
```

NBU UUID とバージョン番号を取得した後、CloudPoint 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>
```

- スナップショットジョブは成功するが、CloudPoint サーバーの証明書が失効している場合、スナップショットジョブからのバックアップがエラー「証明書の検証に失敗しました (Certificate verification failed)」で失敗する

スナップショット操作からのバックアップで、NetBackup はスナップショットの作成中に CloudPoint サーバーと通信します。

バックアップ操作では、CloudPoint サーバーのデータムーバーコンテナと NetBackup メディアサーバーまたはプライマリサーバーとの間で通信が行われます。次のフラグを使用して、各サーバーの証明書の失効状態の確認を実施する必要があります。

- ECA_CRL_CHECK: デフォルトで有効で、バックアップ操作中に検証されます。一方、VIRTUALIZATION_CRL_CHECK はデフォルトで無効で、スナップショットおよびクラウドベンダーの操作中に検証されます。

- VIRTUALIZATION_CRL_CHECK: このフラグが有効で、CloudPoint マシン証明書が失効している場合、スナップショットジョブは失敗します。

p.192 の「[Azure および Azure Stack のセキュリティの構成](#)」を参照してください。

- Windows クラウドインスタンスに対するエージェントレスを使用した接続の確立が CloudPoint で失敗する

エラー 1: <Instance_name>: network connection timed out.

ケース 1: CloudPoint サーバーのログメッセージ:

```
WARNING - Cannot connect to the remote host. SMB Connection timeout
```

```
<IP address> <user>
```

```
...
```

```
flexsnap.OperationFailed: Could not connect to the remote server
```

```
<IP address>
```

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。

- **SMB ポート 445** がネットワークセキュリティグループに追加され、**CloudPoint** サーバーからアクセスできることを確認します。
- **SMB ポート 445** がクラウドインスタンスのファイアウォールで許可されていることを確認します。

ケース 2: **CloudPoint** サーバーのログメッセージ:

```
WARNING - Cannot connect to the remote host. WMI Connection  
timeout <IP address> <user>
```

```
...
```

```
flexsnap.OperationFailed: Could not connect to the remote  
server <IP address>
```

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。

- **DCOM ポート (135)** をネットワークセキュリティグループに追加し、**CloudPoint** サーバーからアクセスできることを確認します。
- **ポート 135** がクラウドインスタンスのファイアウォールで許可されていることを確認します。

ケース 3: **CloudPoint** サーバーのログメッセージ:

```
Exception while opening SMB connection, [Errno Connection error  
(<IP address>:445)] [Errno 113] No route to host.
```

回避方法: クラウドインスタンスが起動して実行中であるか、不整合な状態になっていないことを確認します。

ケース 4: **CloudPoint** サーバーのログメッセージ:

```
Error when closing dcom connection: 'Thread-xxxx'"
```

ここで、**xxxx** はスレッド番号です。

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。

- 構成されている **WMI-IN** 動的ポートの範囲または固定ポートがネットワークセキュリティグループに追加されていることを確認します。
- クラウドインスタンスファイアウォールから **WMI-IN** ポートを確認して有効にします。

エラー 2: <Instance_name>: Could not connect to the virtual machine.

CloudPoint サーバーのログメッセージ:

```
Error: Cannot connect to the remote host. <IP address> Access denied.
```

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。

- ユーザーに管理者権限が付与されていることを確認します。
- ユーザーの **UAC** が無効になっていることを確認します。
- ファイアウォールが無効な場合、**RHEL** システムで **CloudPoint** のクラウド操作が失敗する

CloudPoint 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 **CloudPoint** 操作が失敗します。これはネットワーク構成の問題で、**CloudPoint** 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

- **CloudPoint** を停止します。

```
# docker run --rm -it
-v /var/run/docker.sock:/var/run/docker.sock
-v /cloudpoint:/cloudpoint veritas/flexsnap-cloudpoint:<version>
stop
```

- **Docker** を再起動します。

```
# systemctl restart docker
```

- **CloudPoint** を再起動します。

```
# docker run --rm -it
-v /var/run/docker.sock:/var/run/docker.sock
-v /cloudpoint:/cloudpoint veritas/flexsnap-cloudpoint:<version>
start
```