

Veritas NetBackup™ CloudPoint インストールガイド

Ubuntu、RHEL

リリース 8.3

Veritas NetBackup CloudPoint インストールガイド

最終更新日: 2020-09-13

マニュアルバージョン: 8.3 Rev 0

法的通知と登録商標

Copyright © 2020 Veritas Technologies LLC. All rights reserved.

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

この製品には、サードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア（「サードパーティプログラム」）が含まれている場合があります。一部のサードパーティプログラムは、オープンソースまたはフリーソフトウェアライセンスの下で利用できます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このVeritas製品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、をご覧ください。

<https://www.veritas.com/licensing/process>

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、本書の提供、内容の実施、また本書の利用によって偶発的あるいは必然的に生じる損害については責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

ライセンスソフトウェアおよび文書は、FAR 12.212 に定義される商用コンピュータソフトウェアと見なされ、Veritasがオンプレミス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。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。サポートサービスとテクニカルサポートへの問い合わせ方法については、次の弊社の **Web** サイトにアクセスしてください。

<https://www.veritas.com/support>

次の URL で Veritas Account の情報を管理できます。

<https://my.veritas.com>

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

世界中 (日本以外)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

マニュアル

マニュアルの最新バージョンがあることを確認してください。各マニュアルには、2 ページ目に最終更新日が示されます。マニュアルのバージョンは、各ガイドの 2 ページ目に示されます。最新のマニュアルは、次のベリタス **Web** サイトで入手できます。

<https://sort.veritas.com/documents>

マニュアルに関するご意見やご感想

ご意見、ご感想をお待ちしています。改善すべき点や、マニュアル上の誤記、欠落がありましたらお寄せください。お送りいただく際は、マニュアルの題名とバージョン、章のタイトル、セクションのタイトルを明記してください。ご意見、ご感想の送信先アドレス:

NB.docs@veritas.com

ベリタスのコミュニティサイトで、マニュアルに関する情報を確認したり、質問を投稿することもできます。

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

第 1 部	CloudPoint のインストールおよび構成	8
第 1 章	CloudPoint のインストールの準備	9
	配備方法について	9
	CloudPoint を実行する場所の決定	10
	クラウドでの CloudPoint の配備について	11
	システム要件への準拠	11
	CloudPoint ホストのサイズ変更に関する推奨事項	17
	CloudPoint をインストールするインスタンスの作成または物理ホストの準備	19
	Docker のインストール	19
	CloudPoint データを格納するボリュームの作成とマウント	21
	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	22
第 2 章	Docker イメージを使用した CloudPoint の配備	23
	CloudPoint のインストール	23
	CloudPoint が正常にインストールされたことの確認	29
	CloudPoint での AWS KMS の構成	30
第 3 章	CloudPoint クラウドプラグイン	35
	AWS プラグインの構成に関する注意事項	35
	AWS プラグイン構成の前提条件	39
	CloudPoint の AWS アクセス権の構成	40
	CloudPoint に必要な AWS アクセス権	42
	クロスアカウントの構成を作成する前に	45
	Google Cloud Platform プラグインの構成に関する注意事項	48
	CloudPoint で必要な Google Cloud Platform アクセス権	50
	CloudPoint の GCP サービスアカウントの構成	52
	プラグイン構成のための GCP サービスアカウントの準備	53
	Microsoft Azure プラグインの構成に関する注意事項	54
	Microsoft Azure でのアクセス権の設定	57

第 4 章

CloudPoint クラウドプラグインを構成する方法	59
CloudPoint ストレージアレイプラグイン	60
NetApp プラグインの構成に関する注意事項	60
NetApp プラグインの構成パラメータ	61
NetBackup アクセスの専用 LIF の構成	62
NetApp ストレージでサポートされる CloudPoint 操作	62
Nutanix Files プラグインの構成に関する注意事項	65
Nutanix Files プラグイン構成の前提条件	65
Nutanix Files プラグインの考慮事項および制限事項	66
Nutanix Files ファイルサーバーでサポートされる CloudPoint 操作	67
Nutanix Files の NetBackup 問題のトラブルシューティング	68
Dell EMC Unity アレイプラグインの構成パラメータ	69
サポートされる Dell EMC Unity アレイ	70
Dell EMC Unity アレイでサポートされる CloudPoint 操作	70
Pure Storage FlashArray プラグインの構成に関する注意事項	71
サポート対象の Pure Storage FlashArray モデル	72
Pure Storage FlashArray モデルでサポートされている CloudPoint 操作	72
HPE RMC プラグインの構成に関する注意事項	73
RMC プラグインの構成パラメータ	74
サポート対象の HPE ストレージシステム	74
HPE ストレージアレイでサポートされている CloudPoint 操作	74
Hitachi プラグインの構成に関する注意事項	77
Hitachi プラグインの構成パラメータ	78
サポート対象の Hitachi ストレージアレイ	78
Hitachi アレイでサポートされる CloudPoint 操作	79
InfiniBox プラグインの構成に関する注意事項	80
InfiniBox プラグインの構成パラメータ	81
InfiniBox アレイでサポートされる CloudPoint 操作	81
CloudPoint ストレージアレイのプラグインの構成方法	84

第 5 章

CloudPoint アプリケーションエージェントとプラグイン	85
Microsoft SQL プラグインの構成に関する注意事項	86
Oracle プラグインの構成に関する注意事項	87
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	88
MongoDB プラグインの構成に関する注意事項	89
インストールと構成の処理について	89
Linux ベースエージェントのインストールの準備	90
Windows ベースエージェントのインストールの準備	90

CloudPoint エージェントのダウンロードとインストール	91
Linux ベースのエージェントの登録	94
Windows ベースのエージェントの登録	97
CloudPoint アプリケーションプラグインの構成	100
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	101
クラウド資産に対する NetBackup 保護計画の作成	102
NetBackup 保護計画へのクラウド資産のサブスクリプション	103
スナップショットのリストアについて	104
SQL AG データベースをリストアするためのプロセス	107
Microsoft SQL Server のリストアの要件および制限事項	107
Oracle のリストアの要件および制限事項	108
MongoDB のリストアの要件および制限事項	109
SQL AG データベースをリストアする前に必要な手順	110
SQL データベースの同じ場所へのリカバリ	110
代替の場所への SQL データベースのリカバリ	113
SQL Server スナップショットのリストア後に必要な追加手順	115
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	115
SQL AG データベースをリストアした後に必要な追加手順	118
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	119
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	119
MongoDB スナップショットのリストア後に必要な追加手順	121
Oracle スナップショットのリストア後に必要な追加手順	122
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	123

第 6 章

CloudPoint のエージェントレス機能を使用した資産の保護	125
エージェントレス機能について	125
エージェントレス構成の前提条件	126
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	126
エージェントレス機能の構成	127

第 2 部

CloudPoint のメンテナンス	130
--------------------------	-----

第 7 章

CloudPoint のログ	131
CloudPoint のログ記録のしくみについて	131
Fluentd ベースの CloudPoint ログ記録のしくみ	132

	CloudPoint fluentd 構成ファイルについて	132
	fluentd 構成ファイルの変更	133
	CloudPoint ログ	133
第 8 章	CloudPoint のトラブルシューティング	135
	CloudPoint の再起動	135
	CloudPoint ログ記録のトラブルシューティング	136
	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	137
	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	138
	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	138
第 9 章	CloudPoint のアップグレード	140
	CloudPoint のアップグレードについて	140
	サポート対象のアップグレードパス	140
	アップグレードのシナリオ	141
	CloudPoint のアップグレードの準備	141
	CloudPoint のアップグレード	142
第 10 章	CloudPoint のアンインストール	154
	CloudPoint のアンインストールの準備	154
	CloudPoint のバックアップ	156
	CloudPoint プラグインの構成解除	159
	CloudPoint エージェントの構成解除	160
	CloudPoint エージェントの削除	161
	CloudPoint のスタンドアロン Docker ホスト環境からの削除	162
	CloudPoint のリストア	165

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 Docker イメージを使用した CloudPoint の配備](#)
- [第3章 CloudPoint クラウドプラグイン](#)
- [第4章 CloudPoint ストレージアレイプラグイン](#)
- [第5章 CloudPoint アプリケーションエージェントとプラグイン](#)
- [第6章 CloudPoint のエージェントレス機能を使用した資産の保護](#)

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。

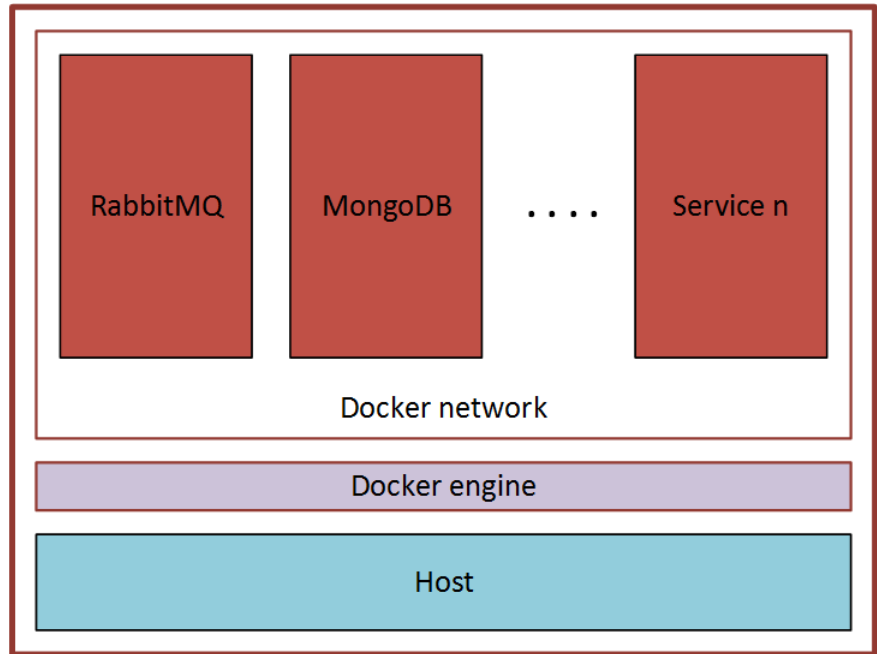
- [配備方法について](#)
- [CloudPoint を実行する場所の決定](#)
- [クラウドでの CloudPoint の配備について](#)
- [システム要件への準拠](#)
- [CloudPoint ホストのサイズ変更に関する推奨事項](#)
- [CloudPoint をインストールするインスタンスの作成または物理ホストの準備](#)
- [Docker のインストール](#)
- [CloudPoint データを格納するボリュームの作成とマウント](#)
- [インスタンスまたは物理ホストで特定のポートが開いていることの確認](#)

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。

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。

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。

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。

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 16.04 および 18.04 Server LTS ■ Red Hat Enterprise Linux (RHEL) 7.x
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
Amazon Web Services (AWS) インスタンス	■ Elastic Compute Cloud (EC2) インスタンスタイプ: t3.large ■ vCPU: 2 ■ RAM: 16 GB ■ ルートディスク: ソリッドステートドライブ (GP2) 付き 64 GB ■ データボリューム: スナップショット資産データベースに対する暗号化があるタイプ GP2 の 50 GB EBS (Elastic Block Store) ボリューム。この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: 16 GB ■ ルートディスク: 64 GB SSD ■ データボリューム: スナップショット資産データベース用の 50 GB 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/書き込みを設定します。 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
Google Cloud Platform (GCP) VM	■ 仮想マシン形式: n1-standard-2 ■ 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

CloudPoint がインストールされているホスト	要件
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 Docker コンテナ	10 GB
CloudPoint エージェントとプラグイン	350 MB (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

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 p.86 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 p.89 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 単一ノード構成がサポート対象です。 p.87 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。

カテゴリ	サポート
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 ■ 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。
クラウドプラットフォーム	■ Amazon Web Services (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 以降の仕様の 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 以前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。 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 以降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 標準以降の仕様の 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 以降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 のタイプのディスクをサポートします。 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。 ■ Google Cloud Platform (GCP) アプリケーションを保護する場合、アプリケーションは n1-standard-2 以降の仕様の GCP 仮想マシン形式でホストされている必要があります。

カテゴリ	サポート
ストレージプラットフォーム	■ NetApp ストレージアレイ p.60 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.69 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.73 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.71 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.77 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.80 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。

注意:

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!"
```

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 ホストのサイズ変更に関する推奨事項

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。したがって、**Oracle** や **Microsoft SQL Server** などのデータベースアプリケーションでは、他の資産と比べて、より多くの容量を設定する必要があります。

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

表 1-7 一般的な **CloudPoint** ホスト構成

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.xlarge 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させられます。

- 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。

CloudPoint をインストールするインスタンスの作成または物理ホストの準備

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 インストールの要件を満たすサポート対象の Ubuntu または RHEL インスタンスイメージを選択します。
- インストールの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 または RHEL オペレーティングシステムを物理 x86 サーバーにインストールします。
- インストールの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。

Docker のインストール

表 1-8 Docker 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 18.03 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

プラットフォーム	説明
RHEL 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> ■ CloudPoint が Azure クラウドに配備される場合、共有マウントを有効にします。 ■ <code>docker.service</code> システムユニットファイルを編集し、パラメータ MountFlags=slave を MountFlags=shared に変更します。 ■ ユニットファイルを保存して閉じてから、次のコマンドを使用して変更内容を確認します。 <pre># cat /usr/lib/systemd/system/docker.service grep MountFlags</pre> 出力は <code>MountFlags = shared</code> として表示されます。 ■ 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。 <code>/etc/selinux/config</code> 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 <code>Current Mode</code> 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

CloudPoint データを格納するボリュームの作成とマウント

CloudPoint をクラウド環境に配備する前に、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。

表 1-9 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
Amazon Web Services (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

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 1-10 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。

Docker 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](#)
- [CloudPoint が正常にインストールされたことの確認](#)
- [CloudPoint での AWS KMS の構成](#)

CloudPoint のインストール

このセクションの手順を完了する前に、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.10 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.11 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.19 の「[CloudPoint をインストールするインスタンスの作成または物理ホストの準備](#)」を参照してください。
- Docker をインストールします。
p.19 の「[Docker のインストール](#)」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.21 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.22 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: 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。

CloudPoint イメージ名は次のような形式です。

```
Veritas_CloudPoint_8.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> (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。
<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)	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。

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。次の手順は、**CloudPoint** サーバーを **VeritasNetBackup** マスターサーバーに登録することです。

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は、『**NetBackup Snapshot Client 管理者ガイド**』で手順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.135 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。

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

コマンドの出力は次のようになります。

CONTAINER ID	IMAGE	CREATED	STATUS
f4c70b6accff hours	veritas/flexsnap-agent:8.3.0.8549	6 hours ago	Up 6
1cfe9f79f260 hours	veritas/flexsnap-nginx:8.3.0.8549	6 hours ago	Up 6
331c81a09ba2 hours	veritas/flexsnap-idm:8.3.0.8549	6 hours ago	Up 6
4a2337b0af95 hours	veritas/veritas/flexsnap-notification:8.3.0.8549	6 hours ago	Up 6
b4096679da38 hours	veritas/flexsnap-policy:8.3.0.8549	6 hours ago	Up 6
27cd6a38d120 hours	veritas/flexsnap-scheduler:8.3.0.8549	6 hours ago	Up 6
524dde7a1060 hours	veritas/flexsnap-onhostagent:8.3.0.8549	6 hours ago	Up 6
8bf5d31d948f hours	veritas/flexsnap-agent:8.3.0.8549	6 hours ago	Up 6
a1566d261f70 hours	veritas/flexsnap-coordinator:8.3.0.8549	6 hours ago	Up 6
e8a4bd103b1f hours	veritas/flexsnap-api-gateway:8.3.0.8549	6 hours ago	Up 6
52f26268ed26 hours	veritas/flexsnap-certauth:8.3.0.8549	6 hours ago	Up 6

da76eadf3c25 hours	veritas/flexsnap-rabbitmq:8.3.0.8549	6 hours ago	Up 6
4206a48a4d6b hours	veritas/flexsnap-mongodb:8.3.0.8549	6 hours ago	Up 6
b54d1a6201e4 hours	veritas/flexsnap-fluentd:8.3.0.8549	6 hours ago	Up 6

メモ: イメージ名列に表示される数字 (8.3.0.8549) 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ます。実際の出力には、コンテナ名や使用されているポートなどの追加の詳細情報が含まれることがあります。

CloudPoint での AWS KMS の構成

これは CloudPoint インスタンスが AWS クラウドに配備されている場合にのみ該当します。

AWS KMS (Key Management Service) を使用して CloudPoint の構成情報を暗号化および復号するように CloudPoint を構成する場合は、次の手順を実行します。CloudPoint は、CloudPoint 環境内で AWS KMS を構成するために使用できる REST API を提供します。

CloudPoint AWS KMS の構成の前提条件

- AWS クラウドの EC2 インスタンスに CloudPoint が正常にインストールされ、構成されていることを確認します。
p.23 の「[CloudPoint のインストール](#)」を参照してください。
- AWS IAM ロールを作成し、CloudPoint EC2 インスタンスに関連付けたことを確認します。
IAM ロールには、少なくとも次のアクセス権が必要です。

```
kms:DescribeKey
kms:GenerateDataKey
kms:Decrypt
```

詳しい手順については、次の AWS KMS のマニュアルを参照してください。

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html#working-with-iam-roles>

- カスタマ管理の CMK (カスタママスターキー) を作成したことを確認します。AWS KMS を CloudPoint で設定するには、CMK のキー ID が必要です。
詳しい手順については、次の AWS KMS のマニュアルを参照してください。
<https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html>

CloudPoint で AWS KMS を構成するには

- 1 次の CloudPoint ID 管理 API を使用して、CloudPoint 管理者ユーザーアカウントの認証トークンを生成します。

```
POST /v4/idm/login
```

CloudPoint インスタンスに接続できるシステムで、次の cURL コマンドを入力します。

```
# curl -k https://<cloudpointhostFQDN>/cloudpoint/api/v4/idm/login  
-X 'POST' -H "Content-Type: application/json" -d  
'{"email":"<username>", "password":"<password>"}'
```

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
<cloudpointhostFQDN>	ホストで CloudPoint の初期構成の実行中に指定された FQDN (完全修飾ドメイン名) を表します。
<username>	初期構成時に CloudPoint 管理者ユーザーとして指定されたユーザー名を表します。
<password>	CloudPoint 管理者ユーザーアカウントのパスワードを表します。

- 2 コマンドプロンプトで、API 出力を確認します。次のような出力が表示されます。

```
{  
  "accessToken":  
    "eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJWZXJpdGFzIiwidXN",  
  "applicationId": "",  
  "applicationPath": "",  
  "errorCode": ""  
}
```

accessToken として表示される英数字エントリは、ホスト上のすべての CloudPoint API 要求を承認するために使用されるトークンを表します。トークンをコピーします。これは、以降の手順で必要になります。

メモ: ここに示す英数字の認証トークンは、表示のみを目的としています。環境内でこのコマンドを実行するときに生成される実際のトークンを使用します。

3 CloudPoint Key Management Service API POST /v4/kms を使用して、新しい AWS KMS 構成を作成します。

同じコマンドプロンプトから、次の cURL コマンドを入力します。

```
# curl -k "https://<cloudpointhostFQDN>/cloudpoint/api/v4/kms"  
-X 'POST' -H "Content-Type: application/json"  
-H "Authorization: Bearer <authtoken>"  
-d '{"platform":"aws", "masterKeyId":"<cmk_keyid>",  
"credentials":{"type":"iamrole",  
"regionname":"<cmk_regionname>"}}'
```

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
<cloudpointhostFQDN>	ホストで CloudPoint の初期構成の実行中に指定された FQDN (完全修飾ドメイン名) を表します。
<authtoken>	前の手順で生成した英数字の認証トークンを表します。
<cmk_keyid>	CloudPoint 用に作成した、AWS カスタマが管理する CMK (カスタママスターキー) のキー ID を表します。
<cmk_regionname>	CloudPoint インスタンスが配備されている CMK リージョンを表します。

- 4 コマンドプロンプトで API 出力を確認し、タスクが完了するまで待機します。
- 5 AWS KMS が正しく設定されているかどうかを、CloudPoint API `GET /v4/kms` を使用して迅速に確認できます。

次の cURL コマンドを実行します。

```
# curl -k -X GET  
"https://<cloudpointhostFQDN>/cloudpoint/api/v4/kms"  
-H "accept: application/json"  
-H "Authorization: Bearer <authtoken>"
```

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
<cloudpointhostFQDN>	ホストで CloudPoint の初期構成の実行中に指定された FQDN (完全修飾ドメイン名) を表します。
<authtoken>	前の手順 2 で生成した英数字の認証トークンを表します。

HTTP 200 状態は、構成が正常に実行されたことを示します。

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。

- [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](#)
- [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

AWS (Amazon Web Services) 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 3-1 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 3-2 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。
領域	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ャルを暗号化します。

CloudPoint が AWS クラウドに配備されている場合:

表 3-3 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	

CloudPoint の構成パラメータ	説明
領域	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。
領域	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ホワイト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。

- 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。

- **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。

現在、CloudPoint では、そのような構成の作成はブロックされていません。プラグインの構成間にクラウド資産の重複がある場合は、プラグインの構成を削除して再度追加し、重複資産が存在しないようにして、構成の問題を解決する必要がある場合があります。

ただし、その構成の資産に関連付けられているスナップショットがある場合、CloudPoint では、プラグインの構成を削除することは許可されません。

- 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/>

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.40 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。
<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。
<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.45 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する必要があります。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.42 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.35 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"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "EC2Recovery",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:AttachNetworkInterface",
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2>DeleteTags",
        "ec2:CreateTags",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:CreateVolume",
        "ec2>DeleteVolume",
        "ec2:DescribeIamInstanceProfileAssociations",

```

```

        "ec2:AssociateIamInstanceProfile",
        "ec2:AssociateAddress",
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:RestoreSecret",
        "secretsmanager:PutSecretValue",
        "secretsmanager>DeleteSecret",
        "secretsmanager:UpdateSecret"
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "SNS",
    "Effect": "Allow",
    "Action": [
        "sns:Publish",
        "sns:GetTopicAttributes"
    ],
    "Resource": [
        "arn:aws:sns:*:*:*"
    ]
}
]
}

```

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。

Create role

Select type of trusted entity

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID* 165323042987

Options ☐ Require external ID (Best practice when a third party will assume this role)
☐ Require MFA

- 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。

Summary

Policy ARN: arn:aws:iam::165323042987:policy/cp-pun-test-policy
 Description: To test EC2 permission template required for GP.

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

The 'Trust relationships' tab is selected, showing a single trusted entity:

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

The 'Conditions' section indicates 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。

The screenshot shows the AWS IAM console 'Summary' page for a role named 'CP_Role'. The role's ARN is 'arn:aws:iam::165323042987:role/CP_Role'. The role description is 'CP Role'. The instance profile ARN is 'arn:aws:iam::165323042987:instance-profile/CP_Role'. The path is '/'. The creation time is '2018-06-13 23:16 UTC+0930'. The maximum CLI/API session duration is '1 hour'. The 'Permissions' tab is selected, showing 'Permissions policies (2 policies applied)'. The policies listed are 'CP_Policy' (Managed policy) and 'Assume_Role_CP_CROSS_AC_ROLE' (Inline policy). The 'Assume_Role_CP_CROSS_AC_ROLE' policy is expanded, showing its JSON content:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::935928673755:role/CP_CROSS_AC_ROLE"
    }
  ]
}
```

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yal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 3-4 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 3-5 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。

現在、CloudPoint では、そのような構成の作成はブロックされていません。プラグインの構成間にクラウド資産の重複がある場合は、プラグインの構成を削除して再度追加し、重複資産が存在しないようにして、構成の問題を解決する必要がある場合があります。

ただし、その構成の資産に関連付けられているスナップショットがある場合、CloudPoint では、プラグインの構成を削除することは許可されません。

p.50 の「[CloudPoint で必要な Google Cloud Platform アクセス権](#)」を参照してください。

p.52 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.53 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.50 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.48 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
¥
/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 CloudPoint 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
.
.
.
weT9odE4ry181tNU¥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 3-6 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	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	アプリケーション ID。
シークレットキー	アプリケーションのシークレットキー。
地域	クラウド資産を検出する 1 つ以上の地域。 メモ: 行政クラウドを設定する場合は、US Gov アリゾナ、US Gov テキサス、または US Gov バージニアを選択します。
リソースグループの接頭辞	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い場合でも資産を保護する	このチェックボックスで、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が決まります。

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、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 クラウド環境の資産のスナップショットのタグ付けはサポートされていません。Azure では、スナップショットごとに最大 15 個のタグがサポートされていますが、API を使用して手動で、または CloudPoint を使用して保護ポリシーを介して、スナップショットにタグを割り当てることはできません。
- 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。
現在、CloudPoint では、そのような構成の作成はブロックされていません。プラグインの構成間にクラウド資産の重複がある場合は、そのようなプラグインの構成を削除して再度追加し、重複資産が存在しないようにして、構成の問題を解決する必要があります。
ただし、その構成の資産に関連付けられているスナップショットがある場合、CloudPoint では、プラグインの構成を削除することは許可されません。
- 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。また、CloudPoint 2.2.1 以降で作成されたスナップショットの[既存のリストアを上書き (Overwrite existing restore)]オプションも無効になります。
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、たとえばインプレース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。したがって、NetBackup 2.2.1 リリースにアップグレードした場合は、古いバージョンの CloudPoint を使用して作成されたスナップショットでは[既存のリストアを上書き (Overwrite existing restore)]オプションは利用できません。
- 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

場所	リージョン
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 (ソプリン) ■ ドイツ北東部 (ソプリン)

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ロール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ロールの定義を、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/images/write",
    "Microsoft.Compute/images/delete",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Compute/snapshots/write",
    "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.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ロールを作成するには、次の Azure マニュアルの手順に従ってください。

<https://docs.microsoft.com/en-us/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ロールを作成するには、次の Azure マニュアルの手順に従ってください。

<https://docs.microsoft.com/en-us/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: ロールを作成する前に、以前に指定されたロール定義 (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、ReaderSupportRole.json は、ロール定義テキストを含んでいる入力ファイルとして使用されます。

このロールを使用するには、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ロールを割り当てます。
- 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.54 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。

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 マスターサーバーに 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。

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。

- [NetApp プラグインの構成に関する注意事項](#)
- [Nutanix Files プラグインの構成に関する注意事項](#)
- [Dell EMC Unity アレイプラグインの構成パラメータ](#)
- [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](#)
- [Hitachi 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](#)
- [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 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.61 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.62 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 4-1 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 4-2 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 false に設定されている LUN だけが検出されます。 ["state": "online", "vol_type": "rw", "is_snapshot_auto_delete_enabled": "false"] 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 の配備では、CloudPoint は NetApp ストレージ上のすべての NFS 共有を検出します。 CloudPoint で共有の検出を可能にするには、共有にアクティブな junction_path が構成されている必要があります。
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。

CloudPoint 操作	説明
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。
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。

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対する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なりました。**CloudPoint** を構成し、ネットワークファイルシステム (NFS) 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 **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機能ロジックが含まれています。**NetBackup** マスターサーバーでこのプラグインを設定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、バックアップする必要がある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 @: l-mock.veritas.com

CloudPoint Server: l-mock.veritas.com

Selected Plugin: Nutanix Files

Credentials

Enter Plugin ID:
PUNE_NUTANIX_FILES_01

File Server FQDN:
l-mock.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 4-3 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.65 の「[Nutanix Files プラグイン構成の前提条件](#)」を参照してください。

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 4-4 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	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 4-5 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

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

- 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。

- スナップショットのエクスポート
スナップショットをエクスポートすると、CloudPoint はターゲットホストにスナップショットを接続し、エクスポート ID を使用してそのスナップショットを追跡します。
- スナップショットのデポート
スナップショットをデポートすると、CloudPoint はエクスポートされたスナップショットをターゲットホストから切断し、エクスポート ID を削除します。
- 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 4-6 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 4-7 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
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.74 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.74 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.74 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 4-8 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 4-9 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 4-10 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 4-11 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。
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。

CloudPoint 操作	説明
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。
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。

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、ストレージレイと通信します。
- Hitachi ストレージ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.78 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.78 の「[サポート対象の Hitachi ストレージレイ](#)」を参照してください。

p.79 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 4-12 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 4-13 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.11 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 4-14 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。
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。

CloudPoint 操作	説明
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)

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.81 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.81 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 4-15 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 4-16 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 MASTER 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)

CloudPoint ストレージ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 マスターサーバーに 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。

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ライブ](#)
- [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](#)

- **MongoDB** のリストアの要件および制限事項
- **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
- **MongoDB** スナップショットのリストア後に必要な追加手順
- **Oracle** スナップショットのリストア後に必要な追加手順
- **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。

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回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。

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.11 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.101 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.11 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

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。

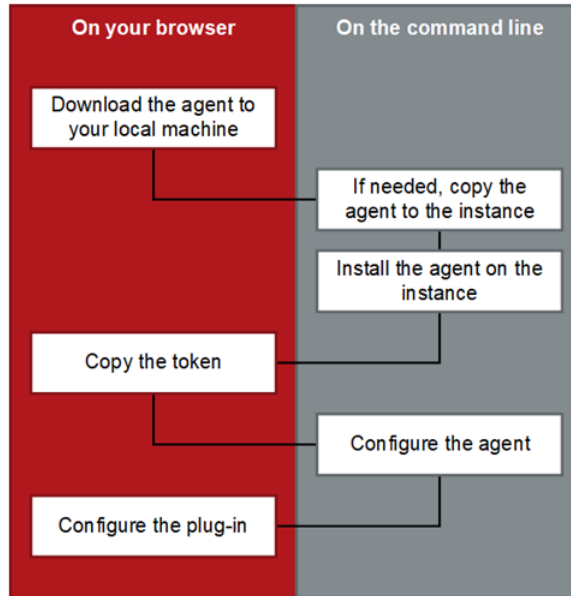
表 5-1 MongoDB プラグインの構成パラメータ

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。

図 5-1 CloudPoint エージェントのインストールと構成の処理



p.90 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.90 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.91 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.88 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.89 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.22 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。

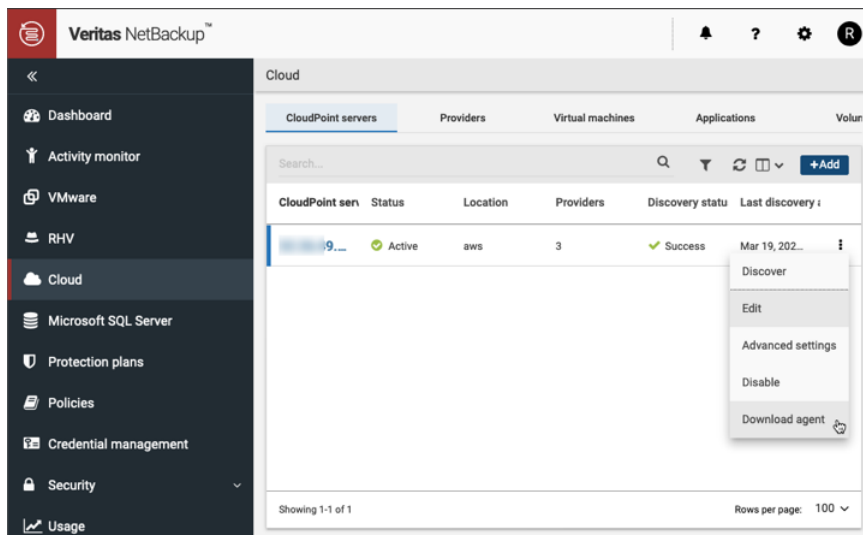
このセクションで説明されている手順を実行する前に、次の操作を行います。

- 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.90 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.90 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、マスター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。

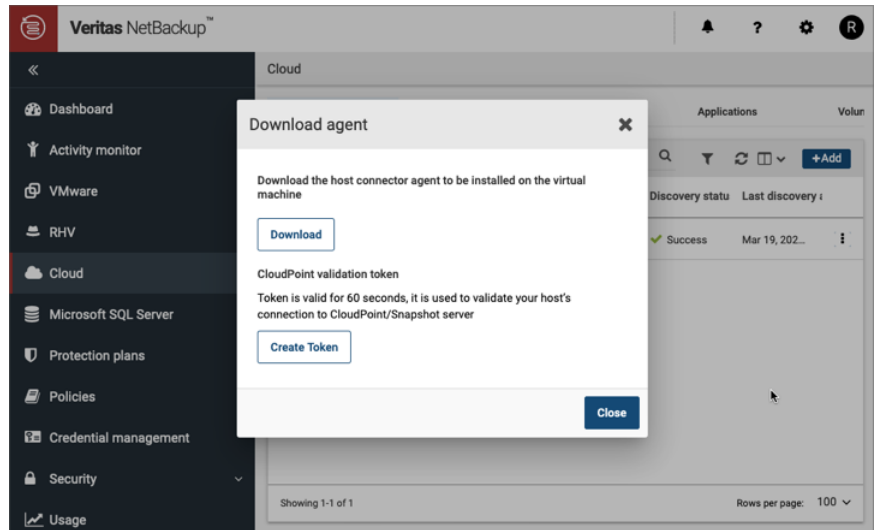
- 3 目的の CloudPoint サーバー行で、右側の処理ボタンをクリックし、次に[エージェントをダウンロード (Download agent)]を選択します。



- 4 [エージェントをダウンロード (Download agent)] ダイアログボックスで、[ダウンロード (Download)] 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 [エージェントをダウンロード (Download 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、[エージェントをダウンロード (Download 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。

```
msiexec /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.94 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.97 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.91 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.161 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.91 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>.
```

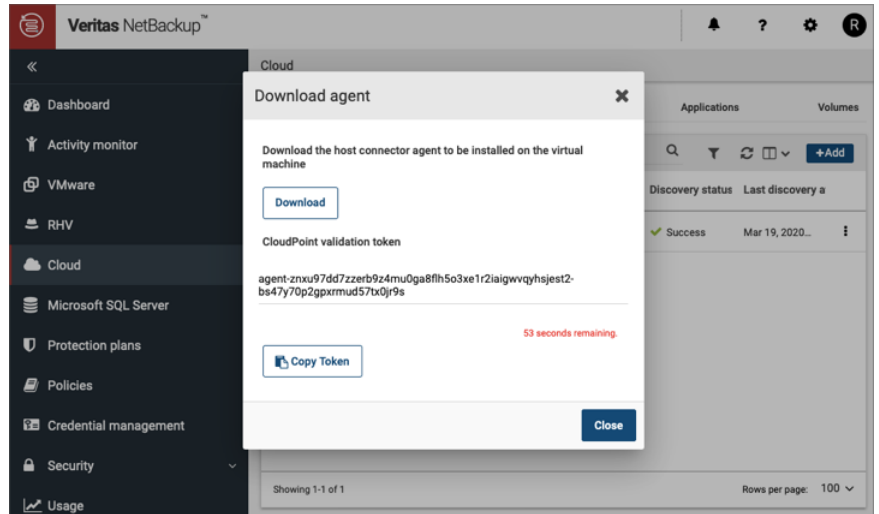
Linux ベースのエージェントを登録するには

- 1 NetBackup Web UI に戻り、[エージェントをダウンロード (Download 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[エージェントをダウンロード (Download agent)]を選択します。

- [エージェントをダウンロード (Download 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。



メモ: トークンは 60 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、[エージェントをダウンロード (Download 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.100 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.91 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。

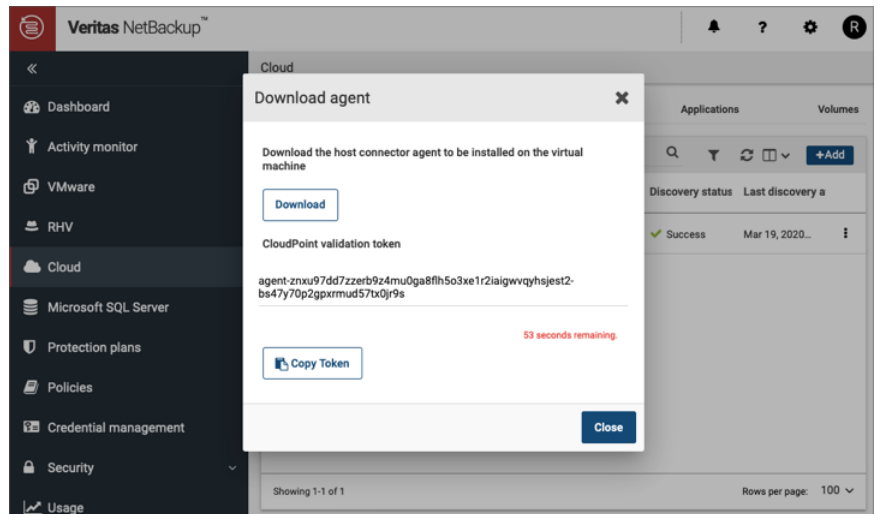
Windows ベースのエージェントを登録するには

- 1 NetBackup Web UI に戻り、[エージェントをダウンロード (Download 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[エージェントをダウンロード (Download agent)]を選択します。
 - [エージェントをダウンロード (Download 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。



メモ: トークンは 60 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、[エージェントをダウンロード (Download 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.100 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.94 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.97 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.87 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.89 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.86 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。
 - 計画の名前と説明を入力します。
 - [サポート対象の作業負荷 (Supported workload)] で、[クラウド (Cloud)] を選択します。
 - [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.103 の「[NetBackup 保護計画へのクラウド資産のサブスクリプション](#)」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プション

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プションできます。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て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。

続行する前に、NetBackup Web UI から保護計画に資産を割り当てす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プションするには

- 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。

- **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斷してから、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、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
- 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 5-2 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.119 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。
 - **AWS** または **GCP** プラグイン構成からリージョンまたはゾーンを削除すると、そのリージョンまたは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リストア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リストア操作を再開できます。
- p.107 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.108 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.109 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.110 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.110 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.118 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.110 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.115 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.110 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.122 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と、次のエラーが表示されます。
`*flexsnap.GenericError: 資産を保護できません* (*flexsnap.GenericError: Unable to protect asset *)`

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.121 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。

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、スタンドアロンの 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

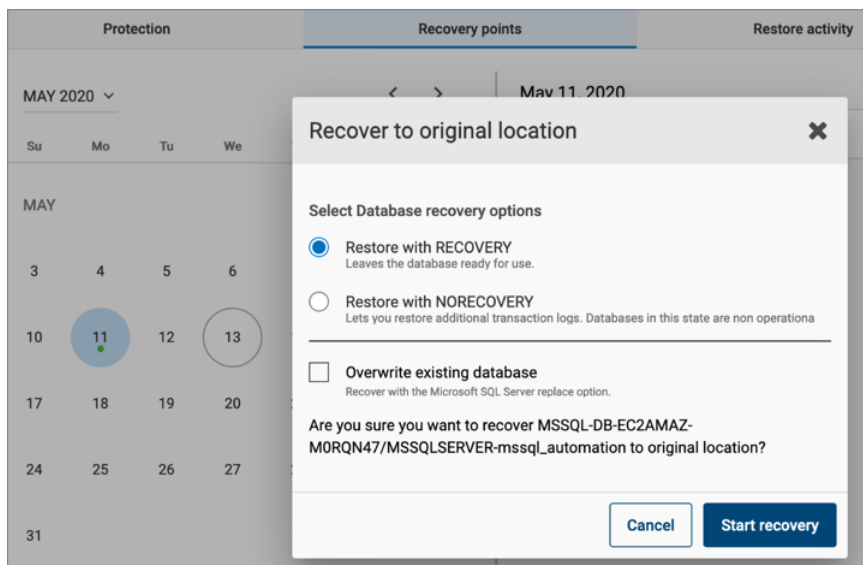
- 1 NetBackup Web UI にサインインします。
- 2 左側のナビゲーションペインで、[作業負荷 (Workloads)]、[クラウド (Cloud)]の順にクリックし、次に[アプリケーション (Applications)]タブを選択します。

- 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、スタンドアロンの 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。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、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願いします。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、しばらく待つてから、`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。

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。

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
```

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オンし、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](#)
- [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](#)
- [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、SSH 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自身がホストから削除されます。

現在、CloudPoint エージェントレス機能は Linux ファイルシステム資産、Oracle データベース、および MongoDB データベース資産を検出して動作します。エージェントレス機能は Microsoft Windows または Windows ベースのアプリケーションではサポートされません。

p.126 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.127 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

エージェントレス機能を構成する前に、次の操作を実行します。

- 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

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。
- 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。

p.126 の「[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](#)」を参照してください。

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詳しくは、オペレーティングシステムまたは配布に固有のマニュアルを参照してください。

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。

1. 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。
2. 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。
3. visudo コマンドを使用して、/etc/sudoers ファイルを編集します。

- ```
sudo visudo
```
4. `/etc/sudoers` ファイルに次のエントリを追加します。  
  
`hostuserID ALL=(ALL) NOPASSWD: ALL`
  5. `/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
```

6. 変更を `/etc/sudoers` ファイルに保存します。
7. **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。
8. 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。

## エージェントレス機能の構成

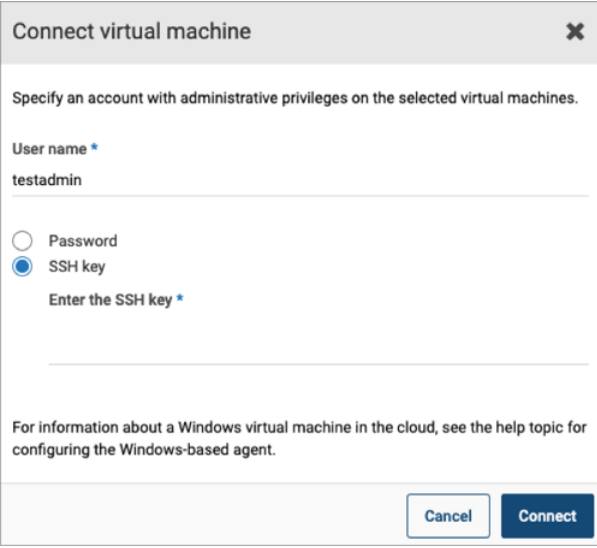
**CloudPoint** エージェントレス機能を構成する前に、すべての前提条件を確認します。

p.126 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。





- 4 [接続 (Connect)] ダイアログボックスで、SSH キーオプションを選択します。



The image shows a 'Connect virtual machine' dialog box. It has a title bar with a close button (X). The main content area contains the instruction 'Specify an account with administrative privileges on the selected virtual machines.' Below this is a 'User name \*' field with the text 'testadmin' entered. There are two radio button options: 'Password' (unselected) and 'SSH key' (selected). Below the 'SSH key' option is a label 'Enter the SSH key \*' followed by an empty text input field. At the bottom of the dialog, there is a note: 'For information about a Windows virtual machine in the cloud, see the help topic for configuring the Windows-based agent.' At the very bottom, there are two buttons: 'Cancel' and 'Connect'.

- 5 SSH ユーザー名と SSH キーを入力します。
- 6 [接続 (Connect)] をクリックします。

# CloudPoint のメンテナンス

- [第7章 CloudPoint のログ](#)
- [第8章 CloudPoint のトラブルシューティング](#)
- [第9章 CloudPoint のアップグレード](#)
- [第10章 CloudPoint のアンインストール](#)

# 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](#)

## 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/fluvent/fluvent.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/fluvent/fluvent.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/fluent/fluent.conf` 構成ファイルを開き、内容を編集してプラグイン定義を追加または削除します。
- 2 ファイルに対するすべての変更を保存します。
- 3 `flexsnap-fluentd` コンテナサービスを次のコマンドを使用して再起動します。

```
sudo docker restart flexsnap-fluentd
```

変更がすぐに有効になり、変更後に生成される新しいログメッセージにのみ適用されることに注意してください。ファイルの変更は、構成ファイルが更新される前に生成された古いログには適用されません。

## 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 7-1 CloudPoint ログファイル

ログ	説明
/cloudpoint/logs/flexsnap.log	このログファイルには、すべての製品ログが含まれています。
/cloudpoint/logs/flexsnap-cloudpoint.log	このログファイルには、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。
/cloudpoint/logs/flexsnap-ipv6config	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。

# 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 の再起動](#)
- [CloudPoint ログ記録のトラブルシューティング](#)
- 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
- [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
- [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

## 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。

---

**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 を再起動するには

- ◆ 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:** 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 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。

```
sudo cat /cloudpoint/logs/flexsnap.log | grep <flexsnap-service
name>
```

CloudPoint バージョン 2.2.x からアップグレードする場合は、次の点を考慮してください。

- Docker コマンド (# sudo docker exec flexsnap-coordinator flexsnap-log) を使用して CloudPoint ログを取得できません。このコマンドを実行すると、次のエラーメッセージが表示されます。

flexsnap-log は非推奨です。(flexsnap-log is deprecated.)

/cloudpoint/logs/flexsnap.log からの現在のログを取得します (Retrieve current logs from /cloudpoint/logs/flexsnap.log)

- 次のコマンドを実行すると、すべてのログを MongoDB データベースからディスク上のファイルに取り込むことができます。

```
sudo docker exec flexsnap-coordinator flexsnap-log --file
/cloudpoint/logs/<previousversion_logs>.log
```



- ログが原因で、MongoDB データベースでより多くのディスク領域を使用している場合は、次のコマンドを使用してデータベースを破棄できます。  
# sudo docker exec flexsnap-coordinator flexsnap-log --purge

## 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.a1f2ac945cd844e393c9876f347bd817' in vhost '/'
```

この問題は、エージェントホストが突然シャットダウンされた場合でも、エージェントと 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.97 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.135 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 マスターが作成された後で新しい NBU UUID とバージョン番号を更新する必要があります。

- このタスクを実行するためには、**NetBackup** 管理者が **NetBackup Web** 管理サービスにログインしている必要があります。次のコマンドを使用してログオンします。

```
/usr/opensv/netbackup/bin/bpnbat -login -loginType WEB
```

- マスター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 < Master
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 <Master Server
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>
```

# 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](#)

## 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 9-1 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
2.2.x	8.3

NetBackup バージョン 8.3 以降は、CloudPoint 8.3 でのみ機能します。以前のバージョンの CloudPoint はサポートされていません。

## アップグレードのシナリオ

次の表に、CloudPoint の配備とアップグレードのさまざまなシナリオを示します。

表 9-2 導入シナリオ

シナリオ	説明	処理
スタンドアロン	CloudPoint はクラウド資産と構成を管理します。	NetBackup によって管理される CloudPoint サーバーを移行する必要があります。 <a href="https://www.veritas.com/support/en_US">https://www.veritas.com/support/en_US</a> でサポートケースを開くか、 <a href="https://www.veritas.com/content/support/en_US/contact-us">https://www.veritas.com/content/support/en_US/contact-us</a> で地域に該当する電話番号から、ベリタステクニカルサポートにお問い合わせください。
NetBackup と CloudPoint	■ NetBackup は、オンプレミスのストレージアレイ資産と構成を管理します。    ■ NetBackup はクラウド資産とクラウドの構成を管理します。	サーバーをアップグレードできます。 p.142 の「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 8.3 の要件を満たしていることを確認します。  
p.11 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、/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.156 の「CloudPoint のバックアップ」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。

**NetBackup バージョン 8.2.x 以前で登録されている CloudPoint サーバーをアップグレードするには**

- 1 NetBackup マスターサーバーで、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`
  - 2 CloudPoint をサポート対象の最新バージョンにアップグレードします。
  - 3 NetBackup マスターサーバーをアップグレードします。
- 詳しくは、『Veritas NetBackup アップグレードガイド』を参照してください。
- 4 NetBackup プロセスを再起動します。
  - 5 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、NetBackup の構成を更新します。

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。
  - [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 マスターサーバーで、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>
```

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 マスターサーバーへの PATCH API 呼び出しを行います。

`https://nbu-master/netbackup/config/servers/snapshot-mgmt-servers/cp-hostname`

## NetBackup に登録されていない 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_8.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 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 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。

```
Load -i VRTScloudpoint-docker-8.3.0.8549.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:8.3.0.8549
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:8.3.0.8549
```



```
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:8.3.0.8549
Loaded image: veritas/flexsnap-fluentd:8.3.0.8549
60b2acb680f6: Loading layer [=====>]
3.584kB/3.584kB
f595300c08bc: Loading layer [=====>]
3.584kB/3.584kB
Loaded image: veritas/flexsnap-mongodb:8.3.0.8549
Loaded image: veritas/flexsnap-agent:8.3.0.8549
Loaded image: veritas/flexsnap-scheduler:8.3.0.8549
8df81d5ea017: Loading layer [=====>]
7.68kB/7.68kB
7d0351be3c82: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-nginx:8.3.0.8549
2ab7b82b7b67: Loading layer [=====>]
433.6MB/433.6MB
cb5786a5d4da: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-coordinator:8.3.0.8549
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:8.3.0.8549
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:8.3.0.8549
7eb7d2ecf33a: Loading layer [=====>]
12.92MB/12.92MB
4cbef47218cf: Loading layer [=====>]
3.072kB/3.072kB
Loaded image: veritas/flexsnap-certauth:8.3.0.8549
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:8.3.0.8549
Loaded image: veritas/flexsnap-notification:8.3.0.8549
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:8.3.0.8549

Loaded image: veritas/flexsnap-cloudpoint:8.3.0.8549
```

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 **2.2.2.4722** 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:2.2.2.4722 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-onhostagent ...done
Stopping container: flexsnap-email-service ...done
Stopping container: flexsnap-identity-manager-service ...done
Stopping container: flexsnap-notification ...done
Stopping container: flexsnap-cloudpointconsole ...done
Stopping container: flexsnap-policy ...done
Stopping container: flexsnap-licensing ...done
Stopping container: flexsnap-telemetry ...done
Stopping container: flexsnap-indexingsupervisor ...done
Stopping container: flexsnap-vic ...done
Stopping container: flexsnap-scheduler ...done
Stopping container: flexsnap-agent ...done
Stopping container: flexsnap-coordinator ...done
Stopping container: flexsnap-api ...done
Stopping container: flexsnap-api-gateway ...done
Stopping container: flexsnap-auth ...done
```

```
Stopping container: flexsnap-authorization-service ...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:8.3.0.8549 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: Wed Apr 1 14:37:53 UTC 2020
WARNING: No swap limit support
Docker server version: 18.09.1
This is an upgrade to CloudPoint 8.3.0.8549
Previous CloudPoint version: 2.2.2.4722
Checking if a 1.0 release container exists ...
Removing exited container flexsnap-cloudpointconsole ...done
Removing exited container flexsnap-api ...done
Removing exited container flexsnap-fluentd ...done
Removing exited container flexsnap-authorization-service ...done
Removing exited container flexsnap-email-service ...done
Removing exited container flexsnap-identity-manager-service
...done
Removing exited container flexsnap-licensing ...done
Removing exited container flexsnap-vic ...done
Removing exited container flexsnap-telemetry ...done
Removing exited container flexsnap-indexingsupervisor ...done
Removing exited container flexsnap-policy ...done
Removing exited container flexsnap-scheduler ...done
Removing exited container flexsnap-onhostagent ...done
Removing exited container flexsnap-notification ...done
Removing exited container flexsnap-agent ...done
Removing exited container flexsnap-coordinator ...done
Removing exited container flexsnap-mongodb ...done
Removing exited container flexsnap-rabbitmq ...done
Removing exited container flexsnap-api-gateway ...done
Removing exited container flexsnap-auth ...done
Deleting network : flexsnap-network ...done
Generating certificates for MongoDB server ...done
Generating certificates for API-gateway container ...done
```

```
Generating certificates for few other service container ...done
Generating certificates for OnhostAgent container ...done
Adding MongoDB certificate to the trust store ...
Importing keystore /cloudpoint/keys/idm_store to
/cloudpoint/keys/.idm_store_tmp...
Entry for alias cacert successfully imported.
Entry for alias mongodb successfully imported.
Import command completed: 2 entries successfully imported,
0 entries failed or cancelled
done
Renewing IDM https certificates ...done
Starting to generate nginx ssl configuration ...done
Creating network: flexsnap-network ...done
Starting docker container: flexsnap-fluentd ...done
Starting docker container: flexsnap-mongodb ...done
Starting docker container: flexsnap-rabbitmq ...done
Starting docker container: flexsnap-certauth ...done
Starting docker container: flexsnap-api-gateway ...done
Starting docker container: flexsnap-coordinator ...done
Starting docker container: flexsnap-agent ...done
Starting docker container: flexsnap-onhostagent ...done
Starting docker container: flexsnap-scheduler ...done
Starting docker container: flexsnap-policy ...done
Starting docker container: flexsnap-notification ...done
Starting docker container: flexsnap-idm ...done
Starting docker container: flexsnap-config ...done
Starting docker container: flexsnap-nginx ...done
```

- 8** CloudPoint のバージョンを検証するには、次のコマンドを実行します。

```
sudo docker ps | grep flexsnap-coordinator
```

- 9** 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。

- 10** CloudPoint サーバーを NetBackup マスターサーバーに登録します。

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。

- 11** 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。

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)]、[エージェントをダウンロード (Download 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)]、[エージェントをダウンロード (Download 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)]、[エージェントをダウンロード (Download 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)]、[エージェントをダウンロード (Download 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.91 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。

- 12 AWS クラウドの EC2 インスタンスに NetBackup を配備している場合、NetBackup の構成を暗号化および復号するために AWS KMS サービスを使用するように NetBackup を構成するオプションが利用できるようになりました。**

これは省略可能な手順であり、NetBackup 配備がデフォルトの暗号化メカニズムを使用していて、AWS KMS がその環境でまだ設定されていない場合にのみ適用できます。

- 13 CloudPoint が AWS クラウドに配備され、Veritas NetBackup 環境に統合されている場合、次の手順では、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 NetBackup の構成を更新します。**

この手順を実行すると、CloudPoint の AWS IAM 構成設定が NetBackup 構成内で更新されるようになります。

次のいずれかの操作を実行します。

- NetBackup Web UI から、CloudPoint サーバーの情報を追加します。
  - 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。
  - 右側の[追加 (Add)]ボタンをクリックし、[CloudPoint サーバーを追加 (Add CloudPoint server)]ダイアログボックスで、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。
  - [追加 (Add)]をクリックして、CloudPoint サーバーの構成を追加します。



- または、NetBackup マスターサーバー上で次のコマンドを実行します。

```
./tpconfig -add -cloudpoint_server <cloudpoint_server_name>
-cloudpoint_server_user_id <user_ID> -manage_workload
manage_workload [-requiredport <IP_port_number>]
```

たとえば、CloudPoint ホスト名が mycphost.mydomain.dom で、構成されている CloudPoint 管理者ユーザーが mycpuser@mycp.com である場合、コマンドの構文は次のようになります。

```
./tpconfig -add -cloudpoint_server mycphost.mydomain.com
-manage_workload manage_workload -cloudpoint_server_user_id
mycpuser@mycp.com
```

メッセージが表示されたら、前のコマンドで指定した CloudPoint ユーザーのパスワードを入力し、確認のためにパスワードを再度入力します。
- または、次の URL を使用して NetBackup マスターサーバーへの PATCH API 呼び出しを行います。

<https://nbu-master/netbackup/config/servers/snapshot-mgmt-servers/>

NetBackup 構成が更新されたら、すぐに CloudPoint の使用を NetBackup で開始できます。CloudPoint がアップグレードされると、資産の検出が再びトリガされます。プラグイン、資産、スナップショット、リストア、およびレプリケーションジョブなどの、すべての既存の CloudPoint 構成設定は保持され、そのまま機能し続けます。新しい AWS リージョンを追加すると、そのリージョン内の資産の検出と操作の実行に、AWS IAM が使用されます。

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 と Veritas NetBackup の統合について詳しくは、『Veritas NetBackup Web UI クラウド管理者ガイド』を参照してください。

[https://www.veritas.com/support/en\\_US/article.100040135](https://www.veritas.com/support/en_US/article.100040135)

---

**メモ:** HPE 3PAR などの、非推奨のプラグイン構成を削除せずに NetBackup をアップグレードすると、アップグレード後に NetBackup の UI にサインインできない場合があります。NetBackup データベースから非推奨のプラグインエントリを消去し、NetBackup の配備を起動して実行するサポートについては、Veritas テクニカルサポートにお問い合わせください。

---

# 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 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.161 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.156 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ます。これらの資産は NetBackup UI には表示されなくなります。たとえば、CloudPoint SQL プラグインを構成解除すると、CloudPoint によって検出されたすべての SQL インスタンスが削除され、NetBackup UI に表示されなくなります。
- ホストからプラグインを構成解除すると、そのホストに属するファイルシステム資産のみが検出され、UI に表示されます。

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。これらの資産は NetBackup UI には表示されなくなります。



### 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.159 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.161 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.162 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.161 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.23 の「[CloudPoint のインストール](#)」を参照してください。

# 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.19 の「[Docker 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。