

NetBackup™ Web UI Microsoft SQL Server 管理 者ガイド

リリース 10.4

最終更新日: 2024-05-14

法的通知と登録商標

Copyright © 2024 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、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、Veritas 社がサードパーティへの帰属を示す必要があるサードパーティ製ソフトウェア（「サードパーティ製プログラム」）が含まれる場合があります。サードパーティプログラムの一部は、オープンソースまたはフリーソフトウェアライセンスで提供されます。本ソフトウェアに含まれる本使用許諾契約は、オープンソースまたはフリーソフトウェアライセンスでお客様が有する権利または義務を変更しないものとします。このVeritas製品に付属するサードパーティの法的通知文書は次の場所から入手できます。

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

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

本書は、現状のままで提供されるものであり、その商品性、特定目的への適合性、または不侵害の暗黙的な保証を含む、明示的あるいは暗黙的な条件、表明、および保証はすべて免責されるものとします。ただし、これらの免責が法的に無効であるとされる場合を除きます。Veritas Technologies LLC およびその関連会社は、本書の提供、パフォーマンスまたは使用に関連する付随的または間接的損害に対して、一切責任を負わないものとします。本書に記載の情報は、予告なく変更される場合があります。

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

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、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次の Web サイトにアクセスしてください。

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

次の URL で 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。

世界共通 (日本を除く)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

マニュアル

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

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

マニュアルに対するご意見

お客様のご意見は弊社の財産です。改善点のご指摘やマニュアルの誤謬脱漏などの報告をお願いします。その際には、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。ご意見は次のアドレスに送信してください。

NB.docs@veritas.com

次の Veritas コミュニティサイトでマニュアルの情報を参照したり、質問したりすることもできます。

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

第 1 章	NetBackup for SQL Server について	8
	NetBackup for SQL Server の概要	8
	NetBackup for SQL Server の詳細な機能	9
第 2 章	インストールとホストの構成	11
	NetBackup for SQL Server のインストールの計画	11
	NetBackup サーバーおよびクライアントの要件	12
	NetBackup クラスタ内で NetBackup for SQL Server を使用するた めの要件	13
	NetBackup for SQL Server のライセンス	14
	SQL Server ホストとユーザー権限の構成	14
	vSphere 用の Veritas VSS プロバイダのインストール	15
	SQL Server VSS Writer サービスの無効化	16
	SQL Server のバックアップとリストアのための NetBackup サービスの設定	17
	SQL Server のローカルセキュリティの権限の構成	18
	自動検出されたマッピングの確認	19
	分散アプリケーション、クラスタ、または仮想マシンのリストアマッピングの設 定	27
	ODBC 接続の構成	28
	非表示の NetBackup for SQL Server の読み取り不可セカンダリインスタ ンスの構成	30
	SQL Server エージェントのプライマリサーバーホスト名の構成	31
	バックアップ操作を許可するジョブ数の設定	32
	1 クライアントあたりの最大ジョブ数の構成	33
第 3 章	SQL Server 管理者用の RBAC の構成	35
	SQL Server 管理者の RBAC の役割	35
	SQL Server ジョブと VMware ジョブを表示および管理するために必要な RBAC 権限	36

第 4 章	SQL Server の検出とクレデンシャルの管理	37
	SQL Server オブジェクトの検出について	37
	高度可用性グループまたは基本可用性グループのオンデマンドの検出	38
	オンデマンドでのデータベースの検出	38
	読み取りスケール可用性グループの検出	39
	SQL Server インテリジェントポリシーで使用するクレデンシャルについて	
	SQL Server クレデンシャルについて	39
	SQL Server 用のクレデンシャルの追加	41
	SQL Server インスタンスまたはレプリカのクレデンシャルの選択	42
	資産に適用されているクレデンシャル名の表示	43
	指定したクレデンシャルの編集または削除	43
	SQL Server インスタンスの削除	44
	SQL Server インスタンスの手動での追加	45
第 5 章	SQL Server の保護計画の管理	46
	SQL Server 可用性グループの保護について	46
	SQL Server 資産を保護するための保護計画の作成	47
	スケジュール	50
	パフォーマンスチューニングおよび設定のオプション	51
	保護計画への SQL Server 資産の追加	56
	Microsoft SQL Server 資産の保護設定のカスタマイズ	58
	SQL Server 資産の保護の削除	59
	NetBackup ドメインをまたぐ SQL Server 可用性グループの保護	60
第 6 章	Snapshot Client を使用するバックアップポリシーの構成	63
	SQL Server 用の NetBackup Snapshot Client について	63
	Snapshot Client を使用した SQL Server の操作	64
	スナップショット方式	66
	SQL Server スナップショットおよびインスタントリカバリバックアップの構成要件	67
	SQL Server のスナップショットポリシーの構成	68
	SQL Server のインスタントリカバリバックアップ用のポリシーの構成	70
	コピーのみのスナップショットバックアップによる差分バックアップの影響	72
	コピーのみのバックアップの作成 (レガシー SQL Server ポリシー)	73
	コピーのみではないインスタントリカバリバックアップの作成 (レガシー SQL Server ポリシー)	73
	SQL Server エージェントのグループ化スナップショットについて	74

	グループ化バックアップされたデータベースのリストア	75
第 7 章	SQL Server の資産の詳細の表示	76
	SQL Server 資産の参照	76
	データベース、インスタンス、可用性グループの保護状態の表示	78
第 8 章	SQL Server のリストア	80
	SQL Server のリストアの要件	80
	完全データベースリカバリの実行	81
	1 つのリカバリポイントのリカバリ	84
	SQL Server のリストアオプション	87
	データベースのリストア (管理者以外のユーザー)	88
	リカバリ用の別のバックアップコピーの選択	89
	SQL Server 可用性データベースのセカンダリレプリカへのリストア	92
	SQL Server 可用性データベースのプライマリレプリカとセカンダリレプリカ へのリストア	94
第 9 章	SQL Server でのインスタントアクセスの使用	97
	インスタントアクセス SQL Server データベースを構成する場合の前提条 件	97
	インスタントアクセスのハードウェアと構成の必要条件	99
	インスタントアクセスデータベースを設定する前の考慮事項	99
	SQL Server インスタントアクセス用の Samba ユーザーの構成	100
	インスタントアクセスデータベースの構成	104
	インスタントアクセスデータベースのライブマウントの詳細の表示	106
	インスタントアクセスデータベースの削除	107
	NetBackup for SQL Server インスタントアクセスのオプション	107
	NetBackup for SQL Server の用語	109
	よく寄せられる質問	109
第 10 章	VMware バックアップを使用した SQL Server の保 護	115
	VMware バックアップを使用したアプリケーションデータベースの保護につ いて	115
	VMware アプリケーションバックアップの制限事項	117
	SQL Server を保護する NetBackup for VMware バックアップの構成につ いて	118
	SQL Server を保護する VMware バックアップポリシーの構成	119
	スナップショットレプリケーションの管理に Replication Director を使用して SQL Server を保護するための VMware ポリシーの構成	121

SQL Server データを保護するための VMware バックアップを使用した保護計画の作成	123
バックアップオプション (Backup options) と詳細オプション (Advanced options)	126
バックアップからのディスクの除外	127
スナップショットの再試行オプション (Snapshot retry options)	128
VMware バックアップを使用した SQL Server データの保護	129
VMware バックアップからの SQL Server データベースのリストア	130

第 11 章

処理速度とトラブルシューティング	131
NetBackup for SQL Server のパフォーマンスに影響を与える要素	132
SQL Server のトラブルシューティング用のデバッグログについて	135
NetBackup for SQL Server クライアントのデバッグレベルの設定	136
Veritas VSS プロバイダのログ	137
クレデンシャルの検証に関するトラブルシューティング	138
VMware のバックアップに関するトラブルシューティング	139
SQL Server の VMware バックアップ中に発生する SQL Server のログの切り捨てエラー	141
NetBackup for SQL Server の操作の監視について	142
NetBackup for SQL Server の最大トレースレベルの設定	143
失敗したファイルグループまたはファイルバックアップのレポート	144
大規模な SQL Server データベースのリストアにおけるタイムアウトエラーの最小化について	144
SQL Server の圧縮バックアップイメージを単一のストライプとして、または複数のストライプを含むイメージとしてリストアすると、SQL Server のリストアが失敗する	145
可用性グループクラスタに不正なバックアップイメージが表示される	145
SQL Server のホスト名または SQL Server データベース名の末尾にスペースがあると SQL Server データベースのリストアは状態コード 5 またはエラー (-1) で失敗する	146
SQL Server のホスト名、データベース名、データベース論理名の末尾にスペースがあると移動操作は状態コード 5 またはエラー (-1) で失敗する	146
可用性グループのレプリカを検出または参照できない	147
SQL Server のディザスタリカバリについて	147
SQL Server のディザスタリカバリの準備	147
ディザスタリカバリの後の SQL Server のデータベースのリカバリ	148

NetBackup for SQL Server について

この章では以下の項目について説明しています。

- [NetBackup for SQL Server の概要](#)
- [NetBackup for SQL Server の詳細な機能](#)

NetBackup for SQL Server の概要

NetBackup Web UI では、SQL Server データベースのバックアップとリストアの機能が提供されます。次の操作を実行できます。

- 検出されたインスタンス、データベースまたは可用性グループの表示
インスタンスは NetBackup 環境内で自動的に検出されます。
- SQL Server インスタンス、データベース、可用性グループのバックアップ
NetBackup は、次の種類の SQL Server バックアップ方式を提供します。
 - 保護計画
SQL Server 管理者は目的のストレージ、バックアップおよびチューニング設定を含む 1 つ以上の保護計画を選択できます。
 - SQL Server インテリジェントポリシー (SIP)
単一のポリシーで、複数のクライアントにわたる複数の SQL Server インスタンスが保護されます。NetBackup 環境で自動的に検出されるインスタンスのリストからポリシーのインスタンスを選択します。
 - クライアントとバッチファイルを使用したポリシー
これらのポリシーには、SQL Server データベースクライアントのリストとバッチファイルが含まれています。バッチファイルには、バックアップのスケジュール設定時に実行する SQL Server バックアップコマンドが含まれています。

- 保護計画またはポリシーで保護されているデータベースをリストアします。
- バックアップおよびリストア操作の監視

このマニュアルでは、Microsoft SQL Server を SQL Server と記述します。また、NetBackup for Microsoft SQL Server を NetBackup for SQL Server と記述します。

NetBackup for SQL Server の詳細な機能

表 1-1 NetBackup for SQL Server の機能

機能	説明
NetBackup 役割ベースのアクセス制御 (RBAC) との統合	NetBackup Web UI は RBAC の役割を提供し、どの NetBackup ユーザーが NetBackup の SQL Server 操作を管理できるかを制御します。ユーザーは SQL Server 操作を管理するために NetBackup 管理者である必要はありません。ただし、それでもユーザーは Windows 管理者グループのメンバーである必要があり、SQL Server 「sysadmin」の役割が割り当てられている必要があります。
保護計画と SQL Server インテリジェントポリシー	次の利点があります。 ■ 単一の保護計画またはインテリジェントポリシーを使用して、複数の SQL Server インスタンス、インスタンスデータベース、可用性グループ、可用性データベースを保護できます。インスタンスは複数のクライアントに分散できます。 ■ 同じ保護計画またはポリシーに完全、差分、トランザクションログのバックアップを含めることができます。 ■ トランザクションログのバックアップ頻度をスケジュール設定できます。 ■ SQL Server コマンドに関する知識や、パッチファイルを記述して使用する必要はありません。その代わりに、この機能は実行時に自動的にパッチファイルを生成します。
SQL Server 資産の管理	NetBackup は自動的に環境内の SQL Server インスタンスと可用性グループを検出します。また、手動検出を実行できます。 インスタンスまたはレプリカが登録されると、SQL Server 作業負荷管理者は、ポリシーまたは保護計画を使用して SQL Server 資産を保護できます。
認証およびクレデンシャル	SQL Server 保護計画と SQL Server インテリジェントポリシーでは次がサポートされます。 ■ Windows 認証 ■ Windows Active Directory 認証 ■ 適切に構成すると、NetBackup サービスアカウントをクライアント上で SQL Server の特権ユーザーとして実行する必要がなくなります。

機能	説明
バックアップおよびリストア機能	バックアップとリストアでは次の機能を利用できます。 ■ バックアップは、NetBackup サーバーによって中央サイトから完全に管理されます。管理者は、ローカルホストまたはネットワークを介したリモートホスト上のインスタンスに対して、自動的な無人のバックアップを行うスケジュールを設定できます。 ■ NetBackupWeb UI は、1 つのインターフェースからデータベースとトランザクションログのバックアップとリストアをサポートします。 注意: Web UI を使用した SQL Server リカバリでは、SQL Server クライアントがバージョン 8.3 以降である必要があります。 ■ 完全バックアップ、差分バックアップ、トランザクションログバックアップのバックアップスケジュール。 ■ 手動バックアップとコピーのみバックアップ。 ■ 読み書き可能なファイルグループのみのバックアップとリストア。この機能は、ポリシーベースのバックアップを使用して実行できます。 ■ SQL Server クラスタと可用性グループを含む、高可用性 (HA) 環境のサポート。 ■ SQL Server オブジェクトの別の場所へのリストア (リダイレクトリストア)。 ■ バックアップ中に複数のストライプを使用するための機能です。 ■ バックアップのパフォーマンスを改善できるチューニングオプション。
リカバリポイント	Web UI には、さまざまなリカバリ操作を簡単に実行できるリカバリポイントが用意されています。インスタントアクセスが構成されている場合は、リカバリポイントからインスタントアクセスデータベースを作成することもできます。
ストリームベースのバックアップおよびリストア	SQL Server の高速処理が可能な仮想デバイスインターフェースを使用した、ストリームベースでの SQL Server オブジェクトのバックアップとリストア
スナップショットバックアップとインスタントアクセスデータベース	NetBackup では、スナップショット方式を使用して SQL Server のバックアップを実行できます。ポリシーを使用したバックアップでは、オフホストバックアップ、インスタントリカバリ、ハードウェアプロバイダを使用するバックアップも利用可能です。 また、NetBackup バックアップイメージから、インスタントアクセスデータベースを作成できます。データベースは瞬時に利用可能になるため、ほぼゼロのリカバリ時間目標を達成できます。NetBackup は、データベースのスナップショットをバックアップストレージデバイスに直接マウントし、そのスナップショットを通常のデータベースとして扱います。
SQL Server を保護する VMware バックアップのサポート	VMware 保護計画と VMware インテリジェントポリシーは、スナップショットを使用した、VMware コンピュータのアプリケーションの整合性を確保した完全バックアップのサポートを提供します。VMware インテリジェントポリシーは、Replication Director (RD) スナップショットもサポートしています。 NetBackup アクセラレータを使用すると、バックアップの速度を上げられます。
レガシー SQL Server ポリシー	バッチファイルとクライアントリストを使うレガシーバックアップポリシーをサポートします。

インストールとホストの構成

この章では以下の項目について説明しています。

- [NetBackup for SQL Server](#) のインストールの計画
- [SQL Server](#) ホストとユーザー権限の構成
- [SQL Server](#) のバックアップとリストアのための [NetBackup](#) サービスの設定
- [SQL Server](#) のローカルセキュリティの権限の構成
- 自動検出されたマッピングの確認
- 分散アプリケーション、クラスタ、または仮想マシンのリストアマッピングの設定
- [ODBC](#) 接続の構成
- 非表示の [NetBackup for SQL Server](#) の読み取り不可セカンダリインスタンスの構成
- [SQL Server](#) エージェントのプライマリサーバーホスト名の構成
- バックアップ操作を許可するジョブ数の設定
- 1 クライアントあたりの最大ジョブ数の構成

NetBackup for SQL Server のインストールの計画

NetBackup 10.4 の NetBackup for SQL Server に含まれる新しい機能を使用するには、NetBackup for SQL Server クライアントを NetBackup 10.4 にアップグレードします。NetBackup メディアサーバーは NetBackup for SQL Server クライアント以上のバージョンを使用する必要があります。

[表 2-1](#) に、NetBackup for SQL Server を実行するために必要なインストール手順を示します。

表 2-1 NetBackup for SQL Server のインストール手順

手順	処理	説明
手順 1	オペレーティングシステムおよびプラットフォームの互換性を確認します。	NetBackup 互換性リスト を参照してください。
手順 2	プライマリサーバーに NetBackup for SQL Server の有効なライセンス、NetBackup オプション、または使用するアドオンがあることを確認します。	p. 14 の「 NetBackup for SQL Server のライセンス 」を参照してください。
手順 3	バックアップを作成するデータベースが存在するコンピュータに、NetBackup クライアントソフトウェアをインストールします。	p. 12 の「 NetBackup サーバーおよびクライアントの要件 」を参照してください。
手順 4	読み取りスケール可用性グループを保護するには、SQL Server Native Client バージョン 11.0.7462 以降の ODBC ドライバが可用性グループのレプリカにインストールされている必要があります。	このバージョンのドライバを使用すると、読み取りスケール可用性グループのデータベースを検出して参照できます。
手順 5	NetBackup クラスタで NetBackup for SQL Server を使用するには、クラスタ環境がサポートされており、NetBackup クラスタが正しく構成されていることを確認します。	p. 13 の「 NetBackup クラスタ内で NetBackup for SQL Server を使用するための要件 」を参照してください。

NetBackup サーバーおよびクライアントの要件

NetBackup をインストールする前に、NetBackup サーバーと NetBackup クライアントの要件を確認します。

NetBackup サーバーの必要条件

NetBackup サーバーが次の要件を満たしていることを確認します。

- NetBackup サーバーソフトウェアが NetBackup サーバー上にインストールされ、実行可能な状態である。
『[NetBackup インストールガイド](#)』を参照してください。
すべての NetBackup サーバーには、デフォルトで NetBackup クライアントソフトウェアが含まれています。そのため、NetBackup サーバーまたはクライアントで NetBackup for SQL Server を使用できます (NetBackup for SQL Server がプラットフォームでサポートされている場合)。
- ストレージユニットで使用されるバックアップメディアが構成されている。必要なメディアボリュームの数は、いくつかの要因によって異なります。
 - 使用中のデバイスとメディアのストレージ容量。

- バックアップを行うデータベースのサイズ。
 - アーカイブを行うデータの量。
 - バックアップのサイズ。
 - バックアップまたはアーカイブの間隔。
 - バックアップイメージの保持期間。
- 『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

NetBackup クライアントの要件

NetBackup クライアントが次の要件を満たしていることを確認します。

- バックアップするデータベースが存在するコンピュータ上に NetBackup クライアントソフトウェアがインストールされている。
データベースがクラスタ化されている場合、クラスタ内の各ノードで同じバージョンの NetBackup を使う必要があります。
- SQL Server 可用性グループの場合、バックアップを作成する可用性グループの各レプリカでクライアントをインストールします。
- SQL Server クラスタ環境では、クラスタ内のそれぞれのノードに NetBackup クライアントをインストールします。各ノードに同じ NetBackup のバージョンがある必要があります。
- VMware 環境では、SQL Server を実行している仮想マシンに NetBackup クライアントソフトウェアをインストールします。
- 複数の NIC を備えている場合は、プライベートインターフェース名を使って NetBackup クライアントをインストールします。
- SQL Server クライアントがプライマリサーバーまたはメディアサーバーとは別のホストに存在する場合、そのホストに NetBackup クライアントをインストールする必要があります。
- NetBackup 10.4 の NetBackup for SQL Server に含まれる新しい機能を使うには、NetBackup for SQL Server クライアントを NetBackup 10.4 にアップグレードする必要があります。NetBackup メディアサーバーは NetBackup for SQL Server クライアントと同じまたはそれ以上のバージョンを使う必要があります。

NetBackup クラスタ内で NetBackup for SQL Server を使用するための要件

NetBackup for SQL Server クラスタに構成された NetBackup サーバー上で NetBackup を使用する場合、次の要件を満たしていることを確認します。

- NetBackup がお使いのクラスタ環境をサポートしている。

ソフトウェアの互換性リスト (SCL)を参照してください。

- NetBackup サーバーソフトウェアが NetBackup クラスタ内にインストールされ、動作するように構成されている。
『NetBackup インストールガイド』を参照してください。
『NetBackup プライマリサーバーのクラスタ化管理者ガイド』を参照してください。
- NetBackup のクライアントソフトウェアが、NetBackup によるフェールオーバーが可能な各ノード上にインストールされ、実行可能な状態である。
- NetBackup サーバーが存在する各ノード上に、NetBackup for SQL Server の有効なライセンスが存在する必要があります。

NetBackup for SQL Server のライセンス

NetBackup for SQL Server エージェントは NetBackup クライアントソフトウェアとともにインストールされます。個別のインストールは必要ありません。エージェントの有効なライセンスがプライマリサーバーに存在する必要があります。

ライセンスを追加する方法に関する詳細情報を参照できます。

『NetBackup 管理者ガイド Vol. 1』を参照してください。

NetBackup クラスタの場合、NetBackup サーバーが存在する各ノード上に、NetBackup for SQL Server の有効なライセンスが存在する必要があります。

SQL Server ホストとユーザー権限の構成

次の表に、SQL Server のバックアップとリストアを実行するユーザーの前提条件を示します。

表 2-2 NetBackup ホストとユーザー権限の前提条件

手順	処理	説明
手順 1	SQL Server を保護するために VMware バックアップの実行を計画している場合は、Veritas VSS プロバイダをインストールします。 T-SQL スナップショットを使用した VMware バックアップの場合は、SQL Server VSS Writer サービスも無効にする必要があります。	p.15 の「 vSphere 用の Veritas VSS プロバイダのインストール 」を参照してください。 p.16 の「 SQL Server VSS Writer サービスの無効化 」を参照してください。
手順 2	必要な RBAC の役割にユーザーを割り当てます。	p.35 の「 SQL Server 管理者の RBAC の役割 」を参照してください。

手順	処理	説明
手順 3	(該当する場合) SQL Server インテリジェントポリシーまたは保護計画を使用するには、必要な SQL Server クレデンシャルを追加します。	データベースの検出に必要な SQL Server クレデンシャルと、リカバリを実行するためのクレデンシャルを追加します。 p.39 の「 SQL Server インテリジェントポリシーで使用されるクレデンシャルについて SQL Server クレデンシャルについて 」を参照してください。
手順 4	NetBackup Client Service と NetBackup Legacy Network Service を構成します。	この構成により、NetBackup がバックアップおよびリストアを実行する場合に SQL Server にアクセスできます。 p.17 の「 SQL Server のバックアップとリストアのための NetBackup サービスの設定 」を参照してください。
手順 5	(該当する場合) SQL Server インテリジェントポリシーまたは保護計画を使用するには、必要なローカルセキュリティの権限を構成します。	SQL Server クレデンシャルに[これらの特定のクレデンシャルを使用 (Use these specific credentials)]オプションを使用した場合、ローカルシステム以外のアカントには追加のローカルセキュリティの権限が必要になります。 NetBackup for SQL Server エージェントは、データにアクセスするときに SQL Server ユーザーとしてログオンするため、こうした権限が必要になります。 p.18 の「 SQL Server のローカルセキュリティの権限の構成 」を参照してください。
手順 6	NetBackup が検出する有効な各ホストマッピングを承認します。	NetBackup は、環境内の NetBackup ホストに関連付けられている、多くの共有名およびクラスタ名を自動的に検出します。プライマリサーバーの[セキュリティ (Security)]、[ホストマッピング (Host mappings)]でこの構成を実行します。 p.19 の「 自動検出されたマッピングの確認 」を参照してください。

vSphere 用の Veritas VSS プロバイダのインストール

Veritas VSS プロバイダを使用するには、Windows クライアントの NetBackup のインストール後に手動でインストールする必要があります。VMware VSS プロバイダがインストールされている場合はインストールプログラムによって削除され、コンピュータの再起動が必要になることがあります。

Veritas VSS プロバイダをインストールするには

1 次の場所を参照します。

```
install_path¥Veritas¥NetBackup¥bin¥goodies¥
```

2 [vSphere 用の Veritas VSS プロバイダ (Symantec VSS Provider for vSphere)]のショートカットをダブルクリックします。

- 3 プロンプトに従います。
- 4 ユーティリティが完了したら、メッセージが表示される場合はコンピュータを再起動します。
- 5 再起動後、ユーティリティが再開されます。プロンプトに従って、インストールを完了します。

Veritas VSS プロバイダをアンインストールするには

- 1 [プログラムの追加と削除 (Add or Remove Programs)]を開きます。
- 2 [Veritas VSS プロバイダ (Veritas VSS Provider)]をダブルクリックします。

アンインストールプログラムでは、VMware VSS プロバイダは自動的に再インストールされません。

SQL Server VSS Writer サービスの無効化

[T-SQL スナップショットを有効化する (Enable T-SQL snapshots)]オプションを使用して VMware アプリケーションバックアップを実行するには、SQL Server VSS Writer サービスを無効にする必要があります。

このサービスを無効にすると、T-SQL スナップショットを使用しないジョブは失敗します。VM を保護するすべてのポリシーは、同じスナップショット方式を使用する必要があります。T-SQL スナップショット方式を使用するポリシーと使用しないポリシーを混在させないでください。

SQL Server VSS Writer サービスを無効化するには

- 1 NetBackup クライアントがインストールされている SQL Server システムに管理者としてログオンします。
- 2 Windows のサービスアプリケーションを開始します。
- 3 右ペインで、[SQL Server VSS Writer]サービスを右クリックして、[停止 (Stop)]をクリックします。
- 4 右ペインで、[SQL Server VSS Writer]を右クリックして[プロパティ (Properties)]をクリックします。
- 5 [スタートアップの種類 (Startup type)]の一覧で、[無効 (Disabled)]をクリックします。
- 6 [OK]をクリックします。

SQL Server のバックアップとリストアのための NetBackup サービスの設定

NetBackup Web UI を使用したポリシーおよび保護計画の場合、NetBackup はバックアップやリストアを実行する際に、NetBackup Client Service および NetBackup Legacy Network Service を使用して SQL Server にアクセスします。

NetBackup サービスのログオンアカウントには次の要件があることに注意します。

- アカウントには固定のサーバー役割「sysadmin」があります。ドメインアカウント、BUILTIN¥Administrators のメンバー、またはこの役割がある別のアカウントを使用できます。
- (非 VMware バックアップ) ログオンアカウントでローカルシステムを使用する場合、SQL Server の sysadmin 役割を NT AUTHORITY¥SYSTEM または BUILTIN¥Administrators グループに手動で適用する必要があります。
- (VMware バックアップ) ログオンアカウントとしてローカルシステムアカウント以外のアカウントを使用する必要があります。両方のサービスが同じログオンアカウントを使用する必要があります。
- (VMware バックアップ) ログを切り捨てることを選択した場合は、Microsoft SQL Server サービスを実行するアカウントに NetBackup レガシーネットワークサービスの temp ディレクトリに対する完全な権限があることを確認してください。
このディレクトリは C:¥Users¥<ユーザー>¥AppData¥Local¥Temp です。<ユーザー> は NetBackup Legacy Network Service を実行するアカウントです。
- バックアップおよびリストアに gMSA アカウントを使用するには、[クライアントのローカルで定義されているクレデンシヤルを使用 (Use credentials that are defined locally on the client)] オプションを使用してクレデンシヤルを作成する必要があります。

SQL Server のバックアップやリストアのために NetBackup サービスを設定するには

- 1 SQL Server の sysadmin 役割と必要なローカルセキュリティ権限のあるアカウントで、Windows ホストにログオンします。
- 2 Windows サービスアプリケーションで、NetBackup Client Service を開きます。
- 3 次に示すように、アカウントを構成します。
 - (非 VMware バックアップ) [ローカルシステムアカウント (Local System account)] または SQL Server 管理者アカウントが設定されていることを確認します。
インスタンスのクレデンシヤルに[クライアントのローカルで定義されているクレデンシヤルを使用 (Use credentials that are defined locally on the client)]設定を使用する場合は、両方のサービスで同一のログオンアカウントを使用する必要があります。インスタンスのクレデンシヤルに[これらの特定のクレデンシヤルを使う (Use these specific credentials)]設定を使用する場合は、これらのサービス

で同じログオンアカウントを使用するか、別々のログオンアカウントを使用できません。

- (VMware バックアップ) ログオンアカウントの名前を指定して、[OK]をクリックします。
アカウントは、ユーザーアカウントが後ろに続くドメイン名 `domain_name¥account` を含む必要があります。たとえば、`recovery¥netbackup` です。

4 NetBackup Legacy Network Service を開きます。

5 次に示すように、アカウントを構成します。

- (非 VMware バックアップ) [ローカルシステムアカウント (Local System account)] または SQL Server 管理者アカウントが設定されていることを確認します。
インスタンスのクレデンシヤルに[クライアントのローカルで定義されているクレデンシヤルを使用 (Use credentials that are defined locally on the client)]設定を使用する場合は、両方のサービスで同一のログオンアカウントを使用する必要があります。インスタンスのクレデンシヤルに[これらの特定のクレデンシヤルを使う (Use these specific credentials)]設定を使用する場合は、これらのサービスで同じログオンアカウントを使用するか、別々のログオンアカウントを使用できません。
- (VMware バックアップ) ログオンアカウントの名前を指定して、[OK]をクリックします。
このサービスには、NetBackup Client Service と同じログオンアカウントを設定します。

6 別のログオンアカウントを選択した場合は、サービスを再起動します。

7 インスタンスまたはレプリカのクレデンシヤル用に[これらの特定のクレデンシヤルを使用 (Use these specific credentials)]オプションを選択した場合、ローカルシステム以外のアカウントに特定のローカルセキュリティの権限が必要になります。

p.18 の「[SQL Server のローカルセキュリティの権限の構成](#)」を参照してください。

8 仮想環境の場合は、必要なサービスのサービスを設定します。

- VMware バックアップの場合は、バックアップを参照してリストアを実行するために使用する各ホストのサービスを設定します。
- SQL Server クラスタの場合は、クラスタのノードごとにサービスを設定します。
- 可用性グループの場合、バックアップを実行する可用性グループ内のすべてのレプリカでサービスを設定します。

SQL Server のローカルセキュリティの権限の構成

インスタンスまたはレプリカのクレデンシヤル用に[これらの特定のクレデンシヤルを使用 (Use these specific credentials)]オプションを使用する場合、ローカルシステム以外の

アカウントに特定のローカルセキュリティの権限が必要になります。**NetBackup for SQL Server** エージェントは、データにアクセスするときに **SQL Server** ユーザーとしてログオンするため、こうした権限が必要になります。

メモ: この構成は、ローカルセキュリティの権限にのみ適用されます。ドメインレベルの権限については、ドメイン管理者にお問い合わせください。

ローカルセキュリティの権限を構成する方法

- 1 [ローカルセキュリティポリシー (Local Security Policy)]を開きます。
- 2 [ローカルポリシー (Local Policies)]をクリックします。
- 3 [ユーザー権利の割り当て (User Rights Assignment)]では、次のポリシーにアカウントを追加してください。
 - オペレーティングシステムの一部として動作する (Act as part of the operating system)
 - トークンオブジェクトを作成する (Create a token object)
 - 認証後にクライアントを偽装 (Impersonate a client after authentication)
 - [プロセスレベルトークンの置き換え (Replace a process level token)]
- 4 **SQL Server** を再起動します。
- 5 **NetBackup Client Service** と **NetBackup Legacy Network Service** がこのアカウントを使ってログオンする場合、これらのサービスを再起動する必要があります。
- 6 (非 **VMware** バックアップ) **SQL Server** クラスタの場合は、クラスタのノードごとにローカルセキュリティ権限を設定します。**SQL Server** 可用性グループの場合、バックアップを実行するすべてのレプリカでサービスを設定します。

自動検出されたマッピングの確認

特定のシナリオでは、**NetBackup** ホストは他のホストと特定の名前を共有したり、クラスタに関連付けられた名前が付けられます。**NetBackup for SQL Server** で正常にバックアップおよびリストアを実行するには、**NetBackup** によってお使いの環境から検出されたすべての有効な自動検出されたマッピングを承認しておく必要があります。または、マッピングを手動で追加します。

p.21 の「[クラスタの自動検出されたマッピングの承認](#)」を参照してください。

p.23 の「[複数 NIC 環境での SQL Server クラスタ用に自動検出されたマッピング](#)」を参照してください。

p.26 の「[ホスト名の手動マッピング](#)」を参照してください。

複数のホスト名がある構成の例は、次のとおりです。

- ホストが完全修飾ドメイン名 (FQDN) および短縮名または IP アドレスに関連付けられる
- SQL Server がクラスタ化されている場合は、ホストはノード名とクラスタの仮想名に関連付けられます。

これらのマッピングは、NetBackup Web UI の[セキュリティ (Security)]、[ホストマッピング (Host mappings)]ノードで構成されます。マッピングを管理する nbhostmgmt コマンドも使うことができます。詳しくは、『[NetBackup セキュリティおよび暗号化ガイド](#)』と『[NetBackup Web UI 管理者ガイド](#)』を参照してください。

クラスタの自動検出されたマップ

SQL Server クラスタ環境で次が該当する場合にはノード名をクラスタの仮想名にマッピングする必要があります

- バックアップポリシーにクラスタ名 (または仮想名) が含まれている
- NetBackup クライアントがクラスタ内の複数のノードにインストールされている場合、仮想名を各ノードにマッピングする必要があります。
NetBackup クライアントが 1 つのノードにのみインストールされている場合にはマッピングは必要ありません。

クラスタの自動検出されたマッピングの承認

クラスタの自動検出されたマッピングを承認するには

- 1 NetBackup Web UI で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に展開します。
- 2 [承認するマッピング (Mappings to approve)]タブをクリックします。

お客様の環境のホストが一覧表示されるほか、これらのホストに対して NetBackup によって検出されたマッピングまたは追加のホスト名が一覧表示されます。ホストには、マッピングごと、またはマッピングに関連付けられている名前ごとに 1 つのエントリがあります。

たとえば、ホスト `client01.lab04.com` と `client02.lab04.com` で構成されるクラスタの場合は、次のエントリが表示されます。

ホスト	自動検出されたマッピング
<code>client01.lab04.com</code>	<code>client01</code>
<code>client01.lab04.com</code>	<code>clustername</code>
<code>client01.lab04.com</code>	<code>clustername.lab04.com</code>
<code>client02.lab04.com</code>	<code>client02</code>
<code>client02.lab04.com</code>	<code>clustername</code>
<code>client02.lab04.com</code>	<code>clustername.lab04.com</code>

- 3 ホストの名前をクリックします。
- 4 検出されたマッピングを使用する場合は、ホストのマッピングを確認して[承認 (Approve)]をクリックします。

たとえば、次のマッピングが `client01.lab04.com` で有効な場合は、それらのマッピングを承認します。

自動検出されたマッピング	名前が有効なホスト
<code>client01</code>	クライアントの短縮名
<code>clustername</code>	クラスタの仮想名
<code>clustername.lab04.com</code>	クラスタの仮想名の FQDN

- 5
- ホストの有効なマッピングの承認が完了したら、[ホスト (Hosts)] タブをクリックします。
- ホスト `client01.lab04.com` と `client02.lab04.com` に対し、次のような[マッピングされたホストまたは IP アドレス (Mapped host or IP address)] のエントリが表示されます。

ホスト	マッピング済みのホスト名/IP アドレス
<code>client01.lab04.com</code>	<code>client01.lab04.com</code> 、 <code>client01</code> 、 <code>clustername</code> 、 <code>clustername.lab04.com</code>
<code>client02.lab04.com</code>	<code>client02.lab04.com</code> 、 <code>client02</code> 、 <code>clustername</code> 、 <code>clustername.lab04.com</code>

- 6
- NetBackup によって自動的に検出されなかったマッピングは、手動で追加できます。
- 表 2-3 において、FCI は SQL Server フェールオーバークラスティンスタンスを意味します。WSFC は Windows Server フェールオーバークラスタを意味します。

表 2-3 SQL Server 環境用にマッピングされたホスト名の例

環境	ホスト	マッピング済みのホスト名
FCI (2 つのノードから成るクラスタ)	Node 1 の物理名	SQL Server クラスタの仮想名
	Node 2 の物理名	SQL Server クラスタの仮想名
基本または高度可用性グループ (プライマリとセカンダリ)	プライマリ名	WSFC 名
	セカンダリ名	WSFC 名
1 つの FCI (プライマリ FCI またはセカンダリ FCI) から成る基本または高度可用性グループ	プライマリ FCI 名	WSFC 名
	セカンダリ FCI 名	WSFC 名
	Node 1 の物理名	SQL Server クラスタの仮想名
	Node 2 の物理名	SQL Server クラスタの仮想名

複数 NIC 環境での SQL Server クラスタ用に自動検出されたマッピング

複数 NIC 環境に SQL Server クラスタがある場合は、その環境のホストごとに有効な自動検出されたマッピングを承認する必要があります。プライベートネットワーク上の SQL Server クラスタの仮想名を、各 SQL Server クラスタノードのプライベート名にマッピングする必要があります。

複数 NIC 環境で SQL Server クラスタ用に自動検出されたマッピングを承認するには

- 1 NetBackup Web UI で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に展開します。
- 2 [承認するマッピング (Mappings to approve)]タブをクリックします。
お客様の環境のホストが一覧表示されるほか、これらのホストに対して NetBackup によって検出されたマッピングまたは追加のホスト名が一覧表示されます。ホストには、マッピングごと、またはマッピングに関連付けられている名前ごとに 1 つのエントリがあります。

たとえば、ホスト client01-bk.lab04.com と client02-bk.lab04.com で構成される複数 NIC 環境のクラスタの場合は、次のエントリが表示されます。

ホスト (Host)	自動検出されたマッピング
client01-bk.lab04.com	clustername-bk.lab04.com
client02-bk.lab04.com	clustername-bk.lab04.com

- 3 ホストの名前をクリックします。
- 4 検出されたマッピングを使用する場合は、ホストのマッピングを確認して[承認 (Approve)]をクリックします。

たとえば、次のマッピングが client01-bk.lab04.com で有効な場合は、そのマッピングを承認します。

自動検出されたマッピング	名前が有効なホスト
clustername-bk.lab04.com	プライベートネットワーク上の SQL Server クラスタの仮想名

- 5 ホストの有効なマッピングの承認が完了したら、[ホスト (Hosts)] タブをクリックします。
- ホスト `client01-bk.lab04.com` と `client02-bk.lab04.com` に対し、[マッピングされたホストまたは IP アドレス (Mapped host or IP address)] に次の値が表示されます。

ホスト (Host)	マッピングされたホストまたは IP アドレス (Mapped host or IP address)
<code>client01-bk.lab04.com</code>	<code>clustername-bk.lab04.com</code>
<code>client02-bk.lab04.com</code>	<code>clustername-bk.lab04.com</code>

- 6 NetBackup によって自動的に検出されなかったマッピングは、手動で追加できます。

複数 NIC 環境の SQL Server クラスタ用にマッピングされたホスト名の例

表 2-4 複数 NIC 環境の SQL Server クラスタ用にマッピングされたホスト名の例

ホスト	マッピング済みのホスト名
<i>Node 1</i> のプライベート名	プライベートネットワーク上の SQL Server クラスタの仮想名
<i>Node 2</i> のプライベート名	プライベートネットワーク上の SQL Server クラスタの仮想名

SharePoint SQL 可用性グループのバックアップとリストアの自動検出マッピングの承認

SharePoint SQL 可用性グループの自動検出マッピングを承認するには

- 1 NetBackup Web UI で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に展開します。
- 2 [承認するマッピング (Mappings to approve)]タブをクリックします。

お客様の環境のホストが一覧表示されるほか、これらのホストに対して NetBackup によって検出されたマッピングまたは追加のホスト名が一覧表示されます。ホストには、マッピングごと、またはマッピングに関連付けられている名前ごとに 1 つのエントリがあります。

たとえば、ホスト `client01.lab04.com` と `client02.lab04.com` で構成される SharePoint SQL の場合は、次のエントリが表示されます。

ホスト	自動検出されたマッピング
client01.lab04.com	client01、clustername、clustername.lab04.com
client01.lab04.com	aglistenename
client01.lab04.com	aglistenename.lab04.com
client02.lab04.com	client02、clustername、clustername.lab04.com
client02.lab04.com	aglistenename
client02.lab04.com	aglistenename.lab04.com

- 3 ホストの名前をクリックします。

- 4
- 検出されたマッピングを使用する場合は、ホストのマッピングを確認して[承認 (Approve)]をクリックします。

たとえば、次のマッピングが `client01.lab04.com` で有効な場合は、それらのマッピングを承認します。

自動検出されたマッピング	名前が有効なホスト
<code>client01</code>	クライアントの短縮名
<code>aglistenename</code>	SharePoint SQL 可用性グループのリスナー名
<code>aglistenename.lab04.com</code>	SharePoint SQL 可用性グループのリスナー名の FQDN。

- 5
- ホストの有効なマッピングの承認が完了したら、[ホスト (Hosts)]タブをクリックします。

ホスト `client01.lab04.com` と `client02.lab04.com` に対し、次のような[マッピングされたホストまたは IP アドレス (Mapped host or IP address)]のエントリが表示されます。

ホスト	マッピング済みのホスト名/IP アドレス
<code>client01.lab04.com</code>	<code>client01.lab04.com</code> 、 <code>client01</code> 、 <code>aglistenename</code> 、 <code>aglistenename.lab04.com</code>
<code>client02.lab04.com</code>	<code>client02.lab04.com</code> 、 <code>client02</code> 、 <code>aglistenename</code> 、 <code>aglistenename.lab04.com</code>

- 6
- NetBackup** によって自動的に検出されなかったマッピングは、手動で追加できます。

ホスト名の手動マッピング

NetBackup によって自動的に検出されなかったマッピングは、手動で追加できます。

ホスト名を手動でマッピングするには

- 1 NetBackup Web UI で、[セキュリティ (Security)]、[ホストマッピング (Host mappings)]の順に展開します。
- 2 [ホスト (Hosts)]タブをクリックします。
- 3 [共有マッピングまたはクラスタマッピングの追加 (Add shared or cluster mappings)]をクリックします。

たとえば、名前にはクラスタの仮想名を入力します。[追加 (Add)]をクリックして、その仮想名をマッピングするホストを選択します。

分散アプリケーション、クラスタ、または仮想マシンのリストアマッピングの設定

この構成は SQL Server クラスタまたは SQL Server 可用性グループのリストアに必要です。

分散アプリケーション、クラスタ、または仮想マシンのリストアマッピングを設定するには

- 1 NetBackup Web UI を開きます。
- 2 左側で、[ホスト (Hosts)]、[ホストプロパティ (Host properties)]の順にクリックします。
- 3 プライマリサーバーを選択します。
- 4 必要に応じて、[接続 (Connect)]をクリックします。次に、[クライアントの編集 (Edit client)]をクリックします。
- 5 [分散アプリケーションリストアマッピング (Distributed application restore mapping)]を選択します。
- 6 [追加 (Add)]をクリックします。
- 7 アプリケーションホスト名とコンポーネントホスト名を指定します。

参照先「[SQL Server のエントリの例](#)」

SQL Server のエントリの例

表 2-5 SQL Server のエントリの例

環境	アプリケーションホスト	コンポーネントホスト
FCI (2 つのノードから成るクラスタ)	SQL Server クラスタの仮想名	Node 1 の物理名
	SQL Server クラスタの仮想名	Node 2 の物理名

環境	アプリケーションホスト	コンポーネントホスト
高度または基本可用性グループ (プライマリとセカンダリ)	WSFC 名	プライマリレプリカ名
	WSFC 名	セカンダリレプリカ名
1 つの FCI (プライマリ FCI またはセカンダリ FCI) からなる高度または基本可用性グループ	WSFC 名	プライマリレプリカ FCI 名
	WSFC 名	セカンダリレプリカ FCI 名
	SQL Server クラスタの仮想名	Node 1 の物理名
	SQL Server クラスタの仮想名	Node 2 の物理名
VMware	VM 表示名、VM BIOS UUID、VM DNS 名 ([VM ホスト名 (VM hostname)] 以外のプライマリ VM 識別子)	VM のホスト名

ODBC 接続の構成

NetBackup は、NetBackup クライアントからターゲット SQL Server インスタンスへの ODBC 接続の暗号化設定を処理します。これらの設定は、接続しているクライアントのホストプロパティで構成され、hostProperties API エンドポイントまたは nbsetconfig コマンドでのみ構成できます。

メモ: RBAC の役割のデフォルトの Microsoft SQL Server 管理者には、ホストプロパティを編集する権限がありません。代わりに、作業負荷管理者はローカルでホストにログオンし、nbsetconfig コマンドを使用してホストプロパティを変更できます。

ODBC 接続は、ODBC 接続文字列を使用して作成されます。この文字列は、キーと値のペアに応じて接続の動作を変更するキーと値のペアのリストで構成されます。

表 2-6 ODBC 接続の hostProperties API エンドポイントパラメータ

パラメータ	説明
encrypt: true false	TLS を使用して接続を暗号化するかどうか。 10.4 以降に更新された NetBackup クライアントの場合、クライアントからターゲット SQL Server インスタンスへの SQL Server ODBC 接続はデフォルトで暗号化されます。
trustServerCertificate: true false	ターゲット SQL Server インスタンスの証明書を信頼するかどうか。 10.4 以降のクライアントの場合、アップグレード時に予期しない接続エラーが発生しないように、TrustServerCertificate はデフォルトで true に設定されています。

パラメータ	説明
preferredODBCDriver: {driver 1, driver 2, ...}	接続中に使用するサポート対象の SQL Server ODBC ドライバの名前。値には、1 つまたは複数の個別のドライバ名を指定できます。優先設定順にドライバ名を一覧表示します。または、値を "NEWEST" または "OLDEST" に設定します ("NEWEST" または "OLDEST" は単独で指定する必要があります)。 ドライバの SQL Server は暗号化をサポートしません。セキュリティポリシーが厳格で、懸念をお持ちのお客様は、NEWEST ドライバまたは自社で認定されているバージョンを使用する必要があります。 利用可能なドライバ値は次のとおりです。 "SQL Native Client" "SQL Server Native Client 10.0" "SQL Server Native Client 11.0" "SQL Server" "ODBC Driver 11 for SQL Server" "ODBC Driver 13 for SQL Server" "ODBC Driver 17 for SQL Server" "ODBC Driver 18 for SQL Server" "OLDEST" "NEWEST"

ホストプロパティ API エンドポイントの使用例

次の例では、ホストプロパティ API エンドポイントを使用して暗号化を有効にし、ターゲットクライアント証明書を信頼し、**NetBackup** でドライバの "SQL Server" を使用する必要がありますを示しています。そのドライバが利用できない場合、**NetBackup** は "ODBC Driver 17 for SQL Server" を使用する必要があります。

```
PATCH https://{primary-server}/netbackup/config/hosts/{client-host-id}/  
host-properties?fieldset%5BhostProperties%5D=clientMssql  
Body:  
{  
  "data": {  
    "type": "hostProperties",  
    "id": "{client-host-id}",  
    "attributes": {  
      "clientMssql": {  
        "trustServerCertificate": true,  
        "preferredODBCDriver": [  
          "SQL Server",  
          "ODBC Driver 17 for SQL Server"  
        ],  
        "encrypt": true
```

```

    }
  }
}

```

非表示の NetBackup for SQL Server の読み取り不可セカンダリインスタンスの構成

非表示になっている読み取り不可セカンダリインスタンスをサポートするには、追加の構成が必要です。プライマリから NetBackup へのポート番号を提供するセカンダリの構成がないため、NetBackup ユーザーが提供する必要があります。これらの設定は、クライアントのホストプロパティで構成され、hostProperties API エンドポイントまたは bpsetconfig コマンドでのみ構成できます。

メモ: RBAC の役割のデフォルトの Microsoft SQL Server 管理者には、ホストプロパティを編集する権限がありません。代わりに、作業負荷管理者はローカルでホストにログオンし、bpsetconfig コマンドを使用してホストプロパティを変更できます。

このエントリは複数文字列のエントリです。各エントリは、SQL Server ユーティリティを使用してインスタンスに接続するために通常使用される形式です: host¥instance,port

host-properties API の例

https://{{host}}/netbackup/config/hosts/{{host-uuid}}/host-properties

```

"clientMssql": {
  "trustServerCertificate": true,
  "preferredODBCDriver": [
    "OLDEST"
  ],
  "configList": [
    "host16vm5¥¥SQL2K22,1633",
    "host16vm6¥¥SQL2K22,1634"
  ],
  "encrypt": true
}

```

host-properties パッチ API の例

patch: https://{{host}}/netbackup/config/hosts/{{host-uuid}}/host-properties

```

{

```

```
"data": {
  "type": "hostProperties",
  "id": "{host-uuid}",
  "attributes": {
    "clientMssql": {
      "configList": [
        "host16vm5¥¥SQL2K22,1633",
        "host16vm6¥¥SQL2K22,1634"
      ]
    }
  }
}
```

SQL Server エージェントのプライマリサーバーホスト名の構成

環境によっては、**NetBackup for SQL Server** がサーバー主導のバックアップおよびリストアに使用するホスト名の上書きが必要になる場合があります。具体的には、プライマリサーバーが自身を1つのホスト名で認識しているときに、クライアントが別のホスト名でプライマリサーバーに接続する必要がある場合です。たとえば、プライマリサーバーに複数の IP アドレスまたは関連付けられたホスト名がある場合です。この場合、一部のクライアントホストは、プライマリサーバーが自身で認識しているホスト名で解決やネットワークルーティングを実行できないことがあります。

SQL Server エージェントは、プライマリサーバーのホスト名を複数のソースから次の順序で取得します。

- **NBSERVER** 値。
保護計画では、この名前はプライマリサーバー自身が認識するホスト名です。または、**SQL Server** のバックアップ管理者が構成した操作でのホスト名です。
- **SQL Server** エージェントのレジストリ設定。
NetBackup MS SQL Client インターフェースの **NetBackup** クライアントプロパティのプライマリサーバー名 (現在の **NetBackup** サーバー) です。この設定は次のレジストリエントリに対応します。
`HKEY_CURRENT_USER¥Software¥Veritas¥NetBackup¥NetBackup for Microsoft SQL Server¥DEFAULT_SQL_NB_MASTER_SERVER`
- クライアントホスト上の **NetBackup** レジストリの最初の **SERVER** エントリ。
この設定は、次のレジストリエントリにあります。
`HKEY_LOCAL_MACHINE¥Software¥VERITAS¥NetBackup¥CurrentVersion¥Config¥Server`
- ドメインサーバーの値。

クライアントが最後にホスト ID 証明書を要求したプライマリサーバーのホスト名です。この値は、certmapinfo.json ファイルにあるプライマリサーバーの "serverName" です。

または、クライアント上で `USE_REQUESTED_MASTER = FALSE` を設定して、NBSERVER 値の優先度を低くできます。

- SQL Server エージェントのレジストリ値
- プライマリサーバーの値
- NBSERVER 値
- ドメインサーバーの値

USE_REQUESTED_MASTER 設定を FALSE に変更するには

- 1 テキストファイル (new_config.txt など) に次の文を追加します。

```
USE_REQUESTED_MASTER = FALSE
```

- 2 プライマリサーバーまたはメディアサーバーで、次のコマンドを入力します。

```
# bpsetconfig -h ClientA new_config.txt
```

NetBackup により、クライアントホスト ClientA で構成の変更が設定されます。

バックアップ操作を許可するジョブ数の設定

NetBackup が SQL Server のバックアップを開始するときに、ジョブの数が作成されません。ポリシーの設定によっては、[バックアップストライプ数 (Number of backup stripes)] と [並列バックアップ操作 (Parallel backup operations)]などを設定した場合、追加のジョブが作成されます。

作成するジョブの数を増やしたり、制限できます。ストレージユニットに送信するジョブの数を制御することもできます。

ポリシーごとにジョブ数を制限する (Limit jobs per policy) NetBackup で各ポリシーで同時にバックアップできるインスタンスの最大数を設定します。この設定は、ポリシーの属性で構成します。

1 クライアントあたりの最大ジョブ数 (Maximum jobs per client) ポリシーで、クライアントごとに許可するジョブ最大数。この設定は、すべてのポリシーのすべてのクライアントに適用されます。このプロパティは、Web UI のプライマリサーバーの [グローバル属性 (Global attributes)]ホストプロパティで構成できます。

p.33 の「1 クライアントあたりの最大ジョブ数の構成」を参照してください。

最大並列実行ジョブ数
(Maximum concurrent
jobs)

NetBackup からストレージユニットへ一度に送信可能なジョブの最大数。この設定は、ストレージユニットプロパティで構成します。

『NetBackup 管理者ガイド Vol. 1』を参照してください。

1 クライアントあたりの最大ジョブ数の構成

[1 クライアントあたりの最大ジョブ数 (Maximum jobs per client)] では、1 インスタンスまたはデータベースで並行して実行できるバックアップの最大数を指定します。ポリシーで指定される各インスタンスまたはデータベースにより、新しいバックアップジョブが作成されます。

[1 クライアントあたりの最大ジョブ数 (Maximum jobs per client)] を構成する方法

- 1 Web UI を開きます。
- 2 左側で、[ホスト (Host)]、[ホストプロパティ (Host Properties)] の順に選択します。
- 3 ホストを選択します。
- 4 必要に応じて、[接続 (Connect)] をクリックします。
- 5 [プライマリサーバーの編集 (Edit primary server)] をクリックします。
- 6 [グローバル属性 (Global attributes)] をクリックします。
- 7 [1 クライアントあたりの最大ジョブ数 (Maximum jobs per client)] の値を任意の値に変更します。

デフォルトは 1 です。

次の式を使用して、[1 クライアントあたりの最大ジョブ数 (Maximum jobs per client)] の設定に使用するより小さい値を計算します。

1 クライアントあたりの最大ジョブ数 = $\text{number_of_database_objects} \times \text{number_of_streams} \times \text{number_of_policies}$

次の定義を参照してください。

number of database_objects 並列でバックアップするデータベース、ファイルグループ、またはファイルの数。

number_of_streams データベースサーバーと NetBackup 間のバックアップストリームの数。ストライピング (分散化) しない場合、クライアント上で、ストリームごとに新しいバックアップジョブが開始されます。ストライピングする場合、それぞれの新しいジョブは、ストライプごとに 1 つのストリームを使用します。

number_of_policies このクライアントのバックアップを同時に実行できるポリシーの数。この数は、**2** 以上です。たとえば、**2** つの異なるデータベースのバックアップを実行するために、**1** つのクライアントを **2** つのポリシーに設定できます。これらのバックアップ処理時間帯は、重なる場合があります。

SQL Server 管理者用の RBAC の構成

この章では以下の項目について説明しています。

- [SQL Server 管理者の RBAC の役割](#)
- [SQL Server ジョブと VMware ジョブを表示および管理するために必要な RBAC 権限](#)

SQL Server 管理者の RBAC の役割

SQL Server 資産を保護およびリストアするには、作業負荷管理者がそれらの資産にアクセスし、資産にクレデンシャルを割り当てる権限を持っている必要があります。デフォルトの **Microsoft SQL Server 管理者** という名前の RBAC の役割によって、SQL Server 管理者はこれらの権限を付与されます。または、そのユーザーは、カスタム RBAC の役割で同等の権限を持っている必要があります。

さらに、SQL Server 管理者に追加のアクセス権を付与するために、他のカスタム役割が必要になる場合があります。たとえば、SQL Server クライアントのホストプロパティを管理するための特定の権限を与える役割が必要な場合があります。

次の点に注意してください。

- RBAC の役割を作成するには、RBAC 管理者の役割、または役割を作成する権限が必要です。
- 役割の作成と役割のユーザーへの追加については、NetBackup 管理者にお問い合わせください。

RBAC の権限とデフォルトの役割について詳しくは、NetBackup API のマニュアル (<http://sort.veritas.com/>) を参照してください。

SQL Server ジョブと VMware ジョブを表示および管理するために必要な RBAC 権限

SQL Server 操作のジョブ (SQL Server を保護する VMware バックアップを含む) を表示または管理するには、次のように適切な資産権限が必要です。

- インテリジェントポリシーまたはバッチファイルベースのポリシーから開始された、失敗した可用性データベースのバックアップジョブを再開するには、RBAC ユーザーが可用性グループ資産に必要な RBAC 権限を持っている必要があります。再起動オプションは、可用性グループの資産 ID を持つ親バックアップジョブからのみ利用可能です。SQL Server インスタンスまたはデータベース資産に対する RBAC 権限では、親バックアップジョブは表示できません。
- SQL Server の VMware バックアップまたはリストアのジョブの詳細を表示するには、インスタンスとデータベースに必要な RBAC 権限がユーザーに付与されている必要があります。データベースの対応するバックアップジョブを表示するには、VMware 資産に対する適切な RBAC 権限がユーザーに付与されている必要があります。
- データベース資産に関連付けられているスナップショットジョブを表示するには、データベース資産に必要な RBAC 権限がユーザーに付与されている必要があります。

SQL Server の検出とクレデンシャルの管理

この章では以下の項目について説明しています。

- [SQL Server オブジェクトの検出について](#)
- [SQL Server インテリジェントポリシーで使用されるクレデンシャルについて](#) [SQL Server クレデンシャルについて](#)
- [SQL Server インスタンスの削除](#)
- [SQL Server インスタンスの手動での追加](#)

SQL Server オブジェクトの検出について

NetBackup による検出を定期的に行うことで、インスタンスや環境内の高度可用性グループや基本可用性グループの情報を収集します。(読み取りスケール可用性グループは手動で検出する必要があります)。データは 1 時間後に期限切れになります。NetBackup Discovery Service (nbdisco) では、そのプライマリサーバーのクライアント上のインスタンスと可用性グループに対して、8 時間ごとに「簡易」検出が実行されます。NBARS (NetBackup Agent Request Service) は、5 分ごとにプライマリサーバーをポーリングして、期限切れでないデータを確認します。

詳細検出には、データベースの検出が含まれ、次の状況で実行されます。

- 完全バックアップ、増分バックアップ、またはリストアが実行された後
クライアントは、データベースのデータが変更されて 15 分以上経過する前に詳細を送信します。
- データベースまたは可用性グループの手動検出を実行する場合
- インスタンスまたはレプリカのクレデンシャルを追加した後

デフォルトでは、このサービスは、SQL Server インスタンスを検出すると、プライマリサーバーにレポートします。ただし、ユーザーは `bpsetconfig` ユーティリティを使用して、特定のクライアントの検出をオフにできます。REPORT_CLIENT_DISCOVERIES オプションについて詳しくは、『**NetBackup 管理者ガイド Vol. 1**』を参照してください。

クライアントは、各インスタンスの `NetBackup¥dbext¥mssql` ディレクトリにキャッシュファイル `NB_instancename_cache_v1.0.dat` を保持します。ファイルは削除でき、NetBackup は、詳細検出データが再送信されたときに、次の完全バックアップの後でこのファイルを再作成できます。

Web UI の確認メッセージ

[データベースの検出を開始しています。(Starting the discovery of databases.)] のメッセージが[データベースの検出 (Discover databases)]または[可用性グループの検出 (Discover availability groups)]をクリックした後に表示されます。このメッセージは、検出プロセスを開始するように要求されたことのみを示します。ただし、データベースの検出はさまざまな理由で失敗することがあります。たとえば、インスタンスが有効なクレデンシャルと関連付けられていない場合や、ホストに到達できない場合などです。次のメッセージが表示されたときに、詳細検出が成功したと見なせます: [データベースの検出を正常に開始しました。(Successfully started the discovery of databases.) 一覧を更新するには、[更新]をクリックします。(Click Refresh to update the list.)]

高度可用性グループまたは基本可用性グループのオンデマンドの検出

NetBackup 検出プロセスを手動で開始すると、環境で高度可用性グループまたはレプリカ、基本可用性グループまたはレプリカを迅速に検出できます。オンデマンド検出を実行するには、インスタンスまたはレプリカにクレデンシャルが必要です。

高度可用性グループまたは基本可用性グループを検出するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [可用性グループ (Availability groups)]タブをクリックします。
- 3 [可用性グループの検出 (Discover availability groups)]をクリックします。
- 4 可用性グループのレプリカに関連付けられているホストとインスタンスを選択します。
このリストには、登録されているレプリカのみが表示されます。
- 5 [検出 (Discover)]をクリックします。

オンデマンドでのデータベースの検出

NetBackup 検出プロセスを手動で開始すると、環境内のインスタンスデータベースまたは可用性データベースを迅速に検出できます。

データベースを検出するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [データベース (Databases)]タブをクリックします。
- 3 [データベースの検出 (Discover databases)]をクリックします。
- 4 データベースに関連付けられたホストとインスタンスを選択します。
このリストには、登録されているインスタンスのみが表示されます。
- 5 [検出 (Discover)]をクリックします。

読み取りスケール可用性グループの検出

読み取りスケール可用性グループは自動的に検出されません。可用性グループのレプリカのいずれかを指定し、手動で検出を開始する必要があります。

読み取りスケール可用性グループを検出するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [インスタンス (Instances)]タブをクリックします。
- 3 可用性グループに含まれるレプリカのいずれかを選択して、[クレデンシャルの管理 (Manage credentials)]をクリックします。
- 4 プロンプトに従って、レプリカのクレデンシャルを入力します。
- 5 [可用性グループ (Availability groups)]タブをクリックします。
- 6 [可用性グループの検出 (Discover availability groups)]をクリックします。
- 7 可用性グループのレプリカに関連付けられているホストとインスタンスを選択します。
このリストには、登録されているレプリカのみが表示されます。
- 8 [検出 (Discover)]をクリックします。

SQL Server インテリジェントポリシーで使用するクレデンシャルについて SQL Server クレデンシャルについて

SQL Server のインスタンスまたはレプリカは、バックアップとリストア操作を実行するための適切なアクセス権を持った Windows クレデンシャルを使って登録する必要があります。インテリジェントポリシーは、Windows 認証と Windows Active Directory 認証をサポートします。混在モードまたは SQL Server 認証をサポートしません。データベースまたは可用性グループレベルでは、クレデンシャルはサポートされません。

SQL Server を保護するには、SQL Server インスタンスまたは可用性レプリカにクレデンシャルを追加 (登録) する必要があります。NetBackup Web UI は、Windows 認証および Windows Active Directory 認証をサポートしています。混在モードまたは SQL Server 認証をサポートしません。データベースまたは可用性グループレベルでは、クレデンシャルはサポートされません。

表 4-1 クレデンシャルを登録するオプション

クレデンシャルを登録するオプション	環境または構成
これらの特定のクレデンシャルを使用 (Use these specific credentials) (推奨)	■ SQL Server DBA が SQL Server ユーザークレデンシャルを NetBackup 管理者に提供する。 ■ SQL Serer DBA がクライアント上で特権のある SQL Server ユーザーとして NetBackup サービスを実行することを要求しない。 構成要件 クレデンシャルを登録するために使用されるユーザーアカウントは、SQL Server の「sysadmin」の役割を持ち、Windows 管理者グループのメンバーである必要があります。 NetBackup サービスは、ローカルシステムログオンアカウントを使用できます。別のログオンアカウントを使用する場合は、そのアカウントにも特定のローカルセキュリティ権限が必要です。
クライアントのローカルで定義されているクレデンシャルを使用 (Use credentials that are defined locally on the client)	■ NetBackup サービスはクライアント上で特権のある SQL Server ユーザーとして動作します。 ■ SQL Server DBA がインスタンスまたはレプリカを登録するためのクレデンシャルを提供することを要求しない。 ■ NetBackup 管理者が SQL Server クレデンシャルへのアクセス権を持っていない。 ■ gMSA クレデンシャルを使用します。 構成要件 クレデンシャルを登録するために使用されるユーザーアカウントは、SQL Server の「sysadmin」の役割を持ち、Windows 管理者グループのメンバーである必要があります。 NetBackup Client Service と NetBackup Legacy Network Service 用のログオンアカウントを構成する必要もあります。

SQL Server ホストがクラスタ化されている、または複数の NIC を使用している場合のインスタンスの登録

NetBackup が SQL Server クラスタを検出すると、[インスタンス (Instances)] タブに 1 つのエントリを追加します。このインスタンスはクラスタ内のすべてのノードを表します。ホスト名は SQL Server クラスタの仮想名です。このインスタンスにクレデンシャルを追加するときに NetBackup はアクティブノードでクレデンシャルを検証します。クラスタのすべてのノードのクレデンシャルを有効にする必要があります。

NetBackup が複数の NIC を使用する SQL Server ホストを検出すると、[インスタンス (Instances)] タブで NetBackup のクライアント名を使用してエントリを追加します。パブリックインターフェース名を使用して NetBackup クライアントをインストールした場合、プライベートインターフェース名として NetBackup クライアント名を構成する必要があります。次に、そのプライベートインターフェース名でインスタンスにクレデンシャルを追加します。複数の NIC を使用する SQL Server クラスタでは、SQL Server クラスタの仮想プライベート名でインスタンスにクレデンシャルを追加します。

Microsoft SQL Server フェールオーバークラスタインスタンス (FCI) の登録

NetBackup は、クラスタ名と物理ノード名でフェールオーバークラスタインスタンス (FCI) を検出して表示します。たとえば、インスタンス FCI は、その物理ノードである hostvm10 と hostvm11 の両方が、クラスタ名の sql-fci とともに列挙されます。FCI 用に存在するデータベースも、ノード名およびクラスタ名とともに列挙されます。データベースを保護する方法に応じて、クラスタ名 (すべてのノードに対して有効) または物理ノード名のいずれかにクレデンシャルを追加します。

クレデンシャルの検証

クレデンシャルを追加すると、NetBackup によってクレデンシャルが検証され、データベースと可用性グループの検出が開始されます。検出が完了すると、[データベース (Databases)] または [可用性グループ (Availability group)] タブに結果が表示されます。

SQL Server クラスタの場合、または可用性グループのインスタンスが SQL Server クラスタの一部である場合、NetBackup はアクティブノードでクレデンシャルを検証します。クラスタのすべてのノードのクレデンシャルを有効にする必要があります。SQL Server 可用性グループの場合、レプリカは個別に登録されて検証されます。登録日に、クレデンシャルが追加または更新された日時が反映されます。クレデンシャルが有効かどうかは示されません。

SQL Server 用のクレデンシャルの追加

この種類のクレデンシャルにより、NetBackup は SQL Server にアクセスできます。

SQL Server 用のクレデンシャルを追加するには

- 1 左側の [クレデンシャルの管理 (Credential management)] をクリックします。
- 2 [指定したクレデンシャル (Named credentials)] タブで [追加 (Add)] をクリックし、次のプロパティを指定します。
 - クレデンシャル名 (Credential name) (例: `server_credential1`)
 - タグ (Tag) (例: 作業負荷名)
 - 説明 (Description) (例:「このクレデンシャルは作業負荷名へのアクセスに使用」)
- 3 [次へ (Next)] をクリックします。

- 4 [Microsoft SQL Servers]を選択します。
- 5 SQL Server に接続するために必要な認証の詳細を指定します。
p.39 の「[SQL Server インテリジェントポリシーで使用するクレデンシャルについて SQL Server クレデンシャルについて](#)」を参照してください。
- 6 [次へ (Next)]をクリックします。
- 7 クレデンシャルへのアクセス権を付与する RBAC の役割を 1 つ以上追加します。
 - [追加 (Add)]をクリックします。
 - 役割名を選択します。
 - 役割に付与するクレデンシャル権限を選択します。
- 8 [次へ (Next)]をクリックし、プロンプトに従ってウィザードを完了します。

SQL Server インスタンスまたはレプリカのクレデンシャルの選択

SQL Server 資産を完全に検出できるようにするには、インスタンスまたはレプリカに使用するクレデンシャルを選択する必要があります。既存のサーバークレデンシャルから選択するか、新しいクレデンシャルを作成できます。

メモ: データベースと可用性グループの検出は、クレデンシャルの検証後に開始されます。ただし、この資産は Web UI にすぐには表示されない場合があります。資産は検出プロセスが完了した後に表示されます。この日付にクレデンシャルが追加または更新された日時が反映されますが、クレデンシャルが有効であるかどうかは示されません。

認証に使用するクレデンシャルの種類の推奨事項と要件を確認してください。

p.39 の「[SQL Server インテリジェントポリシーで使用するクレデンシャルについて SQL Server クレデンシャルについて](#)」を参照してください。

p.42 の「[SQL Server インスタンスまたはレプリカの既存のクレデンシャルの選択](#)」を参照してください。

p.43 の「[SQL Server インスタンスまたはレプリカの新しいクレデンシャルの追加](#)」を参照してください。

SQL Server インスタンスまたはレプリカの既存のクレデンシャルの選択

可用性グループの場合、各レプリカをクレデンシャルに登録する必要があります。

SQL Server インスタンスまたはレプリカの既存のクレデンシャルを選択するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [インスタンス (Instances)]タブをクリックします。

- 3 インスタンスまたはレプリカのチェックボックスにチェックマークを付け、[クレデンシャルの管理 (Manage credentials)]をクリックします。
- 4 [既存のクレデンシャルから選択してください (Select from existing credentials)]をクリックします。
- 5 [次へ (Next)]をクリックします。
- 6 選択した資産に使用するクレデンシャルを選択し、[次へ (Next)]をクリックします。

SQL Server インスタンスまたはレプリカの新しいクレデンシャルの追加

可用性グループの場合、各レプリカをクレデンシャルに登録する必要があります。

SQL Server インスタンスまたはレプリカに新しいクレデンシャルを追加するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [インスタンス (Instances)]タブをクリックします。
- 3 インスタンスまたはレプリカのチェックボックスにチェックマークを付け、[クレデンシャルの管理 (Manage credentials)]をクリックします。
- 4 [クレデンシャルを追加 (Add credentials)]を選択し、[次へ (Next)]をクリックします。
- 5 認証オプションを選択します。

p.39 の「[SQL Server インテリジェントポリシーで使用するクレデンシャルについて SQL Server クレデンシャルについて](#)」を参照してください。

資産に適用されているクレデンシャル名の表示

資産タイプに構成されている指定したクレデンシャルを表示できます。特定の資産に対してクレデンシャルが構成されていない場合は、このフィールドは空白です。

SQL Server インスタンスのクレデンシャルを表示するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 2 [インスタンス (Instances)]タブで、[クレデンシャル名 (Credential name)]列を見つけてみます。

指定したクレデンシャルの編集または削除

指定したクレデンシャルのプロパティを編集したり、指定したクレデンシャルをNetBackupの[クレデンシャルの管理 (Credential management)]から削除できます。

指定したクレデンシャルの編集

指定したクレデンシャルのタグ、説明、カテゴリ、認証に関する詳細、または権限を変更したい場合はこれを編集できます。クレデンシャル名は変更できません。

指定したクレデンシャルを編集するには

- 1 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
- 2 [指定したクレデンシャル (Named credentials)]タブで、編集するクレデンシャルを特定してクリックします。
- 3 必要に応じて、[編集 (Edit)]をクリックしてクレデンシャルを更新します。
- 4 変更内容を確認して[完了 (Finish)]をクリックします。

指定したクレデンシャルの削除

NetBackup で不要になった、指定したクレデンシャルは削除できます。削除するクレデンシャルを使用する資産がある場合は、それらの資産に別のクレデンシャルを適用してください。そうしないと、それらの資産のバックアップとリストアが失敗する可能性があります。

指定したクレデンシャルを削除するには

- 1 左側の[クレデンシャルの管理 (Credential management)]をクリックします。
- 2 [指定したクレデンシャル (Named credentials)]タブで、削除するクレデンシャルを特定してクリックします。
- 3 [削除 (Delete)]をクリックします。

SQL Server インスタンスの削除

環境内に存在しなくなったインスタンスを削除するには、この手順を使用します。

SQL Server インスタンスを削除するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックし、[インスタンス (Instances)]タブをクリックします。
- 2 インスタンスのチェックボックスに移動してチェックマークを付けます。
- 3 [削除 (Remove)]をクリックします。

メモ: インスタンスを削除すると、削除されたインスタンスに関連付けられているすべての資産は保護されなくなります。既存のバックアップイメージのリカバリは引き続き可能ですが、インスタンスのバックアップは失敗します。

SQL Server インスタンスの手動での追加

新たに検出された SQL Server インスタンスが自動的に表示されます。ところが、検出サービスが新しいインスタンスを検出するのを待ちたくない場合があります。この場合に、インスタンスを手動で追加できます。

SQL Server インスタンスを手動で追加するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックし、[インスタンス (Instances)]タブをクリックします。
- 2 [追加 (Add)]をクリックします。
- 3 インスタンスが存在するホストの名前と[インスタンス名 (Instance name)]を指定します。
 - SQL Server クラスタの場合、ホスト名は SQL Server クラスタの仮想名です。クラスタの各ノードを追加する必要はありません。
 - 複数 NIC 環境の場合、ホスト名は SQL Server ホストまたは仮想 SQL Server のプライベートインターフェース名です。
 - フェールオーバークラスタインスタンスの場合は、SQL Server クラスタの仮想名を入力します。
NetBackup は、FCI を物理ノード名とクラスタ名で列挙します。
- 4 [次へ (Next)]をクリックします。
- 5 インスタンスへのアクセス権を持つ役割を確認します。[追加 (Add)]をクリックして、追加の役割にインスタンスへのアクセス権を付与します。
- 6 このインスタンスのクレデンシャルを追加するには、[クレデンシャルの管理 (Manage credentials)]をクリックします。

p.42 の「[SQL Server インスタンスまたはレプリカのクレデンシャルの選択](#)」を参照してください。

この時点でクレデンシャルを省略することができます。インスタンスは登録解除済みとしてマーク付けされ、[登録済み (Registered)]列が空になります。

- 7 [完了 (Finish)]をクリックします。

SQL Server の保護計画の管理

この章では以下の項目について説明しています。

- [SQL Server 可用性グループの保護について](#)
- [SQL Server 資産を保護するための保護計画の作成](#)
- [保護計画への SQL Server 資産の追加](#)
- [Microsoft SQL Server 資産の保護設定のカスタマイズ](#)
- [SQL Server 資産の保護の削除](#)
- [NetBackup ドメインをまたぐ SQL Server 可用性グループの保護](#)

SQL Server 可用性グループの保護について

NetBackup for SQL Server は SQL Server Always On および読み取りスケール可用性グループのバックアップとリストアをサポートします。サポートされるバージョンと環境については、『[アプリケーションとデータベースエージェントの互換性リスト](#)』を参照してください。

次の方法で可用性グループ環境を保護できます。

- 優先レプリカまたはプライマリレプリカを保護する保護計画を使用します。
- 優先レプリカまたはプライマリレプリカを保護するポリシーを使用します。
- 可用性グループが複数の NetBackup ドメインにわたる場合、自動イメージレプリケーション (A.I.R.) を使用し、他の NetBackup ドメインにバックアップをレプリケートできます。

p.60 の「[NetBackup ドメインをまたぐ SQL Server 可用性グループの保護](#)」を参照してください。

ポリシーまたは保護計画を構成する前に、次の点に注意してください。

- **NetBackup** は、バックアップが行われる各レプリカがクレデンシャルに登録されている場合のみ、可用性グループ環境を完全に保護できます。
- **NetBackup** は、可用性グループ内の各レプリカでバックアップジョブを実行します。バックアップソースではないレプリカでは、ジョブはバックアップをスキップします。

制限事項

NetBackup は、可用性データベースの場合、次の形式のバックアップをサポートしません。

- ファイルグループまたはファイルのスナップショットバックアップ
- インスタントリカバリバックアップ
- VMware バックアップ

SQL Server ではセカンダリレプリカで次の種類のバックアップをサポートしていません。

- 完全バックアップ
セカンダリレプリカで完全バックアップが実行される場合、**NetBackup** は完全バックアップをコピーのみのバックアップに変換します。
- SQL Server インテリジェントポリシーで実行される特定の差分バックアップ
 - 可用性グループがバックアップ対象として追加されると、差分バックアップはスキップされます。
 - 可用性データベースがバックアップ対象として追加されると、差分バックアップは失敗します。
- レガシー (バッチファイルベース) ポリシーで実行される差分バックアップ
この種類のバックアップは失敗します。
- コピーのみのトランザクションログのバックアップ
この種類のバックアップは失敗します。
- (SQL Server 2022) 読み取り可能でないセカンダリ上のファイルグループのバックアップに問題があります。Microsoft 社の制限事項のため、現時点ではサポートされていません。

SQL Server 資産を保護するための保護計画の作成

保護計画を作成して、SQL Server 資産のスケジュールバックアップを実行できます。最初に SQL Server の保護計画を作成します。次に、SQL Server 資産に対してこの保護計画を選択します。

SQL Server 資産を保護するための保護計画を作成するには

- 1 左側で[保護 (Protection)]、[保護計画 (Protection plans)]、[追加 (Add)]の順にクリックします。

- 2 [基本プロパティ (Basic properties)]で、[名前 (Name)]と[説明 (Description)]を入力し、[作業負荷 (Workload)]リストから[Microsoft SQL Server]を選択します。

(省略可能) ポリシー名の接頭辞を追加します。ユーザーが保護計画に資産をサブスクライブする際、**NetBackup** は自動的にポリシーを作成します。このとき **NetBackup** はポリシー名にこの接頭辞を付加します。

- 3 [スケジュールと保持 (Schedules and retention)]で、[追加 (Add)]をクリックします。

バックアップの頻度と保持期間を選択できます。[完全 (Full)]、[差分増分 (Differential incremental)]、[トランザクションログ (Transaction log)]のバックアップスケジュールを設定できます。

[属性 (Attributes)]タブで、次の操作を行います。

- [バックアップ形式 (Backup type)]、バックアップを実行する頻度、このスケジュールのバックアップを保持する期間を選択します。

[開始時間帯 (Start Window)]タブで、次の操作を行います。

- 画面上で設定可能なオプションを使用して、該当スケジュールの[開始曜日 (Start day)]、[開始日時 (Start time)]、[終了曜日 (End day)]、[終了日時 (End time)]を定義します。または、時間のボックス上にカーソルをドラッグして、スケジュールを作成できます。
- 右側のオプションを使用して、スケジュールを複製、削除、またはスケジュールの変更を元に戻します。

[属性 (Attributes)]タブと[開始時間帯 (Start window)]タブでオプションをすべて選択したら、[保存 (Save)]をクリックします。

[バックアップスケジュールのプレビュー (Backup schedule preview)]ウィンドウを確認して、すべてのスケジュールが正しく設定されていることを確認します。

- 4 [ストレージオプション (Storage options)]で、手順 3 で設定したスケジュールごとにストレージ形式を設定します。

オプションは、NetBackup で使用するように現在設定されているストレージオプションによって異なります。

保護計画では、NetBackup 8.1.2 以降のメディアサーバーがアクセスできるストレージのみを使用できます。

ストレージオプション 要件

説明

スナップショットバックアップを実行する
(Perform snapshot backups)

ある特定の時点の、クライアントボリュームの読み取り専用のディスクベースコピーを実行します。NetBackup では、クライアントのプライマリボリュームまたは元のボリュームから直接データをバックアップするのではなく、スナップショットからデータのバックアップが行われます。差分バックアップまたはトランザクションログバックアップを実行するためにスナップショットは使用できません。この場合、NetBackup によってストリームベースのバックアップが実行されます。

[自動 (Automatic)]、[VxVM]、[VSS]のいずれかを選択できます。

p.66 の「スナップショット方式」を参照してください。

SQL Server の動的ファイル割り当てによって、任意のコンポーネントファイルに広大な空き領域が含まれる可能性が少なくなります。

バックアップストレージ (Backup storage)
このオプションには、OpenStorage が必要です。テープ、ストレージユニットグループ、および Replication Director はサポートされません。

[編集 (Edit)]をクリックして、ストレージターゲットを選択します。ストレージターゲットを選択したら、[選択したストレージの使用 (Use selected storage)]をクリックします。

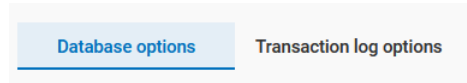
トランザクションログのオプション
(Transaction log options)

トランザクションログのスケジュールを設定するときに、データベースのバックアップに使用されるのと同じストレージを使用するように選択できます。または、トランザクションログ用に一意のストレージを選択できます。

- 5 [バックアップオプション (Backup options)]で、必要なオプションを構成します。

p.51 の「パフォーマンスチューニングおよび設定のオプション」を参照してください。

[データベースのオプション (Database options)]タブをクリックして、データベースのオプションを選択します。[トランザクションログのオプション (Transaction log options)]タブをクリックして、トランザクションログのオプションを選択します。



注意: 可用性グループの場合は、データベースとトランザクションログに対して[可用性データベースのバックアッププリファレンス (Availability Database Backup Preference)]を選択していることを確認します。

- 6 [アクセス権 (Permissions)]で、該当の保護計画にアクセスできる役割を確認します。

別の役割のアクセス権をこの保護計画に付与するには、[追加 (Add)]をクリックします。表で[役割 (Role)]を選択し、[権限の選択 (Select permissions)]セクションで権限を追加または削除して役割をカスタマイズします。

- 7 [確認 (Review)]で保護計画の詳細が正しいことを確認し、[保存 (Save)]をクリックします。

- 8 これで、SQL Server 資産に対する保護計画を選択できます。

- 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 保護するインスタンス、可用性グループ、またはデータベースを選択します。
- [保護の追加 (Add protection)]をクリックします。
- 作成した保護計画を選択します。

スケジュール

次のスケジュール設定が保護計画に含まれています。

資産の保護計画をカスタマイズする場合は、次のスケジュール設定のみを編集できることに注意してください。

- 開始時間帯 (Start window)
- (SQL Server トランザクションログ) 回復
- (SQL Server トランザクションログ) 保持期間

表 5-1 保護計画のスケジュールオプション

オプション	説明
バックアップ形式 (Backup type)	スケジュールで制御するバックアップ形式。
反復 (Recurrence) (間隔)	バックアップを実行する頻度またはタイミング。
保持期間 (Keep for) (保持)	スケジュールによってバックアップされたファイルを保持する期間。
このバックアップをレプリケートする (Replicate this backup)	別のボリュームにスナップショットをレプリケートします。
長期保持用にすぐにコピーを複製する (Duplicate a copy immediately to long-term retention)	スケジュールが作成された直後に、長期保持用ストレージに選択されたメディアにコピーが複製されます。
開始時間帯 (Start window)	このタブで、バックアップを開始できる時間帯を設定します。

パフォーマンスチューニングおよび設定のオプション

表 5-2 では、保護計画で利用可能なチューニングと設定のオプションについて説明します。一部のオプションは、既存の計画を編集する場合、または計画に資産をサブスクライブする場合に変更できません。

メモ: ファイルグループのバックアップはポリシーにのみ利用可能で、保護計画には使用できません。

表 5-2 パフォーマンスチューニングおよび設定のオプション

フィールド	説明
バックアップストライプ数 (Backup stripes)	このオプションは、バックアップ操作を複数の並列実行ストリームに分割します。ストリームはアクティビティ 모니터のジョブに対応します。たとえば、値が 3 の場合、各データベースは 3 つのジョブを使用してバックアップされます。この構成は、テープドライブによる書き込み速度より SQL Server によるデータのダンプ速度が速い場合に適用されます。 このオプションのデフォルト値は 1 です。範囲は 1 から 32 です。

フィールド	説明
ストライプあたりのクライアントバッファ (Client buffers per stripe)	(ストリームベースのバックアップのみ) このオプションはバッファ領域の可用性に影響します。NetBackup では、このパラメータを使用して、バックアップ操作時に各データストリームの読み込みまたは書き込みのために割り当てるバッファ数が決定されます。より多くのバッファ数を割り当てることによって、NetBackup から NetBackup プライマリサーバーへのデータ送信を高速化できます。 このオプションのデフォルト値は 2 で、Double Buffering を有効にします。この値を大きくすると、パフォーマンスがわずかに向上する場合があります。範囲は 1 から 32 です。
最大転送サイズ (Maximum transfer size)	(ストリームベースのバックアップのみ) このオプションは、SQL Server バックアップイメージの読み込みと書き込みに使われるバッファサイズです。通常、この値を大きくすると、SQL Server のパフォーマンスが向上します。このオプションは、個々のバックアップ操作に対して設定できます。64 KB * 2^MAX_TRANSFER_SIZE のように計算されます。64 KB から 4 MB の範囲でサイズを指定できます。デフォルトは 4 MB です。
バックアップするブロックサイズ (Backup block size)	このオプションはストリームベースのバックアップのみに適用されます。SQL Server がバックアップイメージの読み込みと書き込みのために使用する、増分サイズを設定します。このサイズは個々のバックアップ操作に対して設定できます。512 バイト * 2^BLOCK_SIZE のように計算されます。このオプションの値の範囲は 0.5 KB から 64 KB です。デフォルトは 64 KB です。
並列バックアップ操作 (Parallel backup operations)	このオプションでは、データベースインスタンスごとの、同時に開始するバックアップ処理の数を指定します。範囲は 1 から 32 です。デフォルトは 1 です。
VDI タイムアウト (秒) (VDI Timeout (seconds))	(データベースのみ) SQL Server 仮想デバイスインターフェースのタイムアウト間隔を指定します。選択した間隔は、データベースとトランザクションログのバックアップとリストアに適用されます。 バックアップのデフォルト値は 300 です。リストアジョブのデフォルト値は 600 です。範囲は 300 から 2147483647 です。
Microsoft SQL Server の圧縮を使用 (Use Microsoft SQL Server compression)	SQL Server を使用してバックアップイメージを圧縮するには、このオプションを有効にします。SQL Server の圧縮を有効にした場合、NetBackup の圧縮を有効にしないでください。 SQL Server の圧縮は、スナップショットバックアップではサポートされません。
[利用できないデータベース(オフライン、リストア中など)をスキップ (Skip unavailable (offline, restoring, etc.) databases)]	NetBackup では、NetBackup が正常にバックアップできない状態のデータベースをスキップします。これらの状態にはオフライン、リストア中、リカバリ中、緊急モード、などがあります。 NetBackup では、利用できないデータベースのバックアップがスキップされますが、保護計画にサブスクライブされたその他のデータベースのバックアップは続行されます。バックアップは状態 0 で完了し、ジョブの詳細にデータベースがスキップされたことが示されます。
コピーのみバックアップの作成 (Create copy-only backup)	(データベースのみ) このオプションにより SQL Server は帯域外のバックアップを作成できるので、通常のバックアップシーケンスに干渉しません。

フィールド	説明
Microsoft SQL Server チェックサムの実行 (Perform Microsoft SQL Server checksum)	SQL Server のバックアップチェックサムに、次のオプションのいずれかを選択してください。 ■ なし。バックアップチェックサムを無効にします。 ■ バックアップの前にチェックサムを検証するには、次のオプションのいずれかを選択してください。これらのオプションでは、バックアップ操作またはリストア操作でパフォーマンスが低下することに注意してください。 ■ エラー時続行 (Continue on error)。バックアップ時に検証エラーが発生した場合でも、バックアップは続行します。 ■ エラーによる失敗 (Fail on error)。バックアップ時に検証エラーが発生した場合、バックアップは停止されます。
増分バックアップを完全バックアップに変換 (Convert incremental backup to full backup)	(データベースのみ) データベースに対して以前の完全バックアップが存在しない場合、NetBackup は差分バックアップを完全バックアップに変換します。 エージェントは、各データベースの完全バックアップが存在するかどうかを判断します。以前の完全バックアップが存在する場合は、差分バックアップが次のように完全バックアップに変換されます。 ■ 差分バックアップのデータベースを選択すると、バックアップは完全データベースバックアップに変換されます。 (ポリシー用) [読み取り専用ファイルグループをスキップ (Skip read-only file groups)] オプションを選択すると、バックアップが読み書き可能なファイルグループの完全バックアップに変換されます。 ■ (ポリシー用) 差分バックアップでファイルグループを選択すると、NetBackup は次を行います。 ■ 選択したファイルグループがデフォルトのデータベースファイルグループである場合、NetBackup はバックアップを完全ファイルグループバックアップに変換します。 ■ 選択したファイルグループがセカンダリファイルグループであり、プライマリファイルグループのバックアップが存在しない場合には、NetBackup はバックアップを部分的な完全データベースバックアップに変換します。このバックアップには、選択したファイルグループとデフォルトのファイルグループが含まれます。 ■ 選択したファイルグループがセカンダリファイルグループであり、プライマリファイルグループのバックアップが存在する場合、NetBackup は選択したファイルグループの完全ファイルグループバックアップにバックアップを変換します。 ■ スナップショットバックアップポリシーの場合は、差分バックアップから完全バックアップに正常に変換させるために[完全 (Full)]スケジュールが必要です。 注意: NetBackup は、データベースで完全バックアップを実行したことがない場合にのみ差分バックアップを変換します。完全バックアップが NetBackup カタログに存在しないにもかかわらず、SQL Server が既存の完全 LSN を検出する場合には、NetBackup は完全バックアップではなく差分バックアップを実行します。この場合は、ネイティブツールを使った完全バックアップのリストアや、NetBackup MS SQL Client を使った差分バックアップのリストアが可能です。または、NetBackup でバックアップを期限切れにすると、完全バックアップを NetBackup カタログにインポートできます。その場合は、NetBackup MS SQL Client を使用して完全と差分の両方のバックアップをリストアできます。

フィールド	説明
トランザクションログバックアップを完全バックアップに変換 (Convert transaction log backup to full backup)	(トランザクションログのみ) データベースに対して以前の完全バックアップが存在しない場合、NetBackup はトランザクションバックアップを完全バックアップに変換します。 このオプションでは、完全リカバリデータベースが単純リカバリモデルに切り替えられ、完全リカバリモデルに戻されたかどうかを検出されます。このシナリオでは、ログチェーンは分割され、SQL Server は、以降のログバックアップを作成するには、その前に差分バックアップを必要とします。NetBackup がこの状況を検出した場合は、バックアップはデータベースの差分バックアップに変換されます。 注意: NetBackup は、データベースで完全バックアップを実行したことがない場合にのみトランザクションログのバックアップを変換します。完全バックアップが NetBackup カタログに存在しないにもかかわらず、SQL Server が既存の完全 LSNを検出する場合、NetBackup は完全バックアップではなくトランザクションログのバックアップを実行します。この場合、ネイティブツールを使用した完全バックアップのリストアや、NetBackup MS SQL Client を使用した差分バックアップとログバックアップのリストアが可能です。または、バックアップが期限切れになっている場合、完全バックアップを NetBackup カタログにインポートできます。その場合は、NetBackup MS SQL Client を使用して完全バックアップ、差分バックアップ、ログバックアップをリストアできます。

フィールド	説明
可用性データベースのバックアッププリファレンス (Availability Database Backup Preference)	このオプションは、可用性グループのバックアップが発生する場所を決定します。[データベースのオプション (Database options)] タブで、データベースの設定を選択します。[トランザクションログ (Transaction logs)] タブで、トランザクションログの設定を選択します。 ■ 無効 (Disabled) (ポリシーでの同等の設定は[なし (None)]) 指定したインスタンスでバックアップを実行します。このオプションは、個々の可用性データベースを保護する場合に使用します。 ■ プライマリレプリカを保護する (Protect primary replica) バックアップは、プライマリレプリカで常に行われます。このオプションは、可用性レプリカと標準データベースおよび可用性データベースの両方があるインスタンスに適用されます。 ■ 優先レプリカを保護する (Protect preferred replica) SQL Server のバックアッププリファレンスを優先します。これらのプリファレンスには、優先レプリカ、バックアップの優先度、除外されたレプリカが含まれます。NetBackup によるバックアップジョブは、レプリカごとに開始されることに注意してください。目的のバックアップソースではないレプリカではバックアップがスキップされます。このオプションは、可用性レプリカと標準データベースおよび可用性データベースの両方があるインスタンスに適用されます。 ■ 可用性データベースをスキップする (Skip availability databases) インスタンスの可用性データベースをスキップします。このオプションは、スタンドアロンデータベースと可用性データベースの両方を含むインスタンスを保護し、スタンドアロンデータベースのみを保護する場合に使用します。 注意: 可用性グループを保護する場合は、このオプションを選択しないでください。 個々の可用性データベースのバックアッププリファレンス 個々の可用性データベースを保護するために保護計画を選択する場合は、次の動作に注意してください。 ■ [データベース (Databases)] のプリファレンスが[可用性データベースをスキップする (Skip availability databases)] に設定されている場合は、スケジュール設定されたバックアップを正常に実行できません。[データベース (Databases)] には、[なし (None)]、[優先レプリカを保護する (Protect preferred replica)]、または[プライマリレプリカを保護する (Protect primary replica)] を設定する必要があります。 ■ 可用性データベースをバックアップするためにユーザーが[今すぐバックアップ (Backup now)] を選択すると、選択したノードでバックアップが実行されます。イメージはクラスタ名に基づいてカタログ化されます。
バックアップ後ログを切り捨て (Truncate logs after backup)	(トランザクションログのみ) このオプションでは、トランザクションログの有効な部分がバックアップされ、その後、無効または空とマーク付けされます。デフォルトではこのオプションは有効です。

保護計画への SQL Server 資産の追加

次の手順を使用して、SQL Server 資産を保護計画にサブスクライブします。保護計画に資産をサブスクライブするときに、定義済みのバックアップ設定を資産に割り当てます。

次の点に注意してください。

- バックアップを成功させるには、SQL Server インスタンスまたはレプリカに、[インスタンス (Instances)] タブで有効なクレデンシャルが設定されている必要があります。
p.42 の「[SQL Server インスタンスまたはレプリカのクレデンシャルの選択](#)」を参照してください。
- ユーザーアカウントは、RBAC の役割のデフォルトの Microsoft SQL Server または保護計画と SQL Server の同じ権限を持つ別の役割に割り当てられます。
[デフォルトの RBAC の役割および RBAC 権限](#)について、『[NetBackup Web UI 管理者ガイド](#)』で参照してください。補足情報については、NetBackup 管理者にお問い合わせください。
- NetBackup 環境と管理者以外のユーザーについて、その他の要件を満たしていることを確認します。
p.14 の「[SQL Server ホストとユーザー権限の構成](#)」を参照してください。
- データベースは、データベースのバックアップが存在する場合、データベースインスタンスに検証済みクレデンシャルが含まれる場合、データベースの手動検出が実行されている場合にのみ、[データベース (Databases)] タブに表示されます。

保護計画に SQL Server 資産を追加するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 保護する資産 (複数可) を選択します。

インスタンス内のすべてのデータベース	■ [インスタンス (Instances)] タブで、保護するインスタンスのチェックボックスにチェックマークを付けます。
個々のデータベース	■ [インスタンス (Instances)] タブで、保護するデータベースを含むインスタンスのチェックボックスにチェックマークを付けます。 ■ [データベース (Databases)] タブで、1 つ以上のデータベースのチェックボックスにチェックマークを付けます。
可用性グループ	■ [可用性グループ (Availability groups)] タブで、可用性グループ名のチェックボックスにチェックマークを付けます。
個々の可用性データベース	■ [可用性グループ (Availability groups)] タブで、保護するデータベースを含む可用性グループの名前をクリックします。 ■ [データベース (Databases)] タブで、1 つ以上のデータベースのチェックボックスにチェックマークを付けます。

SQL Server クラスタ

- [インスタンス (Instances)] タブで、クラスタに属するインスタンスのチェックボックスにチェックマークを付けます。
ホスト名は **SQL Server クラスタ** の仮想名です。

SQL Server フェールオーバー クラスタインスタンス (FCI)

- [インスタンス (instance)] タブで、クラスタまたはクラスタ内のノードを保護する必要があるかどうかに応じて、インスタンス名を選択します。
- ホスト名が **FCI** のクラスタ名である場合のインスタンス名。
バックアップはアクティブ ノードで試行されます。両方のノードが同じプライマリサーバーのホストである必要があり、インスタンスには有効なクレデンシャルが登録されている必要があります。
 - ホスト名が **FCI** の物理ノード名のいずれかである場合のインスタンス名。
正常にバックアップを作成するには、このノードがクラスタ内のアクティブ ノードである必要があります。バックアップはクラスタ名に基づいてカタログ化されます。

複数の NIC を使用する SQL Server ホスト

- [インスタンス (instance)] タブで、インスタンスを選択します。
- ホスト名が **SQL Server ホスト** のプライベートインターフェース名である場合のインスタンス名。
 - ホスト名が仮想 **SQL Server** のプライベートインターフェース名である場合の、複数の **NIC** を使用する **SQL Server クラスタ** のインスタンス名。

3 [保護の追加 (Add protection)] をクリックします。

4 保護計画を選択し、[次へ (Next)] をクリックします。

- スナップショットバックアップの場合は、[スナップショットオプション (Snapshot options)] と [スナップショット方式 (Snapshot method)] を一覧表示する保護計画を見つけます。
p.66 の「[スナップショット方式](#)」を参照してください。
- 可用性グループの場合は、[可用性データベースのバックアッププリファレンス (Availability database backup preference)] が [プライマリレプリカを保護する (Protect primary replica)] または [優先レプリカを保護する (Protect preferred replica)] に設定されている保護計画を選択します。
[なし (None)] または [可用性データベースをスキップする (Skip availability databases)] を設定している保護計画に、可用性グループをサブスクライブしないでください。

5 次の 1 つ以上の設定を調整できます。

- **スケジュールと保持 (Schedules and retention)**
バックアップの開始時間帯を変更します。トランザクションログのスケジュールの頻度と保持期間を編集することもできます。
p.50 の「[スケジュール](#)」を参照してください。
- **バックアップオプション (Backup options)** と **構成オプション (Configuration options)**

パフォーマンスチューニングオプションを調整するか、保護計画のオプションを変更または有効にします。

p.51 の「パフォーマンスチューニングおよび設定のオプション」を参照してください。

6 [保護 (Protect)]をクリックします。

選択の結果は、[インスタンス (Instances)]または[データベース (Databases)]の下に表示されます。

Microsoft SQL Server 資産の保護設定のカスタマイズ

スケジュールバックアップの時間帯や他のオプションなど、保護計画の特定の設定をカスタマイズできます。

- p.50 の「スケジュール」を参照してください。
- p.51 の「パフォーマンスチューニングおよび設定のオプション」を参照してください。

Microsoft SQL Server 資産の保護設定をカスタマイズするには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 次のいずれかを実行します。

- | | |
|-----------------|---|
| インスタンスの設定の編集 | ■ [インスタンス (instance)]タブで、編集するインスタンスをクリックします。 |
| データベースの設定の編集 | ■ [データベース (Databases)]タブで、編集するデータベースをクリックします。 |
| 可用性グループの設定の編集 | ■ [可用性グループ (Availability groups)]タブで、編集する可用性グループをクリックします。 |
| 可用性データベースの設定の編集 | ■ [データベース (Databases)]タブで、編集するデータベースをクリックします。 |

- 3 [保護のカスタマイズ (Customize protection)]、[続行 (Continue)]の順にクリックします。
 - 4 次の設定を調整します。
 - バックアップ開始時間帯。
- p.50 の「スケジュール」を参照してください。

- トランザクションログのスケジュールの頻度と保持期間も編集できます。
p.50 の「[スケジュール](#)」を参照してください。
- バックアップオプション (Backup options)
パフォーマンスチューニングオプションを調整するか、保護計画の構成オプションを変更または有効にします。
p.51 の「[パフォーマンスチューニングおよび設定のオプション](#)」を参照してください。

5 [保護 (Protect)]をクリックします。

SQL Server 資産の保護の削除

保護計画のデータベース、インスタンス、または可用性グループのサブスクリプションを解除できます。資産のサブスクリプションが解除されると、バックアップは実行されなくなります。

メモ: 保護計画から資産のサブスクリプションを解除するときに、Web UI で、資産に従来のポリシーが表示される可能性があります。この状況は、保護計画に資産がサブスクリプションされており、その資産に対してバックアップが実行される場合に発生することがあります。資産は、有効なバックアップイメージを持ったまま、保護計画からサブスクリプション解除されます。Web UI には従来のポリシーが表示されますが、資産を保護する有効なポリシーがない場合もあります。

インスタンスの保護を削除するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 サブスクリプションを解除する資産を選択します。

- | | |
|-----------------|---|
| インスタンスの保護の削除 | ■ [インスタンス (instance)]タブで、編集するインスタンスをクリックします。 |
| データベースの保護の削除 | ■ [データベース (Databases)]タブで、編集するデータベースをクリックします。 |
| 可用性グループの保護の削除 | ■ [可用性グループ (Availability groups)]タブで、編集する可用性グループをクリックします。 |
| 可用性データベースの保護の削除 | ■ [データベース (Databases)]タブで、編集するデータベースをクリックします。 |

- 3 [保護の削除 (Remove protection)]、[はい (Yes)]の順にクリックします。
資産に、[保護されていません (Not protected)]と表示されます。

NetBackup ドメインをまたぐ SQL Server 可用性グループの保護

可用性グループが複数の NetBackup ドメインにわたる場合、自動イメージレプリケーション (A.I.R.) を使用して別の NetBackup ドメインにバックアップイメージをレプリケートできます。次の構成要件があります。

- NetBackup のソースドメインとターゲットドメインで次のストレージを構成します。
 - OpenStorage の場合は、各ドメインに同じ種類のディスク装置。ディスク装置の種類は、NetBackup 自動イメージレプリケーション (A.I.R.) に対応している必要があります。
 - NetBackup 重複排除の場合は、各ドメインに、メディアサーバー重複排除プールとして NetBackup が使用できるストレージ。
- バックアップが行われるドメインをソースドメインとして構成します。その後、バックアップをリストアするドメインをターゲットドメインとして構成します。

ドメインをまたぐ SQL Server 可用性グループを保護するために保護計画を作成するための方法

- 1 左側で[保護 (Protection)]、[保護計画 (Protection plans)]、[追加 (Add)]の順にクリックします。
- 2 [基本プロパティ (Basic properties)]で、[名前 (Name)]と[説明 (Description)]を入力します。
- 3 [作業負荷 (Workload)]リストから、[Microsoft SQL Server]を選択します。
- 4 [スケジュールと保持 (Schedules and retention)]で、[追加 (Add)]をクリックします。

完全、差分、またはトランザクションログのバックアップを設定できます。

[属性 (Attributes)]タブで、次の操作を行います。

- [バックアップ形式 (Backup type)]、バックアップを実行する頻度、このスケジュールのバックアップを保持する期間を選択します。
- [このバックアップをレプリケートする (Replicate this backup)]を選択します。
 - バックアップストレージは、対象の A.I.R. 環境でソースになっている必要があります。[レプリケーションターゲット (Replication target)]は、手順 5 で構成します。
 - レプリケーションについて詳しくは、『NetBackup 管理者ガイド Vol. 1』の、NetBackup 自動イメージレプリケーションについての説明を参照してください。

[開始時間帯 (Start Window)]タブで、次の操作を行います。

- 画面で利用可能なオプションを使用して、このスケジュールの開始時間帯を定義します。必要に応じて、このスケジュールに複数のスケジュール時間帯を追加できます。

[バックアップスケジュールのプレビュー (Backup schedule preview)]を確認して、すべてのスケジュールが正しく設定されていることを確認します。

- 5 [ストレージオプション (Storage options)]で、手順 5 で設定したスケジュールごとにストレージ形式を設定します。

保護計画では、NetBackup 8.1.2 以降のメディアサーバーがアクセスできるストレージのみを使用できます。

ストレージオプション	要件	説明
バックアップストレージ (Backup storage)	このオプションには、OpenStorage が必要です。テープ、ストレージユニットグループ、および Replication Director はサポートされません。	[編集 (Edit)]をクリックして、ストレージターゲットを選択します。ストレージターゲットを選択したら、[選択したストレージの使用 (Use selected storage)]をクリックします。
レプリケーションターゲット (Replication target)	バックアップストレージは、対象の A.I.R. 環境でソースになっている必要があります。	[編集 (Edit)]をクリックして、レプリケーションターゲットプライマリサーバーを選択します。プライマリサーバーを選択し、次にストレージライフサイクルポリシーを選択します。[選択したレプリケーションターゲットを使用 (Use selected replication target)]をクリックして、ストレージオプション画面に戻ります。

- 6 [バックアップオプション (Backup options)]で必要なオプションを選択します。
[可用性データベースのバックアッププリファレンス (Availability database backup preference)]の一覧から、次のいずれかを選択します。

- プライマリレプリカを保護する (Protect primary replica)
- 優先レプリカを保護する (Protect preferred replica)

p.51 の「パフォーマンスチューニングおよび設定のオプション」を参照してください。

(省略可能) 調整パラメータにその他の変更を加えます。

- 7 [アクセス権 (Permissions)]で、この保護計画へのアクセス権を持つ役割を確認します。
- 8 [確認 (Review)]で保護計画の詳細が正しいことを確認し、[完了 (Finish)]をクリックします。

追加のリソース

『NetBackup 管理者ガイド Vol. 1』

『NetBackup Deduplication ガイド』

『NetBackup OpenStorage Solutions ガイド』

<http://www.netbackup.com/compatibility>

Snapshot Client を使用するバックアップポリシーの構成

この章では以下の項目について説明しています。

- [SQL Server 用の NetBackup Snapshot Client について](#)
- [Snapshot Client を使用した SQL Server の操作](#)
- [スナップショット方式](#)
- [SQL Server スナップショットおよびインスタントリカバリバックアップの構成要件](#)
- [SQL Server のスナップショットポリシーの構成](#)
- [SQL Server のインスタントリカバリバックアップ用のポリシーの構成](#)
- [コピーのみのスナップショットバックアップによる差分バックアップの影響](#)
- [SQL Server エージェントのグループ化スナップショットについて](#)

SQL Server 用の NetBackup Snapshot Client について

NetBackup for SQL Server には、スナップショットバックアップのサポートが含まれます。スナップショットテクノロジーでは、SQL Server 仮想デバイスインターフェース (VDI: Virtual Device Interface) が静止するため、データベース操作が一時的に凍結します。その後エージェントは、コンポーネントファイルのスナップショットを作成することで、SQL Server オブジェクトのバックアップとリストアを実行できるようになります。特定の時点のデータが取得されます。取得されたスナップショットのバックアップを行っても、データベースの可

用性に影響を与えることはありません。これらのスナップショットは、ストレージユニットにバックアップされます。

別の Snapshot Client ライセンスによって、スナップショットバックアップの追加機能が提供されます。インスタントリカバリ用のスナップショットイメージを構成し、代替クライアントを構成してスナップショットバックアップを実行できます。

NetBackup for SQL Server では、次の NetBackup Snapshot Client 機能を使用できます。

スナップショットバックアップ	ある特定の時点の、クライアントボリュームの読み取り専用のディスクベースコピー。NetBackup では、クライアントのプライマリボリュームまたは元のボリュームから直接データをバックアップするのではなく、スナップショットからデータのバックアップが行われます。
インスタントリカバリ	バックアップをローカルディスクからのリカバリのために使用できるようにします。スナップショットは、テープまたは他のストレージに追加のバックアップコピーを行うためのソースにすることもできます。
オフホストバックアップ	バックアップ処理の負荷が別のバックアップエージェントに移行されます。その結果、バックアップがクライアントのコンピュータリソースに与える影響が減少します。バックアップエージェントによって、クライアントのデータがストレージデバイスに送信されます。

Snapshot Client を使用した SQL Server の操作

このトピックでは、Snapshot Client を使用した SQL Server の操作について説明します。

このトピックでは、Snapshot Client オプションを併用した NetBackup for SQL Server の動作について説明します。

- 「バックアップ方式の選択について」
- 「スナップショットを使用する SQL Server の制限事項について」
- 「Snapshot Client と SQL Server のパフォーマンスに関する注意事項について」
- 「SQL Server スナップショットバックアップについて」
- 「SQL Server スナップショットリストアについて」

バックアップ方式の選択について

標準または Snapshot Client のどちらのバックアップ方式を選択するかは、使用するポリシーによって異なります。Snapshot Client 用に構成されたポリシーを選択した場合、このポリシーに関する追加属性によって、Snapshot Client 機能が決定されます。使用する特定のスナップショット方式も決定されます。

スナップショットを使用する SQL Server の制限事項について

SQL Server による制限のため、特定のオブジェクトはスナップショットを介してバックアップできません。これらのオブジェクトには、データベース差分バックアップ、ファイルグループ差分バックアップおよびトランザクションログのバックアップがあります。Snapshot Client ポリシーを選択して、これらのオブジェクト形式の 1 つをバックアップする場合、NetBackup では、ストリームベースのバックアップが実行されます。NetBackup では、このポリシー構成に指定されているストレージユニットが使用されます。ストレージユニットが指定されていない場合、NetBackup はサーバーのデフォルトのストレージユニットを使用します。

NetBackup for SQL Server によるバックアップの対象

データベース管理者は、データベースおよびファイルグループなどの論理オブジェクトを排他的に使用します。ただし、アーカイブされるデータの内容に関して、ファイルベースのバックアップとストリームベースのバックアップ間の相違を把握しておくと便利です。ストリームベースのバックアップの場合、NetBackup によって、SQL Server が提供するデータストリームの内容が取得されます。ユーザーが複数のストリームを指定した場合、SQL Server によって複数のストリームが開かれ、各ストリームは、NetBackup によって個別のイメージとしてカタログ化されます。

ファイルベースのバックアップの場合、NetBackup によって、オブジェクトを構成するすべての物理ファイルで構成されるファイルリストが作成されます。このファイルリストは、スナップショットを作成する機能を持つ Snapshot Client に供給されます。複数のストリームを指定した場合、NetBackup によってファイルリストは複数のサブリストに分割されます。各サブリストは別々にバックアップされ、個別のイメージを構成します。ファイルベースのバックアップにストリームが複数指定されており、ストリームの数がコンポーネントファイルの数より多い場合は、ファイルベースのストリームの数がファイルの数より多くなることはありません。ストリームベースの SQL Server バックアップでは、SQL Server によって、常に、エンドユーザーが指定した数のストリームが作成されます。

SQL Server データベースのバックアップに使用されるファイルリストは、プライマリファイルグループを構成する物理ファイルで構成されます。ファイルリストは、セカンダリファイルグループおよびトランザクションログからも構成されます。通常、これらは、名前拡張子 .mdf、.ndf および .ldf によってそれぞれ識別されます。ファイルグループのバックアップ用のファイルリストは、このファイルグループに属する物理ファイルで構成されます。さらに、オブジェクトのバックアップ用のファイルリストは、単一の物理ファイルで構成されます。このファイルは、SQL Server ファイルオブジェクトにマッピングされるファイルです。

Snapshot Client と SQL Server のパフォーマンスに関する注意事項について

Snapshot Client を使用して物理ファイルをバックアップする場合、このバックアップは、エクステンツ全体で構成されます。このバックアップは、オブジェクトの実際のデータ内容だけがアーカイブされるストリームベースの SQL Server バックアップと対比されます。スナップショットテクノロジーを使用して SQL Server をバックアップする場合、SQL Server

の動的ファイル割り当てを使用すると便利です。この構成により、任意のコンポーネントファイルに広大な空き領域が含まれる可能性が少なくなります。

また、SQL Server ディスクの初期化に関する注意事項を確認します。

p.132 の「[NetBackup for SQL Server のパフォーマンスに影響を与える要素](#)」を参照してください。

SQL Server スナップショットバックアップについて

SQL Server の Snapshot Client バックアップを実行する場合の特別な注意事項はありません。スナップショットバックアップは、バックアップオブジェクトがデータベース、ファイルグループまたはファイルであり、Snapshot Client に対してポリシーが選択されて構成されている場合に、実行されます。Snapshot Client バックアップで、差分バックアップまたはトランザクションログのバックアップを実行する場合、操作には選択したポリシーが使用されます。ただし、標準データベースバックアップは、構成したストレージユニットを使用して実行されます。

SQL Server スナップショットリストアについて

スナップショットから作成されたバックアップイメージは、標準バックアップイメージとともに表示されます。つまり、方式に関係なくすべてのバックアップ項目は、データベース階層の構成に基づいて時系列順に表示されます。また、バックアップ方式に応じた最適なリカバリ方法を決定するための重み付けは指定されません。

スナップショット方式

スナップショットバックアップでは、次のスナップショット方式とオプションを利用できます。詳しくは、『[NetBackup Snapshot Client 管理者ガイド](#)』を参照してください。

SQL Server に対する Snapshot Client サポートによってこれらの機能がすべて提供されても、すべてのスナップショット方式がサポートされるわけではありません。NetBackup for SQL Server で使用するために利用可能なスナップショット方法について詳しくは、NetBackup Snapshot Client の[互換性リスト](#)を参照してください。

表 6-1

メソッド	説明
自動	バックアップの開始時に、NetBackup によってスナップショット方式が選択されます。必要に応じて、NetBackup は保護計画の資産に対して別の方式を選択します。

メソッド	説明
VSS	VSS は Windows のボリュームシャドウコピーサービスを使用します。VSS はローカルバックアップに使用され、選択される実際のスナップショット方式は、クライアント上に構成されているスナップショットプロバイダによって異なります。 プロバイダの形式 (Provider Type): ■ 自動 (Automatic)。NetBackup は、利用可能なプロバイダをハードウェア、ソフトウェア、システムの順に選択します。 ■ システム (System)。ブロックレベルのコピーオンライトスナップショットに Microsoft システムプロバイダを使用します。 ■ ソフトウェアプロバイダを使用し、ファイルシステムと Volume Manager の間のソフトウェアレベルの I/O 要求をインターセプトします。 ■ ディスクアレイ用のハードウェアプロバイダを使用します。 スナップショット属性 (Snapshot Attribute): ■ 自動 (Automatic)。NetBackup が属性を選択します。 ■ 差分 (Differential)。コピーオンライト形式のスナップショットを使用します。 ■ ブレックス (Plex)。クローンまたはミラー形式のスナップショットを使用します。
vxvm	Volume Manager ボリュームに構成されている任意のデータを含むスナップショットの場合。 ■ バックグラウンドでミラーを再同期化する (Resynchronize mirror in background)。バックアップリソースをより効率的に使用できるようにするには、このオプションを選択します。2 つのバックアップで同じテープドライブが必要な場合、最初のジョブの再同期化操作が完了していない場合でも、2 番目のジョブを開始できます。 ■ ミラーの同期の完了を待機 (Wait for mirror sync completion)。このオプションは MS-SQL-Server ポリシーにはサポートされていません。 ■ 再同期化するボリュームの最大数 (Maximum number of volumes to resynchronize)。同時に再同期するボリュームペアの数。クライアントおよびディスクストレージの I/O 帯域幅がボリュームの同時同期をサポートできない場合は、デフォルトを受け入れます。十分な I/O 帯域幅がある構成では、複数のボリュームを同時に再同期することで、再同期をより早く完了できます。I/O 帯域幅を左右する主な要因は、各クライアント上の HBA の数と速度です。

SQL Server スナップショットおよびインスタントリカバリバックアップの構成要件

スナップショットバックアップ用に NetBackup for SQL Server を構成する前に、次の要件を確認します。

- 使用するスナップショット方式のハードウェア要件とソフトウェア要件について詳しくは、『[NetBackup Snapshot Client 管理者ガイド](#)』を参照してください。
- NetBackup for SQL Server でサポートされるスナップショット方式およびプラットフォームについては、Veritas 社のサポート Web サイトにアクセスしてください。

- SQL Server データベースおよびログファイルが格納されているボリュームを、SQL Server 専用とする必要があります。それ以外の形式のデータベース (Exchange など) は、他のボリュームに格納します。
- NetBackup Snapshot Client が正しくインストールおよび構成され、このオプションのライセンスが登録されている必要があります。詳しくは『[NetBackup Snapshot Client 管理者ガイド](#)』を参照してください。
- 1 つのポリシーに対して構成可能なスナップショット方式は 1 つだけです。クライアントごとに異なるスナップショット方式を使用する場合は、クライアントのグループごとに個別のポリシーと使用するスナップショット方式を作成します。それからポリシーごとに方式を 1 つ選択します。
- NetBackup では可用性グループを使用したインスタントリカバリをサポートしていません。

SQL Server のスナップショットポリシーの構成

この手順では、Snapshot Client ポリシーを構成する方法について説明します。必要に応じて、オフホストバックアップを実行できます。このトピックでは、MS-SQL-Server ポリシー用のスナップショットバックアップに必要な構成についてのみ説明します。

スナップショットバックアップを使用して保護計画を構成することもできます。

p.47 の「[SQL Server 資産を保護するための保護計画の作成](#)」を参照してください。

スナップショット方式の選択方法および代替クライアント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。

SQL Server のスナップショットポリシーを構成する方法

- 1 SQL Server のレガシーポリシーの場合は、NetBackup MS SQL Client を使用してバックアップスクリプト(.bch ファイル)を作成します。
- 2 ポリシーを作成します。
- 3 [属性 (Attributes)] タブをクリックします。
- 4 [ポリシー形式 (Policy type)] リストから、[MS-SQL-Server] を選択します。
- 5 [ポリシーストレージ (Policy storage)] を選択します。

データベース差分、ファイルグループ差分、またはトランザクションログが、Snapshot Client を使用するポリシーの[バックアップ対象 (Backup selections)] リストに含まれている場合、NetBackup によってストリームベースのバックアップが実行されます。選択したストレージユニットが使用されます。ストレージユニットが指定されていない場合、NetBackup はサーバーのデフォルトのストレージユニットを使用します。
- 6 [スナップショットバックアップを実行する (Perform snapshot backups)] を選択します。

- 7 NetBackup によってスナップショット方式が選択されるようにするか、手動でスナップショット方式を選択するかを選択します。

次のいずれかを実行します。

- デフォルトでは、スナップショット方式は NetBackup によって選択されます。この設定を変更した後で、再度 NetBackup によって方式を自動的に選択するように指定する場合は、[Snapshot オプション (Snapshot options)]をクリックします。その後、[スナップショット方式 (Snapshot method)]リストから、[auto]を選択します。
- 特定のスナップショット方式を使用する場合は、[Snapshot オプション (Snapshot options)]をクリックします。[スナップショット方式 (Snapshot method)]リストから、このポリシーに使用する方式を選択します。

- 8 (オプション) 代替クライアントを使用して、クライアントの処理負荷を低減する場合は、次の手順を実行します。

- 代替クライアントは、ディスクアレイを共有するクライアントである必要があります。この構成を行うには、追加構成が必要となる場合があります。
- [オフホストバックアップを実行する (Perform off-host backup)]を選択します。
- [使用 (Use)]リストで、[代替クライアント (Alternate client)]を選択します。次に、[マシン (Machine)]リストでクライアント名を選択します。

メモ: [データムーバーの使用 (Use data mover)]オプションは、NetBackup for SQL Server ではサポートされていません。

- 9 [インスタンスとデータベース (Instances and databases)]タブで、SQL Server を保護する方法を選択します。

- (SQL Server インテリジェントポリシー) [インスタンスとデータベースの保護 (Protect instances and databases)]または[インスタンスグループの保護 (Protect instance groups)]を選択します。
インスタンスオプションを選択した場合、個々のインスタンスまたはデータベースのいずれかを選択できます。
- (SQL Server レガシーポリシー) [バッチファイルで使用するクライアント (Clients for use with batch files)]を選択します。

- 10 (SQL Server インテリジェントポリシー) その他のポリシー情報を次のように追加します。

- スケジュールを追加します。
- (省略可能) バックアップする特定のファイルグループまたはファイルを選択します。デフォルトでは、NetBackup はデータベース全体をバックアップします。

- (省略可能) 調整パラメータに変更を加えます。
- 11 (SQL Server レガシーポリシー) その他のポリシー情報を次のように追加します。
- スケジュールを追加します。
 - クライアントを追加します。
 - バックアップ対象リストにバッチファイルを追加します。
- 12 [作成 (Create)]をクリックして、ポリシーを保存します。

SQL Server のインスタントリカバリバックアップ用のポリシーの構成

メモ: NetBackup では、可用性データベースのインスタントリカバリバックアップをサポートしていません。

次の手順では、インスタントリカバリ用のポリシーを構成する方法について説明します。必要に応じて、ディスクにだけバックアップできます。このトピックでは、**MS-SQL-Server** ポリシー用のインスタントリカバリバックアップに必要な構成についてのみ説明します。

スナップショット方式の選択方法および自動スナップショット選択について詳しくは、『[NetBackup Snapshot Client 管理者ガイド](#)』を参照してください。

インスタントリカバリ用のポリシーを構成する方法

- 1 SQL Server レガシーポリシーの場合、NetBackup MS SQL Client インターフェースを使用してバックアップスクリプトを作成します。
- 2 ポリシーを作成します。
- 3 [属性 (Attributes)]タブをクリックします。
- 4 [ポリシー形式 (Policy type)]リストから、[MS-SQL-Server]を選択します。
- 5 [ポリシーストレージ (Policy storage)]を選択します。

[スケジュール (Schedules)]タブで[インスタントリカバリ (Instant Recovery)]オプションを選択した場合(10を参照)、ストレージユニットは使用されません。NetBackup によって、ディスクスナップショットだけが作成されます。

データベース差分バックアップ、ファイルグループ差分バックアップまたはトランザクションログのバックアップがポリシーに含まれている場合、NetBackup によってストリームベースのバックアップが実行されます。このバックアップでは、選択したストレージユニットを使用します。ストレージユニットが指定されていない場合、NetBackup はサーバーのデフォルトのストレージユニットを使用します。

6 [スナップショットバックアップを実行する (Perform snapshot backups)]をクリックします。

7 NetBackup によってスナップショット方式が選択されるようにするか、手動でスナップショット方式を選択するかを選択します。

次のいずれかを実行します。

- デフォルトでは、スナップショット方式は NetBackup によって選択されます。
- 特定のスナップショット方式を使用する場合は、[スナップショットのオプション (Snapshot options)]をクリックし、[スナップショット方式 (Snapshot method)]リストから選択します。

8 [インスタントリカバリ用または SLP 管理用にスナップショットを保持する (Retain snapshots for Instant Recovery)]を選択します。

これによって、NetBackup はスナップショットからインスタントリカバリを実行できるようにディスク上にスナップショットを保持します。

スナップショットのみを作成するように選択しない場合は、ストレージへの通常のバックアップも実行されます (10を参照)。

9 [インスタンスとデータベース (Instances and databases)]タブで、SQL Server を保護する方法を選択します。

- (SQL Server インテリジェントポリシー) [インスタンスとデータベースの保護 (Protect instances and databases)]または[インスタンスグループの保護 (Protect instance groups)]を選択します。
- (SQL Server レガシーポリシー) [バッチファイルで使用するクライアント (Clients for use with batch files)]を選択します。

10 スケジュールを構成する場合、[スケジュール (Schedules)]タブをクリックします。

- (SQL Server インテリジェントポリシー) 完全バックアップスケジュールを構成します。
- (レガシーポリシー) アプリケーションおよび完全バックアップスケジュールを構成するための指示に従います。

スナップショットバックアップポリシーの場合は、NetBackup に差分バックアップから完全バックアップに正常に変換させるために完全バックアップスケジュールが必要です。

11 (オプション) ディスクイメージだけを作成する場合、完全バックアップスケジュール (インテリジェントポリシー) またはアプリケーションスケジュール (レガシーポリシー) を開いて、[インスタントリカバリ (Instant Recovery)]オプションを選択します。

次のオプションのいずれかを選択します。

- [スナップショットを作成し、さらにスナップショットをストレージユニットへコピー (Snapshots and copy snapshots to a storage unit)]が選択された場合、

NetBackup によりディスクのスナップショットが作成されます。また、NetBackup によって、ポリシーに指定したストレージユニットにクライアントのデータがバックアップされます。

- [スナップショットのみ作成 (Snapshots only)]を選択すると、テープまたは他のストレージユニットにイメージがバックアップされません。NetBackup によって、ディスクスナップショットだけが作成されます。このディスクスナップショットは、従来のバックアップの代替とは見なされないことに注意してください。

12 (SQL Server インテリジェントポリシー) その他のポリシー情報を次のように追加します。

- (省略可能) バックアップする特定のファイルグループまたはファイルを選択します。デフォルトでは、NetBackup はデータベース全体をバックアップします。
- (省略可能) 調整パラメータに変更を加えます。

13 (SQL Server レガシーポリシー) その他のポリシー情報を次のように追加します。

- クライアントを追加します。
- バックアップ対象リストにバッチファイルを追加します。

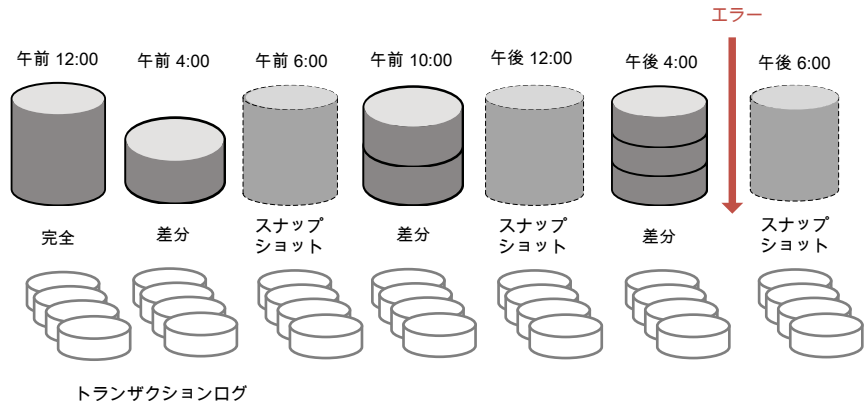
14 [作成 (Create)]をクリックして、ポリシーを保存します。

コピーのみのスナップショットバックアップによる差分バックアップの影響

完全バックアップとスナップショットバックアップの両方を使用して SQL Server を保護する場合は、次のスナップショットバックアップが作成された後、前回のスナップショットバックアップが期限切れになります。最後のバックアップより前の指定した時点へのリストアが必要な場合、差分バックアップは、存在しなくなったスナップショットバックアップに基づくことになります。または、NetBackup を使用して、対域外のコピーのみのバックアップを作成して、バックアップが差分ベースラインをリセットしないようにすることもできます。差分バックアップは、最後の完全バックアップに基づいて実行されます。

障害が発生し、すぐに検出された場合、最後の完全バックアップをリストアできます。その場合、必要なトランザクションログを再生してリカバリを実行できます。ただし、次の完全バックアップまで障害が検出されない場合、リストアに利用できるスナップショットバックアップはありません。コピーのみバックアップを使用する場合、各差分バックアップは、コピーのみではなく最後の完全バックアップに基づいています。最後の完全バックアップをリストアし、最新の差分バックアップをリストアしてから、エラーが発生する前に必要なトランザクションログのバックアップをリストアできます。

図 6-1 完全バックアップおよびコピーのみバックアップを使用する場合のエラー後のリカバリ



コピーのみのバックアップの作成 (レガシー SQL Server ポリシー)

どのバックアップでもコピーのみとして作成できます。インスタントリカバリバックアップはコピーのみとして自動的に作成されます。レガシー SQL Server ポリシーの場合は、バックアップバッチファイルの `COPYONLY TRUE` を設定します。SQL Server インテリジェントポリシーの場合は、[Microsoft SQL Server] タブの [コピーのみバックアップ (Copy-only backup)] を有効にします。

コピーのみバックアップを作成する方法

- 1 テキストエディタで既存のバッチファイルを開きます。
- 2 次のコマンドを入力します。

```
COPYONLY TRUE
```

- 3 バッチファイルを保存します。

コピーのみではないインスタントリカバリバックアップの作成 (レガシー SQL Server ポリシー)

インスタントリカバリバックアップの場合、NetBackup によってバックアップイメージがコピーのみバックアップとして自動的に作成されます。バックアップをコピーのみバックアップとして作成しないようにすることもできます。

コピーのみではないインスタントリカバリバックアップを作成する方法

- 1 テキストエディタで既存のバッチファイルを開きます。
- 2 次のコマンドを入力します。

```
COPYONLY FALSE
```

- 3 バッチファイルを保存します。

SQL Server エージェントのグループ化スナップショットについて

メモ: この機能は SQL Server インテリジェントポリシーとバッチファイルベースのポリシーでのみ利用可能です。保護計画では利用できません。

グループ化されたスナップショットは、データベースのグループを一緒に静止し、それらをグループとしてバックアップするために同時にスナップショットを作成します。NetBackup は、指定したグループサイズまで、自動的にデータベースを検出してグループ化します。すべてのデータベースの構成要素ファイルが同じバックアップ ID で単一のストレージイメージにバックアップされます。つまり、グループのすべてのデータベースバックアップをエクスポートするために、「インポートとコピー」の手順で 1 個のイメージのみが使用されます。

グループ化されたスナップショットの要件

グループ化されたスナップショットを実行するには、一定の要件を満たしている必要があります。次の要件のいずれかが満たされていない場合、標準バックアップが実行されます。

- すべてのバックアップ操作が、完全バックアップである必要があります。差分バックアップとトランザクションログバックアップはサポートされていません。
- (バッチファイルベースのポリシー) グループ内の各バックアップ操作に、同じポリシーを指定する必要があります。
- (バッチファイルベースのポリシー) グループ内の各バックアップ操作に、同じ NetBackup サーバーを指定する必要があります。
- グループサイズは 64 に制限されています。NetBackup は、インスタンスまたはレプリカに 64 を超えるデータベースがある場合、自動的に追加のスナップショットを作成します。

グループ化バックアップされたデータベースのリストア

グループ化バックアップされたデータベースは、他のデータベースと同じようにリストアできます。

p.81 の「[完全データベースリカバリの実行](#)」を参照してください。

p.84 の「[1 つのリカバリポイントのリカバリ](#)」を参照してください。

p.92 の「[SQL Server 可用性データベースのセカンダリレプリカへのリストア](#)」を参照してください。

p.94 の「[SQL Server 可用性データベースのプライマリレプリカとセカンダリレプリカへのリストア](#)」を参照してください。

SQL Server の資産の詳細の表示

この章では以下の項目について説明しています。

- [SQL Server 資産の参照](#)
- [データベース、インスタンス、可用性グループの保護状態の表示](#)

SQL Server 資産の参照

インスタンス、データベース、可用性グループを参照して、保護の有無や利用可能なリカバリポイントなどの詳細を表示できます。

メモ: データベースの従来のポリシー情報が表示されますが、インスタンスや可用性グループの従来のポリシー情報は表示されません。Web UI は、保護計画がインスタンスまたはレプリカを保護するかどうかを示しますが、従来のポリシーの実行の有無は示しません。ただし、個々のデータベースで従来のポリシーを使用してバックアップを作成すると、[次によって保護: (Protected by)]列に従来のポリシー名が表示されます。

SQL Server インスタンスの参照

[インスタンス (instance)]タブで、インスタンスを表示して、インスタンスの保護方法やインスタンスのクレデンシャルなどを管理できます。

SQL Server インスタンスを参照するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [インスタンス (Instances)]タブをクリックします。

- 3 1 つ以上のインスタンスで実行可能な処理を表示するには、インスタンスのチェックボックスにチェックマークを付けます。[今すぐバックアップ (Backup now)]は、インスタンスを 1 つ選択した場合にのみ実行できます。
- 4 インスタンスの詳細を表示するには、インスタンスをクリックします。次のタスクを実行できます。
 - [今すぐバックアップ (Backup now)]をクリックして、インスタンスのバックアップをすぐに実行する
 - [保護の追加 (Add protection)]をクリックして、保護計画にインスタンスを追加する
 - [保護の削除 (remove protection)]をクリックして、保護計画からインスタンスを削除する
 - [データベース (Databases)]タブをクリックして、インスタンスとその保護情報および状態が検出されたデータベースを表示する
 - [アクセス権 (Permissions)]タブをクリックして、インスタンスのアクセス権を持つ役割を表示する

SQL Server 可用性グループの参照

[インスタンス (Instances)]タブで、可用性グループを表示して、データベースとレプリカの詳細、可用性グループの保護方法などを管理できます。

SQL Server 可用性グループを参照するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 1 つ以上の可用性グループに実行可能な処理を表示するには、可用性グループのチェックボックスにチェックマークを付けます。[今すぐバックアップ (Backup now)]は、可用性グループを 1 つ選択した場合にのみ実行できます。
- 3 可用性グループをクリックして、その詳細を表示します。次のタスクを実行できます。
 - [今すぐバックアップ (Backup now)]をクリックして、インスタンスのバックアップをすぐに実行する
 - [保護の追加 (Add protection)]をクリックして、保護計画に可用性グループを追加する
 - [保護の削除 (remove protection)]をクリックして、保護計画から可用性グループを削除する
 - [データベース (Databases)]タブをクリックして、可用性グループとその保護情報および状態が検出されたデータベースを表示する
 - [レプリカ (Replicas)]タブをクリックして、可用性グループとその保護情報および状態が検出されたレプリカを表示する

- [アクセス権 (Permissions)] タブをクリックして、可用性グループのアクセス権を持つ役割を表示する

SQL Server データベースの参照

メモ: データベースは、データベースのバックアップが存在する場合、データベースインスタンスに検証済みクレデンシャルが含まれる場合、データベースの手動検出が実行されている場合にのみ、[データベース (Databases)] タブに表示されます。

SQL Server データベースを参照するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [データベース (Databases)] タブをクリックします。
- 3 1 つ以上のデータベースで実行可能な処理を表示するには、各データベースのチェックボックスにチェックマークを付けます。[今すぐバックアップ (Backup now)] は、データベースを 1 つ選択した場合にのみ実行できます。
- 4 データベースの詳細を表示するには、データベースをクリックします。次のタスクを実行できます。
 - [今すぐバックアップ (Backup now)] をクリックして、インスタンスのバックアップをすぐに実行する
 - [保護の追加 (Add protection)] をクリックして、保護計画にデータベースを追加する
 - [保護の削除 (remove protection)] をクリックして、保護計画からデータベースを削除する
 - [リカバリポイント (Recovery points)] をクリックして、データベースの利用可能なリカバリポイントを表示する
 - [リストアアクティビティ (Restore activity)] をクリックして、データベースのリストアジョブを表示するには
 - [アクセス権 (Permissions)] タブをクリックして、データベースのアクセス権を持つ役割を表示する

データベース、インスタンス、可用性グループの保護状態の表示

インスタンスまたは可用性グループの保護に使用される保護計画を表示できます。

データベース、インスタンス、可用性グループの保護状態を表示するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [データベース (Databases)]、[インスタンス (Instances)]、[可用性グループ (Availability groups)]のいずれかのタブをクリックします。
- 3 [次によって保護: (Protected by)]列には、資産がどのように保護されているかが示されます。

表 7-1 SQL Server 資産の保護状態

保護の形式または状態	[次によって保護: (Protected by)]列	
	データベース	インスタンスまたは可用性グループ
従来のポリシーによって保護されている資産	従来のポリシー	保護されない [保護 (Protection)]、[ポリシー (Policies)]の順に移動して、インスタンスまたは可用性グループを保護するために従来のポリシーがどのように使用されているかを確認します。
保護計画によって保護されている資産	保護	保護
保護計画またはポリシーによって保護されていない資産	保護されない	保護されない
ポリシーまたは保護計画で保護されている資産 (まだバックアップは作成されていないため、バックアップイメージは存在しない)	保護されない [次によって保護: (Protected by)]列は空白になります。	保護されない

SQL Server のリストア

この章では以下の項目について説明しています。

- [SQL Server のリストアの要件](#)
- [完全データベースリカバリの実行](#)
- [1 つのリカバリポイントのリカバリ](#)
- [SQL Server のリストアオプション](#)
- [データベースのリストア \(管理者以外のユーザー\)](#)
- [リカバリ用の別のバックアップコピーの選択](#)
- [SQL Server 可用性データベースのセカンダリレプリカへのリストア](#)
- [SQL Server 可用性データベースのプライマリレプリカとセカンダリレプリカへのリストア](#)

SQL Server のリストアの要件

SQL Server のリストアを実行するには、次の要件があります。

- NetBackup サービスが正しく構成されている必要があります。
p.14 の「[SQL Server ホストとユーザー権限の構成](#)」を参照してください。
- 管理者または管理者以外の両方がリストアを実行できます。ただし、管理者以外の場合は追加の構成手順が必要です。
管理者は、Windows 管理者グループのメンバーおよびローカルの SQL Server sysadmin の役割のメンバーであるユーザーアカウントをリストア時に指定する必要があります。
管理者以外のユーザーが正常にリカバリするには、次の追加の手順を実行する必要があります。
p.88 の「[データベースのリストア \(管理者以外のユーザー\)](#)」を参照してください。

- NetBackup Web UI にサインインしたユーザーは、RBAC の役割であるデフォルトの Microsoft SQL Server 管理者または SQL Server の同じリストア権限を持つ別の役割に割り当てられます。
デフォルトの RBAC の役割および 役割の権限 について、『NetBackup Web UI 管理者ガイド』で参照してください。補足情報については、NetBackup 管理者にお問い合わせください。
- セキュリティ管理者は、[セキュリティ (Security)]、[ホストマッピング (Host mappings)] でホストに必要なマッピングを構成しています。
ホストマッピングの構成 について詳しくは、『NetBackup Web UI 管理者ガイド』を参照してください。補足情報については、NetBackup 管理者にお問い合わせください。
- 別のサーバー (ホスト) にリストアするには、次の必要条件があります。
 - NetBackup が宛先クライアントと通信できる必要があります。
 - 管理者以外のユーザーは、自分のバックアップからのリストアのみを実行できます。

完全データベースリカバリの実行

完全データベースリカバリでは、データベースを完全にリストアするために必要なすべてのバックアップイメージを選択します。これにより、データベースはリカバリ済みの状態または使用準備完了のままになります。

データベースの完全リカバリを実行するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 2 [データベース (Databases)]タブで、リストアするデータベースを見つけます。
データベースのホスト名は、インスタンスまたはホストの保護方法によって異なります。

SQL Server クラスタの一部で あるデータベース ホスト名は SQL Server クラスタの仮想名です。

SQL Server フェールオーバー クラスタインスタンス (FCI) の一部であるデータベース ホスト名は次のいずれかです。

- FCI のクラスタ名
- FCI の物理ノード名

複数の NIC を使用する SQL Server ホスト ホスト名は次のいずれかです。

- SQL Server ホストのプライベートインターフェース名
- 仮想 SQL Server のプライベートインターフェース名

- 3 [操作 (Actions)]、[リカバリ (Recover)]の順に選択します。

- 4 [リカバリポイント (Recovery points)] タブで、リストアする完全、差分、またはトランザクションログイメージを見つけます。

デフォルトでは、**NetBackup** はプライマリコピーを使用します。別のコピーを選択するには、[コピー (Copies)] をクリックします。

p.89 の「[リカバリ用の別のバックアップコピーの選択](#)」を参照してください。

- 5 [処理 (Actions)]、[完全データベースリカバリの実行 (Perform complete database recovery)] を選択します。

- 6 (該当する場合) トランザクションログの場合、次のいずれかのオプションを選択します。

選択したリカバリポイント (Recovery point selected) 指定された時間にデータベースをリストアします。

指定した時点 (Point in time) データベースのリストアを行う別の時点を選択します。

トランザクションログマーク
(Transaction log mark)

- トランザクションマーク以前にリストアするかどうかを選択します。
- トランザクションマークの名前を入力します。
- 特定の日付の後に発生するトランザクションマークを選択するには、[特定の日時後 (After specific date and time)] を選択します。次に、日付と時刻を指定します。
- [次へ (Next)] をクリックします。

- 7 リカバリするホスト、インスタンス、データベースを選択します。次のオプションがあります。

元のホスト、インスタンス、データベースに
リストアします。

別のインスタンスにリストアします。

[インスタンス (Instance)] フィールドに名前を入力します。

別のホストとインスタンスを選択します。

[インスタンスを変更 (Change instance)] をクリックします。

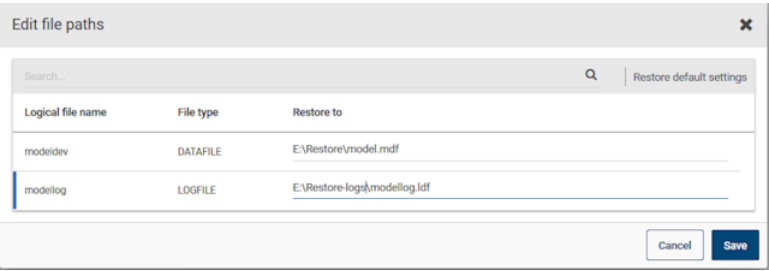
別のデータベースにリストアします。

[データベース名 (Database name)] フィールドに名前を入力します。

8 データベースファイルのリストア先のパスを選択します。次のオプションがあります。

すべてを元のディレクトリにリストア (Restore everything to the original directory)	バックアップされた元のディレクトリにすべてのファイルをリストアします。
すべてを異なるディレクトリにリストア (Restore everything to a different directory)	[リストア用ディレクトリ (Directory for restore)] フィールドに入力したディレクトリにすべてのファイルをリストアします。
ファイルを別々のパスにリストア (Restore files to different paths)	入力したパスに個々のファイルをリストアします。 [ファイルパスを編集 (Edit file paths)]、任意のディレクトリパスの順にクリックして、そのファイルのリストアパスを編集します。

別のパスに対するリストアの例:



9 リカバリターゲットのクレデンシヤルを入力します。または、[既存のクレデンシヤルの選択 (Select existing credentials)]をクリックして、使用するクレデンシヤルを選択します。

ユーザーアカウントはWindows 管理者グループのメンバーである必要があり、ローカルの SQL Server sysadmin の役割のメンバーである必要があります。

10 [次へ (Next)]をクリックします。

11 リカバリオプションを選択します。

- [リストア後のデータベースのリカバリ状態 (Database recovery state after restore)]で、[リカバリ (Recover)]を選択します。
- リストア後に実行する[一貫性チェック (Consistency check)]オプションを選択します。
- その他のリカバリオプションを選択します。

p.87 の「SQL Server のリストアオプション」を参照してください。

- 12 [次へ (Next)]をクリックします。
- 13 [確認 (Review)]ページで、選択したリストアオプションを確認します。
 - 上部の[リカバリセット (Recovery set)]に続くリンクをクリックして、リストアに必要なバックアップイメージを表示します。
 - [編集 (Edit)]をクリックして、[リカバリターゲット (Recovery target)]の設定または[リカバリオプション (Recovery options)]を変更します。
 - [リカバリの開始 (Start recovery)]をクリックします。

1 つのリカバリポイントのリカバリ

個別のリストア操作でバックアップイメージをリストアする場合は、1 つのリカバリポイントのリカバリを実行します。

別のサーバー (ホスト) にリストアするには、次の必要条件があります。

- 代替場所にリストアするための RBAC 権限。
ホストマッピングの構成について詳しくは、『[NetBackup Web UI 管理者ガイド](#)』を参照してください。補足情報については、NetBackup 管理者にお問い合わせください。
- NetBackup が宛先クライアントと通信できる必要があります。

1 つのリカバリポイントをリカバリするには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 2 [データベース (Databases)]タブで、リストアするデータベースを見つけます。
データベースのホスト名は、インスタンスまたはホストの保護方法によって異なります。

SQL Server クラスタの一部で ホスト名は SQL Server クラスタの仮想名です。
あるデータベース

SQL Server フェールオーバー クラスティンスタンス (FCI) の一部であるデータベース ホスト名は次のいずれかです。

- FCI のクラスタ名
- FCI の物理ノード名

複数の NIC を使用する SQL Server ホスト ホスト名は次のいずれかです。

- SQL Server ホストのプライベートインターフェース名
- 仮想 SQL Server のプライベートインターフェース名

- 3 [操作 (Actions)]、[リカバリ (Recover)]の順に選択します。

- 4 [リカバリポイント (Recovery points)] タブで、リストアする完全、差分、またはトランザクションログを見つめます。

デフォルトでは、**NetBackup** はプライマリコピーを使用します。別のコピーを選択するには、[コピー (Copies)] をクリックします。

p.89 の「リカバリ用の別のバックアップコピーの選択」を参照してください。

- 5 [処理 (Actions)]、[1 つのリカバリポイントのリカバリ (Restore single recovery point)] の順に選択します。

- 6 (該当する場合) トランザクションログイメージの場合、次のいずれかのオプションを選択し、[次へ (Next)] をクリックします。

選択したリカバリポイント (Recovery point selected) 指定された時間にデータベースをリストアします。

指定した時点 (Point in time) データベースのリストアを行う別の時点を選択します。

トランザクションログマーク (Transaction log mark)

- トランザクションマーク以前にリストアするかどうかを選択します。
- トランザクションマークの名前を入力します。
- 特定の日付の後に発生するトランザクションマークを選択するには、[特定の日時後 (After specific date and time)] を選択します。次に、日付と時刻を指定します。

- 7 リカバリするホスト、インスタンス、データベースを選択します。次のオプションがあります。

元のホスト、インスタンス、データベースにリストアします。

別のインスタンスにリストアします。 [インスタンス (Instance)] フィールドに名前を入力します。

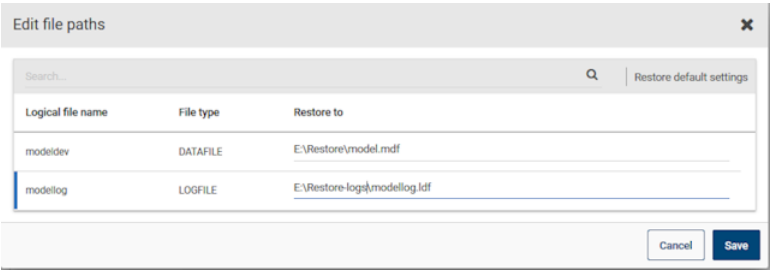
別のホストとインスタンスを選択します。 [インスタンスを変更 (Change instance)] をクリックします。

別のデータベースにリストアします。 [データベース名 (Database name)] フィールドに名前を入力します。

8 データベースファイルのリストア先のパスを選択します。次のオプションがあります。

すべてを元のディレクトリにリストア (Restore everything to the original directory)	バックアップされた元のディレクトリにすべてのファイルをリストアします。
すべてを異なるディレクトリにリストア (Restore everything to a different directory)	[リストア用ディレクトリ (Directory for restore)] フィールドに入力したディレクトリにすべてのファイルをリストアします。
ファイルを別々のパスにリストア (Restore files to different paths)	入力したパスに個々のファイルをリストアします。 [ファイルパスを編集 (Edit file paths)]、任意のディレクトリパスの順にクリックして、そのファイルのリストアパスを編集します。

別のパスに対するリストアの例:



9 リカバリターゲットのクレデンシヤルを入力します。または、[既存のクレデンシヤルの選択 (Select existing credentials)]をクリックして、使用するクレデンシヤルを選択します。

ユーザーアカウントは Windows 管理者グループのメンバーである必要があり、ローカルの SQL Server sysadmin の役割のメンバーである必要があります。

10 [次へ (Next)]をクリックします。

11 リカバリオプションを選択します。

- [リストア後のデータベースのリカバリ状態 (Database recovery state after restore)]オプションを選択します。
- その他のリカバリオプションを選択します。
- [リカバリ (Recovery)]オプションを選択する場合は、リストア後に実行する[一貫性チェック (Consistency check)]オプションを選択します。

p.87 の「SQL Server のリストアオプション」を参照してください。

12 [次へ (Next)]をクリックします。

- 13** [確認 (Review)] ページで、選択したリストアオプションを確認します。
- 上部の[リカバリセット (Recovery set)]に続くリンクをクリックして、リストアに必要なバックアップイメージを表示します。
 - [編集 (Edit)]をクリックして、[リカバリターゲット (Recovery target)]の設定または[リカバリオプション (Recovery options)]を変更します。
 - [リカバリの開始 (Start recovery)]をクリックします。
- 14** リストアが完了したら、差分増分バックアップまたはトランザクションログバックアップのリストアを続行します。
- 各中間バックアップについて、[リストア後のデータベースのリカバリ状態 (Database recovery state after restore)]については、[リストアしています (Restoring)]を選択します。
 - 最終的なバックアップイメージについては、[リカバリ済み (Recovered)]を選択します。

SQL Server のリストアオプション

SQL Server のリストアを実行する際に、次のオプションを選択できます。

表 8-1 リカバリオプション

オプション	説明
リストアは実行せずに、バックアップイメージを検証 (Verify backup image, but do not restore)	NetBackup は、エラーがないかどうかイメージを検証しますが、リストアは実行しません。このオプションは、スナップショットイメージには適用されません。
リストア後のデータベースのリカバリ状態 (Database recovery state after restore)	リストア後にデータベースの状態を選択します。 ■ リカバリ (Recover) リストアシーケンスの最後のイメージをリストアし、データベースを使用できるようにします。 ■ リストアしています (Restoring) 中間バックアップイメージをリストアします。データベースはロード状態のままになるため、追加のバックアップイメージをリストアして適用できます。 ■ スタンバイ (Standby) トランザクションログおよびデータベースのリストア時に、スタンバイデータベースを作成して保持します。このオプションを選択する場合は、スタンバイの取り消しログが必要です。このログは、デフォルトではプライマリデータファイルと同じディレクトリにあります。SQL Server サービスを実行するアカウントには SQLStandBy フォルダのフルアクセス権が必要です。

オプション	説明
一貫性チェック (Consistency check)	リストア後に実行する一貫性チェック。一貫性チェックからの出力は、SQL Server クライアントの進捗ログに書き込まれます。 ■ 実行しない (Do not perform) 一貫性チェックを実行しません。 ■ インデックスを含む完全チェック (Full check, including indexes) 一貫性チェックにインデックスを含めます。エラーはログに記録されます。 ■ インデックスを含まない完全チェック (Full check, excluding indexes) 一貫性チェックからインデックスをエクスクルードします。インデックスをチェックしない場合、一貫性チェックの実行速度は大幅に向上しますが、完全にはチェックされません。一貫性チェックでは、各ユーザー表のデータページおよびクラスタ化インデックスページだけが対象となります。クラスタ化されていないインデックスページの一貫性はチェックされません。 ■ カタログのチェック (Check catalog) 指定したデータベースのシステムテーブル内およびシステムテーブル間の一貫性をチェックします。 ■ 物理チェックのみ (Physical check only) 少ないオーバーヘッドで SQL Server データベースの物理的一貫性をチェックします。このオプションでは、ページヘッダーおよびレコードヘッダーの物理構造の整合性のみを検証します。また、ページのオブジェクト ID やインデックス ID と割り当て構造の間の一貫性もチェックします。
既存のデータベースを上書きする (Overwrite the existing database)	SQL Server は、データベースまたはデータベースファイルがすでに存在する場合は、それらのファイルを上書きできます。 この操作が実行できない場合は、必要な RBAC 権限について NetBackup 管理者にお問い合わせください。
VDI タイムアウト (VDI timeout)	SQL Server 仮想デバイスインターフェースのタイムアウト間隔を指定します。選択した間隔は、データベースとトランザクションログのバックアップとリストアに適用されます。バックアップのデフォルト値は 300 です。リストア操作のデフォルト値は 600 です。範囲は 300 から 2147483647 です。

データベースのリストア (管理者以外のユーザー)

管理者以外のユーザーは SQL Server のリストアを実行できます。ただし、追加の要件と構成手順が必要です。

管理者以外のユーザーに適用される要件は次のとおりです。

- ドメインユーザーグループのメンバーである。
- ローカル SQL Server の sysadmin の役割が付与されている。
- 次に対する完全なアクセス制御権限が付与されている。
 - `install_path¥NetBackup¥dbext¥mssql` フォルダ
 - `HKLM¥SOFTWARE¥ODBC` レジストリハイブ

- `install_path¥NetBackup¥logs¥user_ops` フォルダ

データベースのリストア (管理者以外のユーザー)

- 1 リストアを実行する前に、次の操作を実行する必要があります。
 - SQL Server インスタンスに管理者以外のクレデンシアルを追加する。
p.42 の「[SQL Server インスタンスまたはレプリカのクレデンシアルの選択](#)」を参照してください。
 - データベースの新しいバックアップを実行する。
データベースを特定し、[処理 (Actions)]、[今すぐバックアップ (Backup Now)] の順に選択します。
- 2 リストアを実行するときに、インスタンスの登録に使用したクレデンシアルを指定します。

リカバリ用の別のバックアップコピーの選択

ユーザーは、プライマリバックアップコピーから、または他の利用可能なバックアップコピーから選択してリストアできます。

リカバリ用の別のバックアップコピーを選択するには

- 1 リストアする完全、差分、またはトランザクションログを特定します。
- 2 [コピー (Copies)]をクリックし、目的のコピーを特定します。

以下の例では、[テープ (Tape)]にトランザクションログ用の追加コピーがあります。

April 30, 2021

Backup images/Recovery points	Backup type	
12:00 PM - 02:00 PM	1 Full, 1 Incremental, 6 Transaction log	
12:11:54 PM	Full	Copies > ⋮
12:26:41 PM	Incremental	Copies v ⋮
Storage	Storage server	Storage type
storage1 (Primary copy)	storageserver1	MSDP ⋮
storage2	storageserver1	AdvancedDisk ⋮
E:\storage3	storageserver1	
/storage4	storageserver2	

Perform complete database recovery
Recover single recovery point

- 3 その後、そのコピーの[処理 (Actions)]メニューをクリックして、実行するリストアを選択できます。

この例では、[AdvancedDisk]上のコピーに対して、[完全データベースリカバリの実行 (Perform complete database recovery)]または[1 つのリカバリポイントのリカバリ (Recover single recovery point)]のいずれかを選択できます。

リカバリ用ストレージの編集

以下の例では、リカバリウィザードの[リカバリソース (Recovery source)]ページに、リカバリ用に選択したストレージが表示されています。リカバリに必要なイメージがストレージで利用できない場合、NetBackup によって適切なストレージのプライマリイメージが自動的に選択されます。自動選択を使用しない場合は、ストレージを変更できます。

この例では、AdvancedDisk ストレージ上のトランザクションログのコピーを選択しました。完全イメージと増分イメージは同じストレージで利用できないため、NetBackup によって MSDP ストレージ上のコピーが自動的に選択されます。[編集 (Edit)]をクリックして、[完全 (Full)]イメージ用に選択されたストレージを変更できます。

図 8-1 リカバリ用に選択されたストレージ

Storage for recovery			
Full			
Selected storage	Storage server	Storage type	
 storage1	storageserver1	MSDP	Edit
Incremental			
Selected storage	Storage server	Storage type	
storage2	storageserver2	AdvancedDisk	Edit

リカバリにプライマリコピーのみを使用する場合は、[プライマリコピーのみを選択する (Select only primary copies)]をクリックします (図 8-2を参照)。それ以外の場合は、[編集 (Edit)]をクリックして、使用する特定のストレージを選択できます (図 8-3を参照)。

図 8-2 トランザクションログのプライマリコピーのみを選択

Storage for recovery			
Full			
Selected storage	Storage server	Storage type	
storage1	storageserver1	MSDP	Edit
Incremental			
Selected storage	Storage server	Storage type	
storage1	storageserver1	MSDP	Edit
Transaction log			
☒ Select only primary copies This option automatically selects only the primary copies for the transaction logs.			
Selected storage	Storage server	Storage type	Images
storage1	storageserver1	MSDP	12 of 24
storage2	storageserver2	AdvancedDisk	12 of 24

図 8-3 トランザクションログのストレージの編集

Storage for recovery

Full

Selected storage	Storage server	Storage type	
storage1	storageserver1	MSDP	Edit

Incremental

Selected storage	Storage server	Storage type	
storage1	storageserver1	MSDP	Edit

Transaction log

☐ Select only primary copies
This option automatically selects only the primary copies for the transaction logs.

Selected storage	Storage server	Storage type	Images	
storage1	storageserver1	MSDP	24 of 24	Edit

SQL Server 可用性データベースのセカンダリレプリカへのリストア

この手順では、SQL Server 可用性データベースをセカンダリレプリカにリストアする方法を説明します。セカンダリレプリカが長時間にわたり利用不可でプライマリと同期する必要がある場合はこの手順に従います。または、可用性グループに新しいセカンダリレプリカを追加した後でこれらの手順に従います。

SQL Server 可用性データベースをセカンダリレプリカにリストアするには

- セカンダリレプリカをホストするノードにログオンし、次の処理を実行します。
 - セカンダリレプリカのデータベースへのすべての接続を閉じます。
 - 可用性グループからセカンダリデータベースを削除します。
- 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- [可用性グループ (Availability groups)]タブで、可用性グループ名をクリックします。
- [レプリカ (replica)]タブで、セカンダリレプリカでホストされているインスタンスをクリックします。

- 5 [データベース (Databases)] タブで、リストアするデータベースをクリックします。
- 6 [リカバリポイント (Recovery points)] タブをクリックし、最新のトランザクションログのバックアップを見つけます。

デフォルトでは、NetBackup はプライマリコピーを使用します。別のコピーを選択するには、[コピー (Copies)] をクリックします。

p.89 の「[リカバリ用の別のバックアップコピーの選択](#)」を参照してください。
- 7 [処理 (Actions)] メニューから、[完全データベースリカバリの実行 (Perform complete database recovery)] を選択します。
- 8 次のいずれかのオプションを選択します。

選択したリカバリポイント (Recovery point selected) 指定された時間にデータベースをリストアします。

指定した時点 (Point in time) データベースのリストアを行う別の時点を選択します。

トランザクションログマーク (Transaction log mark)

- トランザクションマーク以前にリストアするかどうかを選択します。
- トランザクションマークの名前を入力します。
- 特定の日付の後に発生するトランザクションマークを選択するには、[特定の日時後 (After specific date and time)] を選択します。次に、日付と時刻を指定します。

- 9 可用性グループのレプリカでデータベースファイルに異なるパスを使用する場合は、[ファイルを別々のパスにリストア (Restore files to different paths)] を選択してファイルパスを編集します。
- 10 リストアするインスタンスのクレデンシャルを入力し、[次へ (Next)] をクリックします。
ユーザーアカウントは Windows 管理者グループのメンバーである必要があり、ローカルの SQL Server sysadmin の役割のメンバーである必要があります。
- 11 次の設定を選択します。
 - リストアしています (Restoring)
 - 既存のデータベースを上書きする (Overwrite the existing database)

p.87 の「[SQL Server のリストアオプション](#)」を参照してください。
- 12 [次へ (Next)] をクリックします。次に、[リカバリの開始 (Start recovery)] をクリックします。
- 13 リストアが完了したら、データベースを可用性グループに接続します。

SQL Server 可用性データベースのプライマリレプリカとセカンダリレプリカへのリストア

状況に応じて、SQL Server 可用性データベースをプライマリレプリカとセカンダリレプリカの両方にリストアしなければならない場合があります。そのような状況には、次の場合にデータベースをリストアすることも含まれます。

- ディザスタリカバリの後
- データベースの論理的な破損が発生した後
- 可用性グループのクローンまたはテスト環境へのリストア
- 過去のある時点へのリストア

このプライマリデータベースのリストアは、セカンダリデータベースのリストアと並列して実行することをお勧めします。

SQL Server 可用性データベースをプライマリレプリカとセカンダリレプリカにリストアするには

- 1 プライマリレプリカのホストにログオンし、次の処理を実行します。
 - SQL Server Management Studio で、データベースのデータの移動を停止し、可用性グループからデータベースを削除します。
 - データベースへのすべての接続を閉じます。
 - SQL Server からプライマリデータベースを削除します。
- 2 NetBackup Web UI の左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 3 [可用性グループ (Availability groups)]タブで、可用性グループ名をクリックします。
- 4 [レプリカ (replica)]タブで、プライマリレプリカでホストされているインスタンスをクリックします。
- 5 [データベース (Databases)]タブで、リストアするデータベースをクリックします。
- 6 [リカバリポイント (Recovery points)]タブをクリックし、最新のトランザクションログのバックアップを見つけます。

デフォルトでは、NetBackup はプライマリコピーを使用します。別のコピーを選択するには、[コピー (Copies)]をクリックします。

p.89 の「[リカバリ用の別のバックアップコピーの選択](#)」を参照してください。
- 7 [処理 (Actions)]メニューから、[完全データベースリカバリの実行 (Perform complete database recovery)]を選択します。
- 8 次のいずれかのオプションを選択します。

選択したリカバリポイント (Recovery point selected)	指定された時間にデータベースをリストアします。
指定した時点 (Point in time)	データベースのリストアを行う別の時点を選択します。
トランザクションログマーク (Transaction log mark)	- トランザクションマーク以前にリストアするかどうかを選択します。 - トランザクションマークの名前を入力します。 - 特定の日付の後に発生するトランザクションマークを選択するには、[特定の日時後 (After specific date and time)]を選択します。次に、日付と時刻を指定します。

- 9 リストアするインスタンスのクレデンシャルを入力し、[次へ (Next)]をクリックします。
ユーザアカウントは Windows 管理者グループのメンバーである必要があり、ローカルの SQL Server sysadmin の役割のメンバーである必要があります。
- 10 次の設定を選択します。
 - リカバリ (Recover)
 - 既存のデータベースを上書きする (Overwrite the existing database)

p.87 の「[SQL Server のリストアオプション](#)」を参照してください。
- 11 [次へ (Next)]をクリックします。次に、[リカバリの開始 (Start recovery)]をクリックします。
- 12 リストアが完了したら、[最初のデータの同期をスキップ (Skip initial data synchronization)]オプションを使用して、データベースを可用性グループに追加します。
- 13 セカンダリレプリカのホストにログオンし、次の手順を完了します。
 - セカンダリレプリカのデータベースへのすべての接続を閉じます。
 - SQL Server からセカンダリデータベースを削除します。
- 14 NetBackup Web UI の左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 15 [可用性グループ (Availability groups)]タブで、可用性グループ名をクリックします。
- 16 [レプリカ (replica)]タブで、セカンダリレプリカでホストされているインスタンスをクリックします。
- 17 [データベース (Databases)]タブで、リストアするデータベースをクリックします。
- 18 [リカバリポイント (Recovery points)]タブをクリックし、プライマリレプリカにリストアしたイメージを見つけます。

- 19 [処理 (Actions)]メニューから、[完全データベースリカバリの実行 (Perform complete database recovery)]を選択します。
- 20 トランザクションログについては、プライマリレプリカで選択したのと同じ指定した時点またはログマークを選択します。
- 21 リストアするインスタンスのクレデンシャルを入力し、[次へ (Next)]をクリックします。
ユーザーアカウントは Windows 管理者グループのメンバーである必要があり、ローカルの SQL Server sysadmin の役割のメンバーである必要があります。
- 22 次の設定を選択します。
 - リストアしています (Restoring)
 - 既存のデータベースを上書きする (Overwrite the existing database)p.87 の「[SQL Server のリストアオプション](#)」を参照してください。
- 23 [次へ (Next)]をクリックします。次に、[リカバリの開始 (Start recovery)]をクリックします。
- 24 リストアが完了したら、データベースを可用性グループに接続します。
- 25 可用性グループの追加レプリカに対して、手順 13 から手順 24 を繰り返します。

SQL Server でのインスタントアクセスの使用

この章では以下の項目について説明しています。

- [インスタントアクセス SQL Server データベースを構成する場合の前提条件](#)
- [インスタントアクセスデータベースを設定する前の考慮事項](#)
- [SQL Server インスタントアクセス用の Samba ユーザーの構成](#)
- [インスタントアクセスデータベースの構成](#)
- [インスタントアクセスデータベースのライブマウントの詳細の表示](#)
- [インスタントアクセスデータベースの削除](#)
- [NetBackup for SQL Server インスタントアクセスのオプション](#)
- [NetBackup for SQL Server の用語](#)
- [よく寄せられる質問](#)

インスタントアクセス SQL Server データベースを構成する場合の前提条件

この前提条件は、SQL Server のインスタントアクセス BYO (Build Your Own) にのみ適用されます。

前提条件:

- BYO サーバーのオペレーティングシステムのバージョンは Red Hat Enterprise Linux 7.6 以降である必要があります。

- Samba サービスがインストールされていること、および次のコマンドを使用して **selinux** ポリシーで **Samba** 共有権限が許可されていることを確認します。

```
setsebool -P samba_export_all_rw=1
```

- **NGINX** がインストールされているストレージサーバー。
 - **NGINX** バージョンは、対応する正式な **RHEL** バージョンのリリースに存在するものと同じである必要があります。対応する **RHEL yum** ソース (**epel**) からインストールする必要があります。
 - **polycoreutils** と **polycoreutils-python** パッケージが同じ **RHEL yum** ソース (**rhel** サーバー) からインストールされていることを確認します。次のコマンドを実行します。

```
semanage port -a -t http_port_t -p tcp 10087
```

```
setsebool -P httpd_can_network_connect 1
```

- ストレージサーバーの **/mnt** フォルダが、どのマウントポイントによっても直接マウントされていないことを確認します。ユーザーマウントポイントはそのサブフォルダに対してマウントされる必要があります。

- 次のコマンドを使用して、**selinux** の **logrotate** 権限を有効にします。

```
semanage permissive -a logrotate_t
```

- 次の条件が満たされた場合にのみ、**SQL Server** バックアップイメージに対してインスタントアクセスがサポートされます。

- スナップショットが、ポリシーまたは保護計画で有効になっています。
- バックアップはデータベースの完全バックアップです。
- プライマリサーバー、メディアサーバー、ストレージサーバー、クライアントはバージョン **8.3** 以降である必要があります。
クラウド **LSU** (論理ストレージユニット) からバックアップコピーを使用してインスタントアクセスする場合、プライマリサーバーとメディアサーバーはバージョン **10.0.1** 以降である必要があります。
クラウド **LSU** (論理ストレージユニット) でのインスタントアクセスの制限事項については、『[NetBackup 重複排除ガイド](#)』を参照してください。
- ストレージサーバーは、以前に指定された前提条件を満たすアプライアンスまたは **BYO** である必要があります。

メモ: 増分バックアップとトランザクションログバックアップのインスタントアクセスは、ベースバックアップイメージのインスタントアクセス機能によって決まります。

インスタントアクセスのハードウェアと構成の必要条件

インスタントアクセスを使用する場合、次のハードウェア要件があります。

表 9-1 ハードウェア構成の必要条件

CPU	メモリ	ディスク
■ 2.2 GHz 以上のクロックレート ■ 64 ビットのプロセッサ ■ 最小 4 コア。8 コアを推奨。64 TB のストレージの場合、Intel x86-64 アーキテクチャでは 8 つのコアを必要とします。	■ 16 GB (8 TB から 32 TB のストレージの場合) ■ 1 TB のストレージの場合は 1 GB の RAM ■ 32 TB 以上のストレージの場合は 32 GB の RAM ■ ライブマウントごとに追加の 500 MB の RAM	ディスクのサイズは、バックアップのサイズによって異なります。 NetBackup とメディアサーバー重複排除プール (MSDP) のハードウェアの必要条件を参照してください。

ドメイン内にある Windows クライアントには、追加の構成要件があります。たとえば、gMSA を使用する SQL Server クライアントなどです。ストレージサーバーの構成要件について詳しくは、次の記事を参照してください。

https://isearch.veritas.com/internal-search/en_US/article.100051793.html

インスタントアクセスデータベースを設定する前の考慮事項

インスタントアクセス SQL Server 機能について、次の点に注意します。

- 次のバックアップオプションまたはシナリオを使用した SQL Server バックアップは、SQL Server インスタントアクセスをサポートしません。
 - アプリケーション対応バックアップ (VMware)
 - ストリームベースのバックアップ
 - NetBackup バックアップ圧縮
 - SQL Server のレガシーバックアップ (バッチファイルを使用)
 - ファイルグループまたはファイルのバックアップ
 - PFI バックアップ (バックアップオプション: [インスタントリカバリ用または SLP 管理用にスナップショットを保持する (Retain snapshot for Instant Recovery or SLP management)])
 - SQL Server データベースミラーリング (スタンドアロンの IA データベースとしての作成のみサポート)

- SQL Server クラスタ (スタンドアロンの IA データベースとしての作成のみサポート)
- Flex WORM ストレージでのインスタントアクセスには、次のサービスが必要です:
 - NGINX、NFS、SAMBA、WINBIND (Active Directory が必要な場合)、SPWS、VPFS
- インスタントアクセスでは、ファイルストリームデータベースのリストアはサポートされません。インスタントアクセスなしで VM 全体をリストアします。または、インスタントアクセスなしでデータベースをリストアします。詳しくは、次の記事を参照してください。
<https://www.veritas.com/docs/100048546>
- ストレージサーバーとプライマリサーバーが NetBackup の以前のバージョンからアップグレードされた後、インスタントアクセスが機能するには、次のコマンドを使用して、アップグレードされたプライマリサーバーで NetBackup Web サービスを再起動します。
 - `/usr/opensv/netbackup/bin/nbwmc stop`
 - `/usr/opensv/netbackup/bin/nbwmc start`

SQL Server インスタントアクセス用の Samba ユーザーの構成

NetBackup クライアントは、Samba 共有にアクセスするために Samba ユーザークレデンシャルを必要とする場合があります。対応するストレージサーバーで SQL Server インスタントアクセス用に Samba ローカルユーザーを構成できます。

ストレージサーバー上の Samba サービスが Windows ドメインの一部である場合は、Windows ドメインユーザーを Samba ユーザーとして使用できます。

AKS (Azure Kubernetes Service) と EKS (Amazon Elastic Kubernetes Service) クラウドプラットフォームの場合、Samba ローカルユーザーのみが Samba 共有にアクセスできます。Samba 共有にアクセスするには、Samba ユーザーを追加する必要があります。

SQL Server インスタントアクセス中に、SQL Server サービスは Samba 共有にアクセスする必要があります。インスタントアクセスデータベースを開始するように Windows ユーザーが指定されている場合、その Windows ユーザーも Samba 共有にアクセスする必要があります。

Windows ユーザーが Samba 共有を利用できるようにする方法

- Windows ユーザーがドメインユーザーであり、ストレージサーバーと同じドメインに存在する場合:
Windows ユーザーは Samba 共有に直接アクセスでき、設定は必要ありません。

- Windows ユーザーがドメインユーザーでなく、ストレージサーバーと同じドメインに存在しない場合:

次のコマンドを実行して、Windows ユーザーの Samba ユーザークレデンシヤルを保存し、Samba アカウントのパスワードを入力します。

```
cmdkey /add:<Samba hostname> /user:<Samba account username> /pass
```

Windows ユーザーは、クレデンシヤルを使用して Samba 共有にアクセスします。

SQL Server サービスが Samba 共有を利用できるようにする方法

- SQL Server サービスが Windows ユーザーとしてログオンする場合は、次のトピックを参照してください。

p.100 の「[Windows ユーザーが Samba 共有を利用できるようにする方法](#)」を参照してください。

- SQL Server サービスがサービスアカウント (NT Service\MSSQLSERVER など) としてログオンする場合

- SQL Server Windows ホストがストレージサーバーと同じドメインに存在する場合:

SQL Server サービスはドメインホストとして認証され、構成は必要ありません。

- SQL Server の Windows ホストがどのドメインにもなく、Samba ゲストアクセスが無効でない場合、SQL Server サービスはゲストとして共有にアクセスできるため、設定は必要ありません。

- 他のすべてのシナリオでは、次の SQL 文を実行して SQL Server サービスアカウントの Samba セッションを作成します。

```
xp_cmdshell 'net use ¥¥<Samba hostname>¥<sharename> <Samba account password> /user:<Samba account username>'
```

SQL Server サービスは、指定された Samba ユーザークレデンシヤルを使用して Samba 共有にアクセスします。共有名は、ストレージサーバーで利用可能な共有である必要があります。そのときに共有がない場合は、共有を作成する必要があります。

Samba セッションは、次の再起動まで有効です。Samba アクセスを取得するには、再起動後にコマンドを再実行する必要があります。

xp_cmdshell が SQL Server に対して有効になっていない場合は、次のコマンドを使用して xp_cmdshell を有効または無効にします。

```
-- enable xp_cmdshell
EXEC sp_configure 'show advanced options', '1'

RECONFIGURE

EXEC sp_configure 'xp_cmdshell', '1'

RECONFIGURE
```

```
-- disable xp_cmdshell
EXEC sp_configure 'show advanced options', '1'

RECONFIGURE

EXEC sp_configure 'xp_cmdshell', '0'

RECONFIGURE
```

次の表では、Samba サービスが Windows ドメインに含まれていない場合に Samba ユーザーを追加または管理する方法を説明します。

表 9-2 Samba ユーザーを追加または管理する手順

ユーザー	手順
NetBackup Appliance ユーザーの場合	NetBackup Appliance の場合、ローカルユーザーは Samba ユーザーでもあります。 ローカルユーザーを管理するには、CLISH にログインし、[Main]>[Settings]>[Security]>[Authentication]>[LocalUser]の順に選択します。 Samba パスワードは、アプライアンスのローカルユーザーのログインパスワードと同じです。
Flex Appliance ユーザーの場合	Flex Appliance アプリケーションインスタンスの場合、インスタンスにログインし、次のようにローカルユーザーを Samba に追加します。 ◆ 必要に応じて、次のコマンドを使用して新しいローカルユーザーを作成します。 ■ #useradd <username> ■ #passwd <username> 既存のローカルユーザーを使用することもできます。 ◆ 次のコマンドを実行して Samba のユーザークレデンシャルを作成し、ユーザーを有効にします。 ■ smbpasswd -a <username> ■ smbpasswd -e <username>

ユーザー	手順
BYO (Build Your Own) ユーザーの場合	新規ユーザーの場合: - Linux ユーザーを作成して Samba に追加します。 たとえば、次のコマンドを実行すると、Samba サービス専用の <code>test_samba_user</code> が作成されます。 <pre># adduser --no-create-home -s /sbin/nologin test_samba_user</pre> <pre># smbpasswd -a test_samba_user</pre> - 新しい SMB パスワードを入力します。 - 新しい SMB パスワードを再入力します。 新しいユーザーが追加されます。 既存のユーザーの場合: Samba サービスに既存のユーザーを追加する場合は、次のコマンドを実行します: <code>smbpasswd -a test_samba_user</code>
AKS および EKS プラットフォームユーザーの場合	新規ユーザーの場合: <code>kubectl</code> を使用してクラスタの MSDP エンジンポッドにログインします。 - 次のコマンドを実行して、MSDP エンジンの <code>rshell</code> にログインします。 <pre>su - msdpadm</pre> - 次の <code>rshell</code> コマンドを実行して、Samba ユーザーを追加します。 <pre>setting samba add-user username=[samba user name] password=[samba password]</pre> 例: <pre>msdp-16.1] > setting samba add-user username=test_samba_user password=Te@Pss1fg0</pre> 同じコマンドを使用して、既存のユーザーのパスワードを更新できます。 AKS および EKS クラウドプラットフォームでは、Samba <code>rshell</code> コマンドによって、クラスタ内のすべての MSDP エンジンに Samba サーバーが構成されます。

SQL Server データベースを自動的に起動するには、Web UI からインスタンスのクレデンシャルを使用してログオンするときに、共有にアクセスできることを確認します。

AKS や EKS などのクラウドプラットフォームの場合は、Windows クレデンシャルマネージャに Samba ユーザーと各 MSDP エンジンホスト名を追加します。この処理により、NetBackup クライアントはインスタントアクセス Samba 共有に自動的に接続できます。

インスタントアクセスデータベースの構成

インスタントアクセスデータベースを構成する際に、データベースをインスタンスに自動的に追加するように選択できます。または、Samba 共有にデータベースをエクスポートできます。

インスタントアクセスデータベースの構成とデータベースの開始

インスタントアクセスデータベースを構成し、インスタンスにデータベースを自動的に追加するには、完全バックアップ、増分バックアップ、トランザクションログバックアップを使用できます。

インスタントアクセスデータベースを構成してデータベースを開始するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 2 [データベース (Databases)]タブで、インスタントアクセスデータベースを構成するデータベースをクリックします。
- 3 [リカバリポイント (Recovery points)]タブをクリックし、バックアップが発生した日付をクリックします。

利用可能なイメージは、各イメージのバックアップタイムスタンプ付きで各行に表示されます。
- 4 バックアップイメージを見つけ、[処理 (Actions)]、[インスタントアクセスの構成 (Configure instant access)]の順に選択します。
- 5 (条件付き) 完全バックアップでは、インスタントアクセスデータベースが作成された後、データベースをインスタンスに追加し、データベースを起動できます。このオプションで[はい (Yes)]、[次へ (Next)]をクリックします。
- 6 (条件付き) トランザクションログに対して、リプレイオプションを選択して[次へ (Next)]をクリックします。
- 7 リカバリ対象とホスト名、インスタンス名を確認し、必要に応じて変更を行います。

ホストとインスタンスを変更するには、[インスタンスを変更 (Change instance)]をクリックします。
- 8 [データベース名 (Database name)]フィールドに、作成するインスタントアクセスデータベースの名前を入力します。

- 9 リカバリターゲットのクレデンシャルを入力します。または、[既存のクレデンシャルの選択 (Select existing credentials)]をクリックして、使用するクレデンシャルを選択します。

ユーザーアカウントは Windows 管理者グループのメンバーである必要があり、ローカルの SQL Server sysadmin の役割のメンバーである必要があります。

- 10 [次へ (Next)]をクリックします。
- 11 リカバリオプションを確認し、必要に応じて変更を加え、[次へ (Next)]をクリックします。

p.107 の「[NetBackup for SQL Server インスタントアクセスのオプション](#)」を参照してください。

- 12 (オプション) 選択したリカバリポイントのバックアップイメージのリストを表示するには、バックアップイメージの数を表示するリンクをクリックします。
- 13 選択したリカバリターゲットとリカバリオプションの概略を確認します。次に、[リカバリの開始 (Start recovery)]をクリックします。
- 14 インスタントアクセスジョブが開始された後、[リストアアクティビティ (Restore activity)]タブをクリックして進捗状況を表示できます。

p.106 の「[インスタントアクセスデータベースのライブマウントの詳細の表示](#)」を参照してください。

インスタントアクセスデータベースを構成して、データベースを開始しない

インスタントデータベースを設定し、Samba 共有にデータベースをエクスポートするには、完全バックアップを使用する必要があります。

インスタントアクセスデータベースを構成して、データベースを開始しないようにするには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 2 [データベース (Databases)]タブで、インスタントアクセスデータベースを構成するデータベースをクリックします。
- 3 [リカバリポイント (Recovery points)]タブをクリックし、バックアップが発生した日付をクリックします。

利用可能なイメージは、各イメージのバックアップタイムスタンプ付きで各行に表示されます。

- 4 バックアップイメージを見つけ、[処理 (Actions)]、[インスタントアクセスの構成 (Configure instant access)]の順に選択します。
- 5 データベースをインスタンスに追加してデータベースを起動する場合は、[いいえ (No)]、[次へ (Next)]の順に選択します。
- 6 リカバリ対象として、次のオプションのいずれかを選択します。

- リカバリターゲットのホスト名を入力するには、[ホスト名の入力 (Enter host name)]をクリックします。
 - ホストのリストから選択するには、[ホスト名を選択 (Select host name)]をクリックします。
- 7 (オプション) 選択したリカバリポイントのバックアップイメージのリストを表示するには、バックアップイメージの数を表示するリンクをクリックします。
 - 8 [リカバリの開始 (Start recovery)]をクリックします。
 - 9 インスタントアクセスジョブが開始された後、[リストアアクティビティ (Restore activity)]タブをクリックして進捗状況を表示できます。
- p.106 の「[インスタントアクセスデータベースのライブマウントの詳細の表示](#)」を参照してください。

インスタントアクセスデータベースのライブマウントの詳細の表示

インスタントアクセスデータベースのライブマウントの詳細を表示できます。

インスタントアクセスデータベースのライブマウントの詳細を表示するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 2 [インスタントアクセスデータベース (Instant access databases)]タブをクリックします。
- 3 [インスタントアクセスデータベース (Instant Access databases)]タブで、ライブマウントの詳細を表示するデータベースをクリックします。

マウント ID (Mount ID) インスタントアクセスのライブマウントの一意の ID。

エクスポートパス (Export path) ストレージサーバーからエクスポートされたインスタントアクセスのライブマウントパス。

リカバリポイント ID (Recovery point ID) リカバリポイントの一意の ID。

ライブマウントパス (Livemount path) Microsoft SQL クライアント上のインスタントアクセスのライブマウントの UNC パス。

エクスポートサーバー (Export server) ライブマウント共有のエクスポート元のサーバー。

インスタントアクセスデータベースの削除

インスタンスに追加できるかどうか不明なインスタントアクセスデータベースを削除できません。

インスタントアクセスデータベースを削除するには

- 1 左側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順に選択します。
- 2 [インスタントアクセスデータベース (Instant access databases)]タブをクリックします。
 このタブには、構成済みのインスタントアクセスデータベースの名前が一覧表示されます。
- 3 インスタントアクセスデータベースを選択します。
- 4 [削除 (Delete)]をクリックします。
- 5 次のいずれかのシナリオに基づいて、該当する手順を実行します。

インスタントアクセスデータベースがインスタンスに追加され、開始されます。	SQL Server インスタンスのクレデンシャルを入力し、[削除 (Delete)]をクリックします。
--------------------------------------	--

インスタントアクセスデータベースがインスタンスに追加されず、開始されません。	データベースを削除する場合は、[削除 (Delete)]をクリックします。
--	---------------------------------------

NetBackup for SQL Server インスタントアクセスのオプション

この表では、インスタントアクセスを実行するときに利用可能なリカバリオプションについて説明します。

表 9-3 リカバリオプション

オプション	説明
リストア後のデータベースのリカバリ状態 (Database recovery state after restore)	リストア後にデータベースの状態を選択します。 ■ リカバリ (Recover) リストアシーケンスの最後のイメージをリストアし、データベースを使用できるようにします。 ■ リストアしています (Restoring) 中間バックアップイメージをリストアします。データベースはロード状態のままになるため、追加のバックアップイメージをリストアして適用できます。 ■ スタンバイ (Standby) トランザクションログおよびデータベースのリストア時に、スタンバイデータベースを作成して保持します。このオプションを選択する場合は、スタンバイの取り消しログが必要です。このログは、デフォルトではプライマリデータファイルと同じディレクトリにあります。SQL Server サービスを実行するアカウントには SQLStandBy フォルダのフルアクセス権が必要です。
一貫性チェック (Consistency check)	リストア後に実行する一貫性チェック。一貫性チェックからの出力は、SQL Server クライアントの進捗ログに書き込まれます。 ■ 実行しない (Do not perform) 一貫性チェックを実行しません。 ■ インデックスを含む完全チェック (Full check, including indexes) 一貫性チェックにインデックスを含めます。エラーはログに記録されます。 ■ インデックスを含まない完全チェック (Full check, excluding indexes) 一貫性チェックからインデックスをエクスクルードします。インデックスを選択しない場合、一貫性チェックの実行速度は大幅に向上しますが、完全にはチェックされません。一貫性チェックでは、各ユーザー表のデータページおよびクラスタ化インデックスページだけが対象となります。クラスタ化されていないインデックスページの一貫性は選択されません。 ■ カタログのチェック (Check catalog) 指定したデータベースのシステムテーブル内およびシステムテーブル間の一貫性をチェックします。 ■ 物理チェックのみ (Physical check only) 少ないオーバーヘッドで SQL Server データベースの物理的一貫性をチェックします。このオプションでは、ページヘッダーおよびレコードヘッダーの物理構造の整合性のみを検証します。また、ページのオブジェクト ID やインデックス ID と割り当て構造の間の一貫性もチェックします。
VDI タイムアウト (VDI timeout)	SQL Server 仮想デバイスインターフェースのタイムアウト間隔を指定します。選択した間隔は、データベースとトランザクションログのバックアップとリストアに適用されます。バックアップのデフォルト値は 300 です。リストア操作のデフォルト値は 600 です。範囲は 300 から 2147483647 です。

p.104 の「[インスタントアクセスデータベースの構成](#)」を参照してください。

NetBackup for SQL Server の用語

この表に、SQL Server データベース管理者または NetBackup 管理者にとって重要な新規用語を示します。

表 9-4 NetBackup for SQL Server の用語

用語	定義
完全バックアップ (Full backup)	すべてのデータファイルとログファイルが含まれるデータベースの完全なバックアップ。(完全バックアップでは、トランザクションログは切り捨てられません。)
増分バックアップ (Incremental backup)	最後の完全バックアップ以降に変更されたブロックのバックアップ。
トランザクションログ (Transaction log)	データベースに対して実行された更新に関する進行中のレコード。
トランザクションログのバックアップ	最後のトランザクションログのバックアップ以降に発生したトランザクションをバックアップします。バックアップが正常に完了すると、ログは消去され、新しいトランザクションをファイルに書き込むことができます。トランザクションログのバックアップは、完全リカバリモデルで実行するように設定されたデータベースに対してのみ実行できます。
リストア (Restore)	データを SQL Server オブジェクトにコピーして戻すこと。
リカバリ (Recovery)	リストアの結果としてデータベースをオンラインにすること。
SQL Server ホスト	SQL Server が存在するホストマシン。SQL Server のインストールをサポートするクラスタの仮想名を指すこともあります。
SQL Server インスタンス	SQL Server のインストール。インスタンスが指定されていない場合は、SQL ホストのデフォルトの SQL インスタンスと見なされます。

よく寄せられる質問

ここでは、BYO (Build Your Own) の Microsoft SQL インスタントアクセスについてよく寄せられる質問をいくつかご紹介します。

表 9-5

適用対象	よく寄せられる質問	回答
BYO	nginx サービスをインストールせずにストレージを構成またはアップグレードした後に、BYO で Microsoft SQL Server インスタントアクセス機能を有効にする方法を教えてください。	次に示す順序で操作を実行します。 1 必要な nginx サービスのバージョンをインストールします。 2 新しい BYO nginx 構成エントリ <code>/etc/nginx/conf.d/byo.conf</code> が、元の <code>/etc/nginx/nginx.conf</code> ファイルの HTTP セクションに含まれていることを確認します。 3 コマンド <code>/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</code> を実行します。
BYO	「MSDP REST API がポート 10087 の HTTPS を介して利用可能であることの確認」で触れている <code>vpfs-config.log</code> ファイルで発生した問題を解決するには、どのようにしたら良いですか。	次に示す順序で操作を実行します。 1 YUM ツールを使用して、 <code>polycoreutils</code> と <code>polycoreutils-python</code> パッケージをインストールします。 2 Nginx の SELinux に必要な次のルールを追加し、10087 ポートにバインドします。 ■ <code>semanage port -a -t http_port_t -p tcp 10087</code> ■ <code>setsebool -P httpd_can_network_connect 1</code> 3 コマンド <code>/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</code> を実行します。

適用対象	よく寄せられる質問	回答
BYO	BYO のインスタントアクセスでは、デフォルトで自己署名証明書が使用され、*.pem 外部証明書のみがサポートされます。 外部 CA (*.pem 証明書) で署名された証明書で置き換えるが必要な場合は、どのようにしたら良いですか。	外部証明書を構成するには、次の手順を実行します。新しい証明書がすでに生成されている場合 (証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります) は、手順 4 に進みます。 1 RSA の公開鍵と秘密鍵のペアを作成します。 2 証明書の署名要求 (CSR) を作成します。 証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります。 3 外部認証局が証明書を作成します。 4 <PDDE ストレージのパス >/spws/var/keys/spws.cert を証明書に置き換え、<PDDE ストレージのパス >/spws/var/keys/spws.key を秘密鍵に置き換えます。 5 次のコマンドを実行して、証明書を再ロードします。 /usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo
BYO	GNOME のインスタントアクセスライブマウント共有で、メディアの自動マウントを無効にする方法を教えてください。 自動マウントが有効になっている場合、ソースフォルダは GNOME のライブマウント共有からマウントされ、小さなディスクが表示されます。このシナリオでは、インスタントアクセス機能が正しく動作しません。 マウントされたディスクコンテンツソースは、ライブマウント共有配下の .../meta_bdev_dir/... フォルダにあり、マウントターゲットは /run/media/... フォルダにあります。	次のガイドラインに従って、GNOME 自動マウントを無効にします。 https://access.redhat.com/solutions/20107

適用対象	よく寄せられる質問	回答
BYO	/var/log/vpfs/vpfs-config.log ファイルの次の問題は、どうすれば解決できますか。 <pre>**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) ****</pre> /usr/opensv/netbackup/bin/nblibcurlcmd failed (1):	次に示す順序で操作を実行します。 1 NetBackup プライマリサーバーが起動しており、ファイアウォールが NetBackup プライマリサーバーとストレージサーバー間の接続をブロックしていないことを確認します。 2 ストレージサーバーで次のコマンドを実行して、接続状態を確認します。 <pre>/usr/opensv/netbackup/bin/bpcintcmd -pn</pre> 3 NetBackup プライマリサーバーを起動し、NetBackup プライマリサーバーとストレージサーバー間の接続を許可してから、次のコマンドを実行します。 <pre>/usr/opensv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</pre>

適用対象	よく寄せられる質問	回答
BYO と Flex Appliance	SQL Server インスタントアクセスが特定の Windows クライアントで機能するように、Samba 共有のホストベースの認証を有効にしてログオンをセキュリティで保護する方法を教えてください。	次に示す順序で操作を実行します。 1 Samba 共有のエクスポート元のストレージサーバーで、1 回限りの操作として次の操作を行います。 ■ 次の Samba オプションを上書きしてゲストログインを無効にします。 map to guest = Never ■ Samba のユーザークレデンシャルを作成します。 ■ smbpasswd -a spws Samba ユーザー spws の Samba パスワードを設定 ■ smbpasswd -e spws Samba ユーザー spws を有効化 2 以前のクレデンシャルを使用して Samba 共有にアクセスする各 Windows クライアントの資格情報マネージャで、spws クレデンシャルを保存します。 3 Windows クライアントに Samba クレデンシャルを保存するには、[コントロールパネル]、[ユーザーアカウント]、[資格情報マネージャ]、[Windows 資格情報の追加]の順に移動します。 4 [インターネットまたはネットワークのアドレス]に、ストレージサーバーのドメイン名を入力します。 5 Samba のユーザー名とパスワードを入力します。 ユーザー名が、Samba 用に作成したユーザークレデンシャルと同じであることを確認します。 6 [OK]をクリックして、ログオンプロンプトなしで<ストレージサーバーのドメイン名>にアクセスできることを確認します。

適用対象	よく寄せられる質問	回答
NetBackup Appliance	MSSQL インスタントアクセスが NetBackup Appliance と Windows クライアントで機能するように、Samba 共有のホストベースの認証を有効にしてログオンをセキュリティで保護する方法を教えてください。	次に示す順序で操作を実行します。 Samba 共有のエクスポート元のストレージサーバーで 1 回限りの操作として、Samba の新しいローカルユーザーのクレデンシアルを次の Appliance CLISH パスで作成します。 Main_Menu > Settings > Security > Authentication > LocalUser - 以前のクレデンシアルを使用して Samba 共有 にアクセスする各 Windows クライアントの資格情報マネージャで、新しいローカルユーザークレデンシアルを保存します。 アプライアンスの場合、smb.conf ファイル構成にはすでに「map to guest = Never」が含まれています。 ローカルユーザーは Samba データベースに自動的に追加され、Samba パスワードはログオンパスワードと同じです。Windows クライアントは、アプライアンスのローカルユーザーのクレデンシアルを使用してアプライアンスの Samba 共有 にアクセスできます。 次に示す順序で操作を実行します。 - アプライアンスのローカルユーザーを管理するには、次の CLISH パスにアクセスします。 Main_Menu > Settings > Security > Authentication > LocalUser Windows クライアントに Samba クレデンシアルを保存するには、[コントロールパネル]、[ユーザーアカウント]、[資格情報マネージャ]、[Windows 資格情報の追加]の順に移動します。 [インターネットまたはネットワークのアドレス]に、ストレージサーバーのドメイン名を入力します。 Samba のユーザー名とパスワードを入力します。 [OK]をクリックして、ログオンプロンプトなしで <ストレージサーバーのドメイン名> にアクセスできることを確認します。

VMware バックアップを使用した SQL Server の保護

この章では以下の項目について説明しています。

- VMware バックアップを使用したアプリケーションデータベースの保護について
- SQL Server を保護する NetBackup for VMware バックアップの構成について
- SQL Server を保護する VMware バックアップポリシーの構成
- スナップショットレプリケーションの管理に Replication Director を使用して SQL Server を保護するための VMware ポリシーの構成
- SQL Server データを保護するための VMware バックアップを使用した保護計画の作成
- VMware バックアップを使用した SQL Server データの保護
- VMware バックアップからの SQL Server データベースのリストア

VMware バックアップを使用したアプリケーションデータベースの保護について

VMware のバックアップポリシーおよび Veritas VSS プロバイダを使用することで、NetBackup では仮想マシンに存在するアプリケーションデータベースの一貫した完全バックアップを作成できます。

VMware アプリケーションバックアップでは次のことができます。

- ログを切り捨てるかどうかを選択します。
- VMware バックアップからデータをリストアおよびリカバリするには、既存のデータベースリストア処理を使用します。

- 1 つの VMware バックアップから、ボリュームレベルのリストア、ファイルレベルのリカバリ、またはデータベースのリストアのリストアオプションを選択します。
- [T-SQL スナップショットを有効化する (Enable T-SQL snapshots)] オプションを指定すると、SQL Server の増分バックアップおよびトランザクションログバックアップの基礎として使用できる SQL Server の完全バックアップが (コピーのみではなく) NetBackup によって作成されます。T-SQL スナップショットは SQL Server 2022 で追加され、SQL Server 2022 以降のシステムで強く推奨されます。この形式のスナップショットは、SQL Server 2019 以前ではサポートされていません。
- VMware バックアップから代替クライアントにデータベースをリストアおよびリカバリします。ターゲットとなる宛先クライアントには、物理コンピュータまたは仮想マシンを使うことができます。

サポートされている環境と構成

仮想システムの互換性については、次の情報を参照してください。

https://www.veritas.com/content/support/en_US/doc/NB_70_80_VE

Veritas VSS プロバイダ

Veritas は、Veritas VSS プロバイダを推奨します。VMware ツールはこのプロバイダを呼び出し、ファイルレベルの一貫したバックアップのために VSS ライターを静止します。この VSS プロバイダ (または VMware VSS プロバイダ) がいない場合、データベースリカバリに手動での手順が必要になることがあり、個別リカバリはサポートされません。

p.15 の「vSphere 用の Veritas VSS プロバイダのインストール」を参照してください。

Veritas VSS プロバイダを使用すると、VMware バックアップで SQL Server 仮想マシンのログを切り捨てることができます。Veritas VSS プロバイダは、完全 VSS バックアップによってログを切り捨てます。VMware VSS プロバイダでは、ログを切り捨てるための基準として使用できない、コピーのみバックアップが作成されます。

SQL Server VSS Writer サービスの無効化

T-SQL スナップショットを使用した VMware バックアップの場合は、SQL Server VSS Writer サービスも無効にする必要があります。

p.16 の「SQL Server VSS Writer サービスの無効化」を参照してください。

NetBackup アクセラレータを使用した VMware の完全バックアップの高速化

[アクセラレータを使用 (Use Accelerator)] ポリシーオプションを選択して、NetBackup アクセラレータを使用すると、VMware の完全バックアップが高速化される可能性があります。(このオプションは保護計画の設定では利用できません) バックアップ時間の短縮によって、VMware バックアップをバックアップ処理時間帯内に簡単に完了できるようになります。この機能を使うには、最初に [アクセラレータを使用 (Use Accelerator)] を有効にして初回バックアップを実行する必要があります。以降のバックアップ時間はかなり減

らすことができます。現在、バックアップが完全スケジュール形式に対してのみ制限されているデータベースエージェントに対するアクセラレータのサポート。

クライアントの変更検出の新しい基準を定期的に確立するには、[アクセラレータ強制再スキャン (Accelerator forced rescan)] オプションを有効にして個別のポリシースケジュールを作成します。

VMware バックアップでアクセラレータを使用する方法について詳しくは、『[NetBackup for VMware 管理者ガイド](#)』を参照してください。

SQL Server のアプリケーション保護を設定した VMware ポリシーでアクセラレータを使用するには、アクセラレーションを最適化するために、以前のバックアップが正常に完了している必要があります。バックアップジョブまたは子ジョブ (ASC を含む) は、未完了の状態 (状態 1) を持つことができます。その場合、バックアップイメージは後続のジョブのベースバックアップとは見なされず、そのジョブのアクセラレーションの最適化はゼロです。

VMware アプリケーションバックアップの制限事項

データベースは、VMware バックアップのためにサポートされる構成の場合にのみカタログ化され、保護されます。必ず、サポート対象のストレージにデータベースとトランザクションログを格納してください。

VMware アプリケーションバックアップでは、次のポリシーオプションと構成はサポートされていません。

- 増分バックアップ。代わりに、SQL Server 増分バックアップの保護計画またはポリシーを作成できます。
- SQL Server クラスタまたは SQL Server 可用性グループ。
- (NetBackup Web UI のみ) プライマリコピー以外のコピーからリストアします。プライマリコピーからのみリストアできます。他のコピーがあっても、リストア用に表示されるのはプライマリコピーのみです。別のコピーからリストアする場合は、そのコピーをプライマリコピーに昇格します。
- SQL Server データベースが次の場所にある場合は、データベースはカタログ化されず、バックアップされません。
 - Raw デバイスマッピング (RDM) を使用するすべての仮想マシン。
 - 独立としてマークされている仮想マシンディスク (vmdk) ボリューム。
 - MBR ディスクを使用するマウントポイント。SQL Server データベースファイルを含むマウントポイントは、ベースになるディスクが GPT ディスクの場合にのみサポートされます。
 - 仮想ハードディスク (VHD)。
 - RAID ボリューム。

- ReFS ファイルシステム。
- 除外された Windows ブートディスク。
- T-SQL スナップショットを使用する VMware バックアップには、次の制限事項が適用されます。
 - T-SQL スナップショットには SQL Server 2022 が必要です。ゲスト仮想マシンに異なるバージョン (2019 と 2022 など) の複数の SQL Server インスタンスがあり、T-SQL スナップショットが有効な場合、ポリシーは SQL Server 2022 のインスタンスまたはデータベースのみを保護します。
 - NetBackup は同時に処理できるデータベースの数を 62 に制限します。
 - ユーザーデータベースのみが保護されます。この方法では、システムデータベースを保護できません。これは Microsoft 社の制限事項です。(ポリシーにはシステムデータベースを含めることができますが、NetBackup はこれらのデータベースをスキップします。)
 - ログの切り捨ては T-SQL スナップショットではサポートされません。

SQL Server を保護する NetBackup for VMware バックアップの構成について

表 10-1 SQL Server を保護する VMware バックアップの構成手順

手順	処理	説明
手順 1	NetBackup サービスのログオンアカウントを構成します。	NetBackup Client Service と NetBackup Legacy Network Service のログオンアカウントは、特定の要件を満たす必要があります。 p.17 の「SQL Server のバックアップとリストアのための NetBackup サービスの設定」を参照してください。 p.18 の「SQL Server のローカルセキュリティの権限の構成」を参照してください。
手順 2	Replication Director を使って VMware スナップショットとスナップショットレプリカを管理する場合は、ストレージライフサイクルポリシー (SLP) を作成します。	『 NetBackup Replication Director ソリューションガイド 』を参照してください。
手順 3	VMware ポリシーを構成します。	p.119 の「SQL Server を保護する VMware バックアップポリシーの構成」を参照してください。 p.121 の「スナップショットレプリケーションの管理に Replication Director を使用して SQL Server を保護するための VMware ポリシーの構成」を参照してください。

手順	処理	説明
手順 4	[VM ホスト名 (VM hostname)]ではなく [プライマリ VM 識別子 (Primary VM identifier)]を使用する場合は、VM のホスト名にその識別子をマッピングする必要があります。	プライマリサーバーの[分散アプリケーションリストアマッピング (Distributed Application Restore Mapping)]ホストプロパティで、このマッピングを設定します。 p.27 の「 分散アプリケーション、クラスタ、または仮想マシンのリストアマッピングの設定 」を参照してください。
手順 5	環境内のホストの自動検出マッピングを確認します。	NetBackup が環境内で検出した有効な自動検出マッピングそれぞれを承認します。プライマリサーバーの[ホスト管理 (Host Management)]プロパティで、この設定を実行します。 p.19 の「 自動検出されたマッピングの確認 」を参照してください。

SQL Server を保護する VMware バックアップポリシーの構成

VMware のバックアップポリシーを使用して、NetBackup では仮想マシンに存在する SQL Server データベースのアプリケーションの一貫した完全バックアップを作成できます。必要に応じて、NetBackup アクセラレータを使用できます。VMware ポリシーを使用して、VMware バックアップから特定の仮想ディスクを除外できます。特定の SQL Server コンポーネントを除外する場合は、MS-SQL-Server ポリシーを使用します。

ログを切り捨てるには、まずログの切り捨てなしで VMware の完全バックアップを実行する必要があります。このバックアップが完了したら、ポリシーでログの切り捨てを有効にします。

ポリシーを作成する前に、追加の構成要件を実行する必要があります。

p.118 の「[SQL Server を保護する NetBackup for VMware バックアップの構成について](#)」を参照してください。

アクセラレータについて詳しくは次を参照してください。

『[NetBackup 管理者ガイド Vol. 1](#)』を参照してください。

SQL Server を保護する VMware バックアップポリシーを構成するには

- 1 NetBackup Web UI を開きます。
- 2 左側で[保護 (Protection)]、[ポリシー (Policies)]の順に選択します。
- 3 新しいポリシーを追加するか、編集するポリシーを開きます。
- 4 [属性 (Attributes)]タブをクリックします。
 - [ポリシー形式 (Policy type)]リストから、[VMware]を選択します。
 - [ポリシーストレージ (Policy storage)]リストで、ディスクストレージユニットを選択します。

NetBackup アクセラレータを使用する場合は、サポート対象のストレージユニット形式を選択します。サポート対象のストレージ形式はすべて、NetBackup のデバイスマッピングファイルに一覧表示されています。

- NetBackup アクセラレータを使用する場合は、[アクセラレータを使用 (Use Accelerator)]をクリックします。
 アクセラレータは初回の完全バックアップを使って基準を確立します。アクセラレータを使って実行される以降のバックアップは非常に高速に実行できます。
 [アクセラレータ強制再スキャン (Accelerator forced rescan)]オプションを有効にするための追加のポリシースケジュールを作成することもできます。このオプションにより、次のアクセラレータバックアップ用の新しい基準が確立されます。
 [Block Level Incremental (BLI) バックアップを実行する (Perform block level incremental backups)]が自動的に選択され、灰色で表示されます。[VMware] タブで[Block Level Incremental (BLI) バックアップを有効にする (Enable block-level incremental backup)]オプションも選択され、灰色で表示されます。
- 5 [スケジュール (Schedules)]タブで、完全バックアップのスケジュールを作成します。
- 6 [クライアント (Clients)]タブで、次の操作を実行します。
 - [VMware インテリジェントポリシーの問い合わせを通じて自動的に選択 (Select automatically through VMware intelligent policy query)]をクリックします。
 - [仮想マシンの自動選択を実行するための NetBackup ホスト (NetBackup host to perform automatic virtual machine selection)]から、使用したいホストを選択します。
 - 問い合わせビルダーを使用して、バックアップする仮想マシンを選択する規則を作成します。
- 7 [VMware]タブで、次の操作を実行します。
 - バックアップのカタログ化に使用する[プライマリ VM 識別子 (Primary VM identifier)]を選択します。
 - [VM バックアップからのファイルリカバリを有効にする (Enable file recovery from VM backup)]を選択します。
 - [アプリケーション保護 (Application protection)]を特定し、[Microsoft SQL Server]をクリックします。
 このオプションは、仮想マシンのバックアップからのデータベースのリカバリを可能にします。このオプションが無効になっている場合、バックアップで仮想マシン全体をリカバリできますが、データベースは個別にリカバリできません。
 - この時点では、[ログを切り捨てる (Truncate logs)]を有効にしないでください。
 この手順の後のほうの説明に従って、最初に、ログの切り捨てを行わずに完全バックアップを実行する必要があります。
 - (該当する場合) [T-SQL スナップショットを有効化する (Enable T-SQL snapshots)]を選択します。

このスナップショット形式では、SQL Server の増分バックアップおよびトランザクションログバックアップの基礎として使用できる SQL Server の完全バックアップが(コピーのみではなく)作成されます。このスナップショット形式では、[スナップショットが存在する場合はバックアップを停止する (Stop the backup if any snapshots exist)]がスナップショットを処理する場合に唯一有効なオプションであり、自動的に選択されます。

注意: T-SQL スナップショットは SQL Server 2022 で追加され、SQL Server 2022 以降のシステムで強く推奨されます。この形式のスナップショットは、SQL Server 2019 以前ではサポートされていません。

- 8 VMware バックアップから特定のディスクを除外する場合は、[ディスクを除外 (Exclude disks)]タブをクリックします。

NetBackup は、SQL Server を保護する VMware バックアップからそれらのディスクを除外します。除外するディスクにデータベースのデータが含まれないようにしてください。
- 9 [保存 (Save)]をクリックしてポリシーを保存します。

トランザクションログを切り捨てない場合、これ以上の処理は必要ありません。
トランザクションログを切り捨てる場合は、手順 10 に進みます。
- 10 ログの切り捨てを行わずに完全バックアップを実行します。

バックアップが完了したら、手順 1 で作成したポリシーを開きます。
- 11 [VMware]タブをクリックします。
- 12 [アプリケーション保護 (Application protection)]を特定し、[Microsoft SQL Server]をクリックします。次に、[ログを切り捨てる (Truncate logs)]をクリックします。

SQL Server の場合、このオプションは仮想マシンの VMware スナップショットが完了したときにトランザクションログを切り捨てます。
- 13 [保存 (Save)]をクリックしてポリシーを保存します。
- 14 VMware の完全バックアップを実行します。

スナップショットレプリケーションの管理に Replication Director を使用して SQL Server を保護するための VMware ポリシーの構成

このトピックでは、スナップショットレプリケーションの管理に Replication Director を使用して SQL Server をバックアップするための VMware ポリシーの構成方法について説明します。NetBackup が NetApp ディスクアレイ上の CIFS 共有にアクセスする必要があることに注意してください。VMware ポリシーについて詳しくは、『[NetBackup for VMware 管理者ガイド](#)』を参照してください。

VMware バックアップで Replication Director を設定する方法については、『[NetBackup Replication Director ソリューションガイド](#)』を参照してください。

スナップショットレプリケーションの管理に Replication Director を使用した SQL Server をバックアップするための VMware ポリシーの構成方法

- 1 NetBackup Web UI を開きます。
- 2 左側で[保護 (Protection)]、[ポリシー (Policies)]の順に選択します。
- 3 ポリシーを作成するか、構成するポリシーを開きます。
- 4 [属性 (Attributes)]タブをクリックします。
 - [ポリシー形式 (Policy type)]リストから、[VMware]を選択します。
 - [ポリシーストレージ (Policy storage)]リストで、使用したいストレージライフサイクルポリシー (SLP) を選択します。スナップショットとスナップショットレプリケーションのためにこの SLP を設定する必要があります。
 - Snapshot Client および Replication Director グループで、[Replication Director を使用 (Use Replication Director)]をクリックします。
- 5 [スケジュール (Schedules)]タブで、完全バックアップのスケジュールを作成します。
- 6 [クライアント (Clients)]タブで、次の操作を実行します。
 - [問い合わせを使用して自動的に選択 (Select automatically through query)]をクリックします。
 - バックアップする仮想マシンを選択する規則を作成するには、問い合わせビルダーを使用します。
 - [仮想マシンの自動選択を実行するための NetBackup ホスト (NetBackup host to perform automatic virtual machine selection)]と使用するホストを選択します。
- 7 [VMware]タブで、次のオプションを有効にします。
 - バックアップのカタログ化に使用する[プライマリ VM 識別子 (Primary VM identifier)]
 - [VM バックアップからのファイルリカバリを有効にする (Enable file recovery from VM backup)]
このオプションは、SQL Server のアプリケーション保護を有効にします。
 - [アプリケーション保護 (Application protection)]を特定し、[Microsoft SQL Server]をクリックします。
このオプションは、仮想マシンのバックアップからの SQL データベースのリカバリを有効にします。このオプションが無効になっている場合、バックアップで仮想マシン全体をリカバリできますが、データベースは個別にリカバリできません。

- この時点では、[ログを切り捨てる (Truncate logs)]を有効にしないでください。この手順の後のほうの説明に従って、最初に、ログの切り捨てを行わずに完全バックアップを実行する必要があります。
 - (該当する場合) [T-SQL スナップショットを有効化する (Enable T-SQL snapshots)]を選択します。
このスナップショット形式では、SQL Server の増分バックアップおよびトランザクションログバックアップの基礎として使用できる SQL Server の完全バックアップが(コピーのみではなく)作成されます。このスナップショット形式では、[スナップショットが存在する場合はバックアップを停止する (Stop the backup if any snapshots exist)]がスナップショットを処理する場合に唯一有効なオプションであり、自動的に選択されます。
注意: T-SQL スナップショットは SQL Server 2022 で追加され、SQL Server 2022 以降のシステムで強く推奨されます。この形式のスナップショットは、SQL Server 2019 以前ではサポートされていません。
- 8 [保存 (Save)]をクリックしてポリシーを保存します。
トランザクションログを切り捨てない場合、これ以上の処理は必要ありません。
トランザクションログを切り捨てる場合は、手順 9 を続行します。
 - 9 ログの切り捨てを行わずに完全バックアップを実行します。
バックアップが完了したら、手順 3 で作成したポリシーを開きます。
 - 10 [VMware]タブをクリックし、[Microsoft SQL Server]の下で、[ログを切り捨てる (Truncate logs)]を選択します。
 - 11 [保存 (Save)]をクリックしてポリシーを保存します。
 - 12 VMware の完全バックアップを実行します。

SQL Server データを保護するための VMware バックアップを使用した保護計画の作成

VMware のバックアップポリシーを使用して、NetBackup では仮想マシンに存在する SQL Server データベースのアプリケーションの一貫した完全バックアップを作成できます。必要に応じて、NetBackup アクセラレータを使用できます。VMware ポリシーを使用して、VMware バックアップから特定の仮想ディスクを除外できます。特定の SQL Server コンポーネントを除外する場合は、MS-SQL-Server ポリシーを使用します。

保護計画を作成する前に、次のような追加の構成要件を実行する必要があります。

- すべてのストレージオプションを構成します。
- NetBackup サービスのログオンアカウントを構成します。

p.17 の「[SQL Server のバックアップとリストアのための NetBackup サービスの設定](#)」を参照してください。

p.18 の「[SQL Server のローカルセキュリティの権限の構成](#)」を参照してください。

- 環境内のホストの自動検出マッピングを確認します。
この処理には、デフォルトのセキュリティ管理者の役割、または類似の RBAC アクセス権を持つ役割が必要です。

SQL Server データを保護するために VMware バックアップを使用して保護計画を作成するには

- 1 バックアップ用にストレージを構成します。
- 2 左側で[保護 (Protection)]、[保護計画 (Protection plans)]の順にクリックし、[追加 (Add)]をクリックします。
- 3 [基本プロパティ (Basic properties)]で、[名前 (Name)]と[説明 (Description)]を入力します。
- 4 [作業負荷 (Workload)]リストで、[VMware]を選択します。
- 5 (オプション) ポリシー名に追加する[ポリシー名接頭辞 (Policy name prefix)]を指定します。NetBackup は、ユーザーがこの保護計画に資産をサブスクライブする際にポリシーを自動的に作成します。
- 6 [スケジュールおよび保持 (Schedules and retention)]で、[スケジュールの追加 (Add schedule)]をクリックします。
 - [属性 (Attributes)]タブで、バックアップの種類として[完全 (Full)]を選択します。
 - [開始時間帯 (Start window)]タブで、バックアップを開始できる時間帯を定義します。
 - [属性 (Attributes)]タブと[開始時間帯 (Start window)]タブでオプションをすべて選択したら、[保存 (Save)]をクリックします。
 - [バックアップスケジュールのプレビュー (Backup schedule preview)]ウィンドウを確認して、すべてのスケジュールが正しく設定されていることを確認します。

p.50 の「[スケジュール](#)」を参照してください。

- 7 [ストレージオプション (Storage options)]で、バックアップに使用するストレージを選択します。

保護計画では、NetBackup 8.1.2 以降のメディアサーバーがアクセスできるストレージのみを使用できます。

ストレージオプション 要件

説明

バックアップストレージ (Backup storage) このオプションには、OpenStorage が必要です。テープ、ストレージユニットグループ、および Replication Director はサポートされません。 [編集 (Edit)]をクリックします。ストレージターゲットを選択し、[選択したストレージの使用 (Use selected storage)]をクリックします。

- 8 [バックアップオプション (Backup options)]で、バックアップに利用可能なオプションを確認します。

p.126 の「バックアップオプション (Backup options) と詳細オプション (Advanced options)」を参照してください。

- 9 [仮想マシンバックアップからのアプリケーションデータのリストアを許可する (Allow restore of application data from virtual machine backups)]で、[Microsoft SQL Server]を選択します。

この時点では、[ログを切り捨てる (Truncate logs)]を有効にしないでください。この手順の後のほうの説明に従って、最初に、ログの切り捨てを行わずに完全バックアップを実行する必要があります。

- 10 (該当する場合) [T-SQL スナップショットを有効化する (Enable T-SQL snapshots)]を選択します。

このスナップショット形式では、SQL Server の増分バックアップおよびトランザクションログバックアップの基礎として使用できる SQL Server の完全バックアップが (コピーのみではなく) 作成されます。このスナップショット形式では、[スナップショットが存在する場合はバックアップを停止する (Stop the backup if any snapshots exist)]がスナップショットを処理する場合に唯一有効なオプションであり、自動的に選択されます。

注意: T-SQL スナップショットは SQL Server 2022 で追加され、SQL Server 2022 以降のシステムで強く推奨されます。この形式のスナップショットは、SQL Server 2019 以前ではサポートされていません。

- 11 [アクセス権 (Permissions)]で、保護計画へのアクセス権を持つ役割を確認します。

別の役割のアクセス権をこの保護計画に付与するには、[追加 (Add)]をクリックします。表で[役割 (Role)]を選択し、[権限の選択 (Select permissions)]セクションで権限を追加または削除して役割をカスタマイズします。

「Configure RBAC」を参照してください。

- 12 [確認 (Review)]で保護計画の詳細が正しいことを確認し、[保存 (Save)]をクリックします。
- 13 トランザクションログを切り捨てない場合、これ以上の処理は必要ありません。
トランザクションログを切り捨てる場合は、手順 14 を続行します。
- 14 ログの切り捨てを行わずに完全バックアップを実行します。
バックアップが完了したら、手順 2 で作成したポリシーを開きます。
- 15 [VMware]タブをクリックします。
- 16 [仮想マシンバックアップからのアプリケーションデータのリストアを許可する (Allow restore of application data from virtual machine backups)]を特定し、[Microsoft SQL Server]をクリックします。次に、[ログを切り捨てる (Truncate logs)]をクリックします。

SQL Server の場合、このオプションは仮想マシンの VMware スナップショットが完了したときにトランザクションログを切り捨てます。
- 17 [保存 (Save)]をクリックして、保護計画を保存します。
- 18 VMware の完全バックアップを実行します。

バックアップオプション (Backup options) と詳細オプション (Advanced options)

ユーザーは、保護計画にサブスクライブするときに次の設定を調整できます。

バックアップオプション

表 10-2 保護計画のバックアップオプション

オプション	説明
バックアップに使用するサーバーまたはホストを選択する	仮想マシンに代わってバックアップを実行するホスト。[Automatic (自動)]を選択すると、ストレージユニットに基づいて、NetBackup にメディアサーバーを選択させることができます。または、ユーザーがリストから別のホストを選択できます。これらのホストは、環境内のその他のメディアサーバーか、アクセスホストとして構成されているホストです。
スナップショットが存在する場合は次の処理を実行します。(If a snapshot exists, perform the following action)	NetBackup が仮想マシンバックアップの新しいスナップショットを作成する前に、スナップショットが見つかったときに NetBackup が適用する処理を指定します。たとえば、いずれかのスナップショットが存在する場合、バックアップの停止を選択できます。スナップショットが自動的に削除されなければ、最終的に仮想マシンのパフォーマンスが低下することがあります。削除されていないスナップショットが存在すると、ディスク容量不足によりリストアに失敗する場合があります。

オプション	説明
選択した仮想ディスクをバックアップから除外 (Exclude selected virtual disks from backups)	バックアップから除外する仮想ディスクを指定します。 p.127 の「バックアップからのディスクの除外」を参照してください。

詳細オプション

表 10-3 保護計画の詳細オプション

オプション	説明
仮想マシンの静止を有効にする (Enable virtual machine quiesce)	デフォルトで、仮想マシンの I/O は NetBackup がスナップショットを作成する前に静止します。ほとんどの場合、このデフォルトを使用する必要があります。ファイルのアクティビティを静止しないと、スナップショットのデータの一貫性は保証されません。静止を無効にすると、一貫性を保つためバックアップデータを分析する必要があります。
仮想マシンバックアップからのアプリケーションデータのリストアを許可する (Allow the restore of application data from virtual machine backups)	このオプションは、仮想マシンの完全バックアップからのアプリケーションデータのリストアをユーザーに許可します。このオプションが無効になっている場合、バックアップで仮想マシン全体をリカバリできますが、データベースは個別にリカバリできません。 p.123 の「SQL Server データを保護するための VMware バックアップを使用した保護計画の作成」を参照してください。 p.121 の「スナップショットレプリケーションの管理に Replication Director を使用して SQL Server を保護するための VMware ポリシーの構成」を参照してください。
トランスポートモード (Transport mode)	バックアップに使用するトランスポートモードまたはデータストアからデータを読み取る方法を指定します。トランスポートモードについて詳しくは、仮想化環境のベンダーのマニュアルを参照してください。
スナップショットの再試行オプション (Snapshot retry options)	p.128 の「スナップショットの再試行オプション (Snapshot retry options)」を参照してください。

バックアップからのディスクの除外

仮想ディスクの除外オプションはバックアップのサイズを減らすことができますが、使用には注意が必要です。これらは複数の仮想ディスクを備えている仮想マシン専用です。

表 10-4 仮想ディスクの除外オプション

除外オプション	説明
すべてのブートディスク (All boot disks)	ブートディスクを再作成する別の手段がある場合に、このオプションを検討します。 仮想マシンのブートディスクはバックアップには含まれません。その他のディスクはバックアップされます。注: データファイルはリストアされたデータディスクで利用可能です。ただし、このバックアップからリストアされる仮想マシンは起動できません。

除外オプション	説明
すべてのデータディスク (All data disks)	データディスクをバックアップする個別の保護計画がある場合にのみ、このオプションを検討してください。 仮想マシンのデータディスクはバックアップに含まれません。ブートディスクのみバックアップされます。注: 仮想マシンがバックアップからリストアされる時、データディスクの仮想マシンデータは失われるか不完全になる可能性があります。
カスタム属性に基づいてディスクを除外する (Exclude disks based on a custom attribute)	カスタム属性を使用した、バックアップから除外するディスクの制御を VMware 管理者に許可する場合、このオプションを使用します。 属性には、除外するディスクのデバイスコントローラの値をカンマで区切って指定する必要があります。たとえば、scsi0-0, ide0-0, sata0-0, nvme0-0 などです。この属性のデフォルト値は NB_DISK_EXCLUDE_DISK です。または、独自の値を選択できます。任意の差分バックアップ間でカスタム属性値にディスクを追加すると、それらのディスクは次のバックアップから除外されます。 VMware 管理者は、VMware インターフェースを使用して、除外するディスクに属性を適用する必要があります。『NetBackup Plug-in for VMware vSphere Web Client ガイド』または『NetBackup Plug-in for VMware vSphere Client (HTML5) ガイド』を参照してください。
除外する特定のディスク (Specific disks to be excluded)	ディスクの仮想デバイスノードを表すディスク形式、コントローラ、LUN を指定して特定のディスクを除外するには、このオプションを使用します。追加のディスクを指定するには、[追加 (Add)] をクリックします。 任意の差分バックアップ間でコントローラを追加すると、それらのディスクは次のバックアップから除外されます。

スナップショットの再試行オプション (Snapshot retry options)

ほとんどの環境では、スナップショットの再試行オプションのデフォルト値は適切です。仮想マシンのサイズと VMware サーバーの処理負荷に基づいてこれらの設定を調整すると役立つ場合があります。

表 10-5 スナップショットの再試行オプション (Snapshot retry options)

オプション	説明
スナップショットの最大試行回数 (Maximum number of times to retry a snapshot)	スナップショットを再試行する回数。
スナップショットの完了までの最長時間 (Maximum length of time to complete a snapshot)	スナップショット操作が完了するまでの分単位の時間。スナップショットが完了しない場合、タイムアウトを強制するためにこのオプションで特定の期間を設定します。後でスナップショットを再試行するには、[スナップショットを再試行するまでに待機する最長時間 (Maximum length of time to wait before a snapshot is retried)] 設定を使用します。

オプション	説明
スナップショットを再試行するまでに待機する最長時間 (Maximum length of time to wait before a snapshot is retried)	スナップショットが再試行されるまでの秒単位の待機時間。

VMware バックアップを使用した SQL Server データの保護

次の手順を使用して、SQL Server データを含む VM を保護計画にサブスクライブします。保護計画に資産をサブスクライブするときに、定義済みのバックアップ設定を資産に割り当てます。

メモ: 自分に割り当てられている RBAC の役割によって、管理する資産と、使用する保護計画にアクセスできるようにする必要があります。

VMware バックアップを使用して SQL Server データを保護するには

- 左側の[VMware]をクリックします。
- [仮想マシン (Virtual machine)]タブまたは[インテリジェント VM グループ (Intelligent VM groups)]タブで、VM または VM グループにチェックマークを付けて[保護の追加 (Add protection)]をクリックします。
- 保護計画を選択し、[次へ (Next)]をクリックします。
- 次の 1 つ以上の設定を調整できます。
 - スケジュールと保持 (Schedules and retention)
バックアップが行われるタイミングと、バックアップの開始時間帯を変更します。
p.50 の「[スケジュール](#)」を参照してください。
 - バックアップオプション (Backup options)
バックアップ、スナップショットオプション、除外オプションで使用するサーバーまたはホストを調整します。
p.126 の「[バックアップオプション \(Backup options\)](#)と[詳細オプション \(Advanced options\)](#)」を参照してください。
 - 詳細オプション (Advanced Options)
保護計画の詳細オプションを変更するか、有効にします。
p.126 の「[バックアップオプション \(Backup options\)](#)と[詳細オプション \(Advanced options\)](#)」を参照してください。

この計画では、VMware イメージからの SQL Server データベースのリストアを許可する必要があります。[仮想マシンバックアップからのアプリケーションデータのリストアを許可する (Allow restore of application data from virtual machine backups)]で、[Microsoft SQL Server]を有効にする必要があります。また、バックアップでログを切り捨てる場合は、[ログを切り捨てる (Truncate logs)]を選択します。

- 5 [保護 (Protect)]をクリックします。

[仮想マシン (Virtual machines)]または[インテリジェント VM グループ (Intelligent VM groups)]に、選択の結果が表示されます。

VMware バックアップからの SQL Server データベースのリストア

次の手順では、完全な VMware バックアップから SQL Server データベースをリストアする方法について説明します。

VMware バックアップから SQL Server データベースをリストアする方法

- 1 右側で[作業負荷 (Workloads)]、[Microsoft SQL Server]の順にクリックします。
- 2 [データベース (Databases)]タブをクリックします。
- 3 リストアするデータベースを選択し、[リカバリ (Recover)]をクリックします。
- 4 バックアップが実行された日付を選択します。
- 5 右側でリカバリポイントを特定します。次に、[処理 (Actions)]、[1 つのリカバリポイントのリカバリ (Recover single recovery point)]の順にクリックします。

注意: 複数のコピーが存在する場合でも、リストアに使用できるのはプライマリコピーのみです。別のコピーからリストアする場合は、最初にそのコピーをプライマリコピーに昇格する必要があります。

処理速度と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。

- **NetBackup for SQL Server** のパフォーマンスに影響を与える要素
- **SQL Server** のトラブルシューティング用のデバッグログについて
- クレデンシャルの検証に関するトラブルシューティング
- **VMware** のバックアップに関するトラブルシューティング
- **SQL Server** の **VMware** バックアップ中に発生する **SQL Server** のログの切り捨てエラー
- **NetBackup for SQL Server** の操作の監視について
- **NetBackup for SQL Server** の最大トレースレベルの設定
- 失敗したファイルグループまたはファイルバックアップのレポート
- 大規模な **SQL Server** データベースのリストアにおけるタイムアウトエラーの最小化について
- **SQL Server** の圧縮バックアップイメージを単一のストライプとして、または複数のストライプを含むイメージとしてリストアすると、**SQL Server** のリストアが失敗する
- 可用性グループクラスタに不正なバックアップイメージが表示される
- **SQL Server** のホスト名または **SQL Server** データベース名の末尾にスペースがあると **SQL Server** データベースのリストアは状態コード 5 またはエラー (-1) で失敗する
- **SQL Server** のホスト名、データベース名、データベース論理名の末尾にスペースがあると移動操作は状態コード 5 またはエラー (-1) で失敗する

- 可用性グループのレプリカを検出または参照できない
- SQL Server のディザスタリカバリについて

NetBackup for SQL Server のパフォーマンスに影響を与える要素

SQL Server や NetBackup のハードウェア環境と設定を含む多くの要因が、バックアップのパフォーマンスに影響を与える可能性があります。

メモ: 次に示す要因の一部は、SQL Server のストリームベースの処理にのみ該当し、スナップショットバックアップまたはリストアには影響しません。

SQL Server インテリジェントポリシーの場合は、これらのパラメータを[Microsoft SQL Server]タブでポリシーに設定します。バックアップパッチファイル (レガシー SQL Server ポリシー) またはリストアパッチファイルの場合は、NetBackup MS SQL Client インターフェースでこれらのパラメータを設定します。NetBackup クライアントプロパティのこれらのパラメータを保存してセッションで使います。

SQL Server のバッファ領域パラメータ

[最大転送サイズ (Maximum transfer size)]、[バックアップするブロックサイズ (Backup block size)]、[ストライプあたりのクライアントバッファ (Client buffers per stripe)]によって、SQL Server のバッファ領域が増加する可能性があります。SQL Server にはこれらの値の増加をサポートするために利用可能なリソースが必要です。バッファ領域パラメータは、ストリームベースのバックアップのためにのみ適用可能です。

[最大転送サイズ (Maximum transfer size)]パラメータは、各バックアップ操作またはリストア操作に対して設定できます。[最大転送サイズ (Maximum transfer size)]は、SQL Server でバックアップイメージの読み取りおよび書き込みに使用されるバッファサイズです。通常、この値を大きくすると、SQL Server のパフォーマンスが向上します。

[バックアップするブロックサイズ (Backup block size)]パラメータは、各バックアップ操作に対して設定できます。リストアに対しては、NetBackup によって、バックアップに使用したサイズと同じサイズが自動的に選択されます。[バックアップするブロックサイズ (Backup block size)]は、SQL Server でバックアップイメージの読み取りおよび書き込みに使用される増分サイズです。

[ストライプあたりのクライアントバッファ (Client buffers per stripe)]によって、バックアップ操作またはリストア操作時に各データストリームの読み込みまたは書き込みのために割り当てられるバッファ数が決定されます。この要素を 1 より大きい値に設定すると、データ転送時のマルチバッファが有効になります。より多くのバッファ数を割り当てることによって、NetBackup から NetBackup メディアサーバーへのデータ送信を高速化できます。マルチバッファは、バックアップまたはリストア操作中に Producer-Consumer で短期的な不

均衡が発生するのを防ぎます。バッファ数には 32 まで設定できますが、通常は値を 2 または 3 に設定すれば十分です。

ストライプと並列バックアップ操作

データベースのサイズと数によっては、バックアップストライプまたは並列バックアップ操作の値を増やすとパフォーマンスとスループットが向上します。

ストライプを設定するために SQL Server エージェントに追加のオーバーヘッドが必要になったとしても、パフォーマンスの向上のほうが重要な大規模データベースでは、複数のストライプ ([バックアップストライプ数 (Number of backup stripes)]) が役立ちます。より小さい規模のデータベースについては、ストライプの使用によってパフォーマンス速度が低下する可能性があります。一般に、SQL Server インスタンスに少数の大規模データベースしかない場合は、ストライプの使用によってパフォーマンスは改善します。インスタンスに多数の小規模データベースがある場合は、[並列バックアップ操作 (Parallel backup operations)] の量を増加することが、パフォーマンスを改善するにはよりよい選択です。ストライプおよび並列バックアップ操作の両方を同時に高めることができますが、システムリソースにかかる負荷が高くなりすぎないように注意します。

p.32 の「バックアップ操作を許可するジョブ数の設定」を参照してください。

注意: ポリシーが複数のストライプを使用するようにも構成されている場合、スケジュールの多重化を有効にしないでください。1 つのバックアップポリシーに対して多重化と複数のストライプの両方が構成されていると、リストアに失敗します。

共有メモリの使用

最適なパフォーマンスを得るには、NetBackup サーバーを NetBackup for SQL Server と同じホスト上にインストールしてください。データの転送にソケットではなく共有メモリを使った場合にも最適化されます。install_path¥NetBackup¥NOSHMF ファイルを作成しないかぎり、共有メモリはデフォルト構成です。

代替バッファ方式

NetBackup for SQL Server では、代替バッファ方式をサポートしています。この方式では、NetBackup と SQL Server 間でデータを転送することなく、同じメモリバッファを共有できるようにすることで、CPU の使用が最適化されます。

通常、バックアップおよびリストアの代替バッファ方式では、CPU 使用率のみが改善され、データ転送速度は向上しません。代替バッファ方式の使用で、転送速度が大幅に低下する場合があります。転送速度を上げるには、バックアップの [最大転送サイズ (Maximum transfer size)] を最大値である 4 MB に設定します。

バックアップ操作での代替バッファ方式について

次のすべての条件に当てはまる場合、この方式がバックアップに対して自動的に選択されます。

- NetBackup 共有メモリが使用されている。
- バックアップがストリームベースである。
- バックアップが多重化されていない。
- バックアップポリシーで、NetBackup 圧縮または NetBackup 暗号化のどちらも指定されていない。
- NetBackup のバッファサイズと SQL Server のブロックサイズが同じである。
 NetBackup のバッファサイズのデフォルトは 64 KB ですが、この値は次の設定で変更できます。
`install_path¥NetBackup¥db¥config¥SIZE_DATA_BUFFERS` (テープバックアップ用) または
`install_path¥NetBackup¥db¥config¥SIZE_DATA_BUFFERS_DISK` (ディスクバックアップ用)
- NetBackup for SQL Server エージェントを、NetBackup Client Service と同じアカウントを使用して起動している。
 自動バックアップポリシーから開始されたバックアップは、NetBackup Client Service で開始されるため、同じアカウントが使用されます。ただし、NetBackup for SQL Server または dbbackup を介して SQL Server バックアップを開始できます。この場合、ログオンアカウントが NetBackup Client Service アカウントと同じである必要があります。その後、バックアップは代替バッファ方式で行うことができます。

リストア操作での代替バッファ方式について

バックアップの条件として、代替バッファ方式を使用する必要があります。リストアの場合も、バックアップが代替バッファ方式で行われている必要があります。代替バッファ方式が使用されたことを検証できます。Using alternate buffer method という文字列を検索します。これは、dbclient ログおよび進捗レポートに表示されます。

SQL Server チェックサム

バックアップを実行する前に、チェックサムを実行することを選択できます。このオプションを有効にすると、バックアップ操作またはリストア操作でパフォーマンスが低下します。

レガシーバックアップポリシーの場合は、スクリプトを作成するときに[ページ検証 (Page verification)]値を設定します。リストアスクリプトの場合は、スクリプトの作成時に[リストアは実行せずに、バックアップイメージを検証 (Verify backup image, but do not restore)]オプションを選択します。

インスタントデータファイルの初期化

データベース、ファイルグループまたはデータベースファイルをリストアする場合、SQL Server によってファイル領域がゼロにリセットされてからリストア操作が開始されます。この処理によって、リカバリ時間の合計が 2 倍になる可能性があります。ファイルの初期化を回避するには、SE_MANAGE_VOLUME_NAME に割り当てられた Windows アカウ

ントで MSSQLSERVER サービスを実行します。詳しくは、SQL Server と Windows のマニュアルを参照してください。

SQL Server のトラブルシューティング用のデバッグログについて

NetBackup では、NetBackup の操作中に発生する可能性のある問題のトラブルシューティングのために、広範囲なデバッグログのセットを提供します。個々のログを作成することも、スクリプトを使用してすべての NetBackup デバッグログを作成することもできます。これらのデバッグログの内容について詳しくは、『[NetBackup トラブルシューティングガイド](#)』を参照してください。

バックアップ操作のデバッグログ

バックアップを実行した後、デバッグログの情報は `install_path\NetBackup\logs` ディレクトリに配置されます。プロセスごとにサブディレクトリが作成されます。デバッグログファイルは `ALL_ADMINS.mmddyy_0000x.log` と名付けられます。統合ログ (VxUL) の場合、ログファイルは Veritas 製品に共通の形式です。

クライアント

次のログを参照してください。

- bphdb (スケジュールバックアップのみ)
- dbclient
- ncfnbcs (VxUL)
- nbdisco (VxUL)
- user_ops\mssql\logs

プライマリサーバー

nbars (VxUL)

スナップショットバックアップ

次のログを参照してください。

- bpbkar (Snapshot Client)
- nbfsd (Snapshot Client)
- bppfi インスタントリカバリ

VMware バックアップ

ASC の問題とエラーのために、次のログはバックアップ済みである VM で作成されます。

- bpbkar
- dbclient
- ncfnbcs (VxUL)

リストア操作のデバッグログ

次のログは、リストア操作に適用されます。

クライアント

次のログを参照してください。

- bpbkar (Snapshot Client)
- bpfis (Snapshot Client)
- bppfi (インスタントリカバリ)
- dbclient
- user_ops¥mssql¥logs

Replication Director を使った Veritas VSS プロバイダのログを参照してください。

スナップショットからの VMware リストア (VMware restores from snapshots using Replication Director)

p.137 の「[Veritas VSS プロバイダのログ](#)」を参照してください。

すべてのデバッグログの作成

すべてのデバッグログを作成する方法

- ◆ 次のバッチファイルを実行します。

```
install_path¥NetBackup¥logs¥mklogdir.bat
```

NetBackup for SQL Server クライアントのデバッグレベルの設定

[クライアントのトレースレベル (Client Trace Level)] についての情報も利用可能です。p.143 の「[NetBackup for SQL Server の最大トレースレベルの設定](#)」を参照してください。

NetBackup for SQL Server クライアントのデバッグレベルを設定する方法

- 1 バックアップ、アーカイブ、および復元インターフェイスを開きます。
- 2 [ファイル (File)]、[NetBackup クライアントのプロパティ (NetBackup Client Properties)] の順に選択します。
- 3 [トラブルシューティング (Troubleshooting)] タブをクリックします。
- 4 [全般 (General)] デバッグレベルを設定します。
- 5 [詳細 (Verbose)] デバッグレベルを設定します。
- 6 [データベース (Database)] デバッグレベルを設定します。
- 7 [OK] をクリックして、変更を保存します。

Veritas VSS プロバイダのログ

Symantec VSS provider は Windows イベントログのアクティビティを記録します。Veritas 次の場所では、デバッグログも利用可能です。

```
install_path¥Veritas VSS provider¥logs
```

レジストリでの Veritas VSS プロバイダのログの有効化

SQL Server がインストールされている NetBackup コンピュータで Veritas VSS プロバイダのログを有効にします。

レジストリで Veritas VSS プロバイダのログを有効にするには

- 1 NetBackup がインストールされているコンピュータに管理者 (Administrator) としてログオンします。
- 2 レジストリエディタを開きます。
- 3 次のキーを開きます。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Veritas¥NetBackup¥CurrentVersion¥Config
```

- 4 CreateDebugLog という名前で新しい DWORD 値を作成します。
- 5 新しい値を右クリックして、[修正]をクリックします。
- 6 [値のデータ (Value data)]ボックスに、1 と入力します。
- 7 [OK]をクリックします。

Veritas VSS プロバイダのログのデバッグレベルを上げる

ログのデバッグレベルを上げるには、C:¥Windows フォルダの pre-freeze-script.bat ファイルと post-thaw-script.bat ファイルの両方を修正します。スクリプト内の BeVssRequestor.exe がコールされる行に -log パラメータを追加します。VMware によって呼び出されるスクリプトが決定されます。

Veritas VSS プロバイダのログのデバッグレベルを上げるには

1 pre-freeze-script.bat の次の行を変更します。

```
BeVssRequestor.exe -pre2 -logscreen !SkipExReplica! !SkipSQL!  
!VMBackupType! !ExcludeList!
```

この行を次のように変更します。

```
BeVssRequestor.exe -pre2 -logscreen !SkipExReplica! !SkipSQL!  
!VMBackupType! !ExcludeList! -log
```

2 また post-thaw-script.bat の次の行も変更します。

```
BeVssRequestor.exe -post2 -logscreen !SkipExReplica! !SkipSQL!  
!VMBackupType! !ExcludeList!
```

この行を次のように変更します。

```
BeVssRequestor.exe -post2 -logscreen !SkipExReplica! !SkipSQL!  
!VMBackupType! !ExcludeList! -log
```

クレデンシャルの検証に関するトラブルシューティング

表 11-1 で、インスタンス、レプリカ、またはインスタンスグループの検証に失敗する理由を説明しています。

表 11-1 クレデンシャルの検証に失敗した理由

状態コードまたはエラー	説明	説明
40	クレデンシャルを検証できませんでした。クライアントへの接続に失敗しました: <client>。	ホスト名が無効です。
46	検証操作がクライアントからの応答の待機中にタイムアウトしました	ホストが停止しているため、ホストに接続できません。

状態コードまたはエラー	説明	説明
41	クライアントでオペレーティングシステムのユーザーまたはパスワードの検証が失敗しました: <client>。	■ ホスト名は正しいが、ユーザー名とパスワードが無効です。 ■ クレデンシャルの使用について[これらの特定のクレデンシャルを使う (Use these specific credentials)]が設定されていますが、ユーザーアカウントに必要なローカルセキュリティ権限である [認証後にクライアントを偽装 (Impersonate a client after authentication)]と[プロセスレベルトークンの置き換え (Replace a process level token)]がありません。 p.18 の「SQL Server のローカルセキュリティの権限の構成」を参照してください。
1939	指定されたユーザーには、SQL Server System Administrator 権限が付与されていません。	クレデンシャルに「sysadmin」ロールがない場合、検証が失敗します。
無効な構成が検出されました。	無効な構成が検出されました。NetBackup Client Service および NetBackup Legacy Network サービスのユーザーは同じユーザーである必要があります。Windows Service Manager でサービスユーザーを変更し、再試行してください。	NetBackup Client Service または NetBackup Legacy Network Service がログオンアカウントで同一のユーザーを必要としているが、使用していません。 p.17 の「SQL Server のバックアップとリストアのための NetBackup サービスの設定」を参照してください。

VMware のバックアップに関するトラブルシューティング

アプリケーションを保護する VMware バックアップを実行するときには、次の点に注意してください。

- アプリケーション状態キャプチャ (ASC) ジョブは、ゲスト仮想マシン上の NetBackup クライアントと通信し、リカバリ用のアプリケーションデータをカタログ化します。
- ポリシーで選択されるアプリケーションに関係なく、VM ごとに 1 つの ASC ジョブが作成されます。
- アクティビティモニターで、ASC メッセージは ASC ジョブの詳細に基づいてフィルタリングされます。
- 失敗の結果、検出ジョブまたは親ジョブが状態コード 1 で終了します。
- 特定アプリケーションのリカバリを有効にしたが、そのアプリケーションが VM に存在しない場合、ASC ジョブは状態 0 を返します。
- bpfis が実行され、VSS スナップショットバックアップがシミュレートされます。このシミュレーションはアプリケーションの論理情報を取得するために必要になります。

表 11-2 VMware ポリシーを使用してデータベースを保護する場合の問題

問題	説明
データベースのバックアップが失敗する。	データベースは、構成が VMware バックアップのためにサポートされている場合にのみ、カタログ化され、保護されます。 p.117 の「 VMware アプリケーションバックアップの制限事項 」を参照してください。
	NetBackup が、除外された Windows ブートディスクにインストールされています。ASC ジョブは、この種類のディスクを検出し、それを独立したディスクと同様に処理します。NetBackup がブートドライブ (通常 C:) にインストールされている場合、[ブートディスクを除外 (Exclude boot disk)] オプションを選択しないでください。
ASC ジョブが状態 1 (部分的に成功) を生成する。	サポート対象のディスクとサポート対象外のディスクの両方に存在するバックアップ用のデータベースを選択しました。サポート対象外のディスクについては、「データベースのバックアップが失敗する」を参照してください。
	マウントされたフォルダには、フルテキストカタログファイルが存在します。データベースはカタログ化されません。
アプリケーション状態キャプチャ (ASC) ジョブが失敗し、データベースが保護されない。	ASC ジョブが失敗しても、VMware スナップショットまたはバックアップは続行されます。アプリケーション固有のデータはリストアできません。 SQL Server Management Studio (SSMS) に問い合わせを行うと、データベースがバックアップされたことが示される場合があります。この場合、データベースがスキップされても、スナップショットは成功しています。
	[仮想マシンの静止を有効にする (Enable virtual Machine quiesce)] オプションを無効にしました。
	データベースオブジェクトが VHD ディスク上にあります。バックアップ内のオブジェクトは、VHD に存在しないものも含めて、すべてカタログ化されません。
	[ディスクを除外 (Exclude disks)] タブで、VMware ポリシーから任意のディスクデータを除外しました。除外するディスクにデータベースのデータが含まれないようにしてください。
	VMware ディスクのレイアウトが前回の検出から変更されています。この場合、[VM 選択問い合わせ結果を再利用 (Reuse VM selection query results for)] オプションの値を小さく設定して、NetBackup に仮想マシンの再検出を強制する必要があります。『 NetBackup for VMware 管理者ガイド 』を参照してください。
	VMware の増分ポリシーを使用して SQL Server を保護することはできません。ただし、VMware のバックアップジョブは成功します。
	[T-SQL スナップショットを有効化する (Enable T-SQL snapshots)] が有効になっている場合は、ゲスト仮想マシン (SQL Server クライアント) で SQL Server VSS Writer サービスが無効になっていることを確認して、ASC ジョブのエラーを防ぎます。

問題	説明
ASC ジョブが状態コード 142 で失敗する。	T-SQL スナップショットバックアップをサポートするには、プライマリサーバー、メディアサーバー、クライアントの NetBackup バージョンがバージョン 10.4 である必要があります。旧バージョンではレガシーの VMware-ASC バックアップがサポートされます。旧バージョンの NetBackup で T-SQL スナップショットバックアップを試行すると、ASC ジョブが状態コード 142 で失敗する場合があります。
バックアップから仮想マシン全体をリカバリできても、データベースを個別にリカバリすることができない。	ポリシーの[VMware]タブで[アプリケーション保護 (Application protection)]オプションの[Microsoft SQL Server]を選択しませんでした。この設定によって、仮想マシンのバックアップからのデータベースのリカバリが可能になります。
トランザクションログのバックアップに失敗する。	ログを切り捨てるには、まずログの切り捨て ([ログを切り捨てる (Truncate logs)]オプション) なしで VMware の完全バックアップを実行する必要があります。
データベースが静止していない。	バックアップ時に Veritas VSS プロバイダも VMware VSS プロバイダもインストールされていません。この場合、リストアされた後、データベースのリカバリは、手動で行う手順が必要になる場合があります。
SQL Server エージェントの差分バックアップからリカバリできない。	VMware バックアップの[T-SQL バックアップを有効にする (Enable T-SQL backups)]オプションを有効にしてバックアップが失敗した場合、NetBackup はバックアップが失敗したことを SQL Server に通知できません。増分バックアップの基礎となる完全バックアップがないため、次の差分バックアップは無効になります。この問題は、次の完全バックアップが成功した後に解決されます。

SQL Server の VMware バックアップ中に発生する SQL Server のログの切り捨てエラー

データベース名に特殊文字が含まれたり、%TEMP% ディレクトリのパスが長すぎると、SQL Server の VMware バックアップ中に SQL Server のトランザクションログの切り捨てが失敗することがあります。SQL Server のログの切り捨て中に、SQL Server エージェントの NetBackup は一時ログバックアップを作成します。このバックアップは、ターゲットのバックアップデバイスの一部として現在のユーザーに設定されている %TEMP% ディレクトリおよびデータベース名を指定します。SQL Server では、バックアップデバイスに使用できるパスは 259 文字に制限されています。特定の状況下では、SQL Server エージェントが 259 文字よりも長いバックアップデバイスを生成し、ログの切り捨ての失敗を引き起こすことがあります。

次の状況がこのエラーを発生させます。

- 259 文字よりも長い %TEMP% ディレクトリが構成されている。
- データベース名と %TEMP% ディレクトリのパスを合わせた長さが 259 文字より長い。

この問題の回避策としては、パスが 259 文字より短くなるよう %TEMP% ディレクトリを構成するという方法があります。

NetBackup for SQL Server の操作の監視について

NetBackup 管理コンソールの[アクティビティモニター (Activity Monitor)]は、NetBackup for SQL Server の操作を監視するために使用します。

このエージェントでは、**NetBackup MS SQL** クライアントインターフェースで表示できる自身の進捗レポートも作成されます。レポートを表示するには、[ファイル (File)]>[状態の表示 (View status)]を選択します。レポートは

`install_path¥NetBackup¥logs¥user_ops¥MsSql¥logs` に保存されます。

ジョブの詳細および進捗レポートには次の種類の情報が含まれます。

- 操作に関する概略
- 操作の進捗状況に関する情報
- 操作の失敗の原因となるエラー状態または警告
- 操作の結果 (成功または失敗、および所要時間)

進捗レポートには次のような操作に関する追加詳細も含まれます。

- 操作のために **NetBackup** がバッチファイルに含めた **SQL Server** コマンド。

```
OPERATION BACKUP
DATABASE "TestDB1"
OBJECTTYPE DATABASE
COPYONLY FALSE
BLOCKSIZE 7
MAXTRANSFERSIZE 6
NUMBUFS 2
STRIPEs 1
SQLCOMPRESSION FALSE
VERIFYOPTION NONE
```

- バックアップを実行した **NetBackup** サーバー、バックアップのために選択した **SQL Server** インスタンスおよびホスト、その他のポリシー情報。

```
NBSERVER "servera"
SQLINSTANCE "SQL2K14"
SQLHOST "SERVERA"
POLICY "sql-server"
NBSCHED "full"
INF - Setting backup catalog name to: servera
```

- **SQL Server** で発生したバックアップまたはリストア操作の進捗と、エラーが発生した場合はエラー。

```

USER - Operation inhibited by NetBackup for Microsoft SQL
Server: Only a full or incremental database backup can be performed
on database <Archive> because it uses the simple recovery model
or
has 'truncate log on checkpoint' set.
INF - OPERATION #1 of batch
C:¥NBU¥Veritas¥NetBackup¥dbext¥mssql¥temp¥__01_35_42_508_00.bch
FAILED with STATUS 1 (0 is normal). Elapsed time = 6(6) seconds.
INF - Results of executing
<C:¥NBU¥Veritas¥NetBackup¥dbext¥mssql¥temp¥__01_35_42_508_00.bch>:
<0> operations succeeded. <1> operations failed.
INF - The following object(s) were not backed up successfully.
INF - Archive

```

NetBackup for SQL Server の最大トレースレベルの設定

メモ: SQL Server のバックアップの場合、この機能はレガシーの SQL Server バックアップポリシーを使用する場合にのみ利用可能です。

NetBackup MS SQL Client またはバッチファイルで最大トレースレベルを設定できます。最大レベルでは出力が大量になるため、通常、内部デバッグにのみ適しています。

NetBackup MS SQL Client で最大トレースレベルを設定する方法

- 1 NetBackup MS SQL Client を起動します。
- 2 [ファイル (File)]、[NetBackup クライアントのプロパティの設定 (Set NetBackup client properties)]の順に選択します。
- 3 [クライアントのトレースレベル (Client Trace Level)]グループで[高 (Maximum)]を選択します。

バックアップまたはリストアバッチファイルでトレースレベルを最大に設定する方法

- 1 NetBackup MS SQL Client を起動します。
- 2 [ファイル (File)]>[スクリプトファイルの管理 (Manage script files)]を選択します。
- 3 変更するバッチファイルを選択し、[ファイルを開く (Open File)]をクリックします。
- 4 次の行を追加します。
TRACELEVEL MAX
- 5 ファイルを保存します。

失敗したファイルグループまたはファイルバックアップのレポート

バックアップポリシー内の特定のデータベースと特定のファイルグループまたはファイルを選択すると、インスタンス全体 (DATABASE \$ALL) を選択する場合とは異なる方法で、**NetBackup** は失敗したファイルグループまたはファイルのバックアップを報告します。次のシナリオを検討します。

- シナリオ 1 - SQLINSTANCE1 (DATABASE \$ALL またはすべてのデータベース) の場合、ファイルグループ FG1、FG2、FG3 をバックアップする。**NetBackup** が FG1、FG2 または FG3 をバックアップできない場合、**NetBackup** はそのデータベースのファイルグループのバックアップをスキップします。親ジョブは状態 0 により完了します。
- シナリオ 2 - SQLINSTANCE1 の DATABASEA と DATABASEC の場合、ファイルグループ FG1、FG2、FG3 をバックアップする。**NetBackup** が DATABASEA または DATABASEC のいずれかのファイルグループのバックアップを作成できない場合、親ジョブは状態コード 2 で完了します。ジョブの詳細は、選択した 1 つ以上のファイルグループのバックアップが作成されなかったことを示しています。

大規模な SQL Server データベースのリストアにおけるタイムアウトエラーの最小化について

大規模な SQL Server のリストアでは、データが **NetBackup** メディアから読み込まれる前に [クライアントの読み込みタイムアウト (Client read timeout)] というエラーが発生する場合があります。このエラーは、リストア操作が開始される前に SQL Server でデータベースファイルの事前書き込みが必要な場合があるために発生します。この処理に必要な時間は、データベースファイルのサイズと、ホストマシンによるディスクへの書き込み速度によって決定されます。たとえば、システムで毎秒 60 MB の速度でディスクへの書き込みが可能であり、データベースのサイズが 2.4 TB である場合を考えます。実際にリストアが開始可能になるまでに、SQL Server によるディスクの準備に 12 時間以上かかります。実際の遅延は、計算値よりさらに 20 % から 40 % 長くなる場合があります。

タイムアウトの問題は、**NetBackup** の [クライアントの読み込みタイムアウト (Client read timeout)] 設定の値を大きくすることによって解決できます。クライアントホストプロパティで、リストアが必要になる可能性のあるデータベースを含む各クライアントのプロパティを変更します。デフォルトの [クライアントの読み込みタイムアウト (Client read timeout)] 設定は、300 秒 (5 分) です。大規模な SQL Server データベースが含まれるクライアントがある場合、この値を大きくする必要がある場合があります。

SQL Server リストア中にファイルの初期化を排除できます。次のトピックを参照してください。

p.132 の「[NetBackup for SQL Server のパフォーマンスに影響を与える要素](#)」を参照してください。

SQL Server の圧縮バックアップイメージを単一のストライプとして、または複数のストライプを含むイメージとしてリストアすると、SQL Server のリストアが失敗する

SQL Server の圧縮バックアップイメージを単一のストライプとして、または複数のストライプを含むイメージとしてリストアすると、SQL Server のリストアが失敗する

この問題は、SQL Server が圧縮データのバッファによりビジー状態で、特定の時間内に送信されたデータをすべて処理できない場合に発生します。Windows Server ではデフォルトで、TCP 接続は TCP 接続状態が 2 分間 FIN_WAIT_2 に設定された後に閉じる必要があります。詳しくは、次の Microsoft 記事を参照してください。

<https://support.microsoft.com/en-us/kb/923200/>

メモ: TCPFinWait2Delay 値が存在しない場合、REG_DWORD レジストリ値としてその値を作成する必要があります。そうしないと、Windows はデフォルト値 240 を使います。

TCP 接続が FIN_WAIT_2 状態を維持する時間を増やす方法

1 NetBackup メディアサーバーで regedit.exe を開きます。

2 次のレジストリサブキーを見つけて選択します。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

3 TCPFinWait2Delay をダブルクリックします。

4 300 の値を入力します。

5 メディアサーバーを再起動します。

6 リストアが正常に完了したら、レジストリ設定を削除するか、設定を元の値に戻します。

この設定の値を増やす場合は、すべての TCP/IP 接続に対して悪影響を及ぼします。値を増やすことにより、メディアサーバーで実行している他のアプリケーション用のポートが不足する場合があります。

7 メディアサーバーを再起動します。

可用性グループクラスタに不正なバックアップイメージが表示される

同一の短縮クラスタ名を持つが、異なるドメインに存在する複数の可用性グループクラスタのバックアップを実行できます。ただし、バックアップを参照する場合は、WSFC (Windows Server Failover Clustering) クラスタの完全修飾ドメイン名 (FQDN) を入力することが重要です。NetBackup MS SQL Client で、[ソースクライアント (Source Client)]

SQL Server のホスト名または SQL Server データベース名の末尾にスペースがあると SQL Server データベースのリストアは状態コード 5 またはエラー (-1) で失敗する

に WSFC クラスタの FQDN を入力します。短縮クラスタ名を使うと、NetBackup でバックアップイメージの正しいリストが表示されない場合があります。

SQL Server のホスト名または SQL Server データベース名の末尾にスペースがあると SQL Server データベースのリストアは状態コード 5 またはエラー (-1) で失敗する

SQL Server のホスト名または SQL Server データベース名の末尾に 1 つ以上のスペースがあると、NetBackup はリストアスクリプトを正しく生成しません。SQL Server のホスト名やデータベース名の末尾のスペースはスクリプトでは切り捨てられます。リストアを正常に実行するには、NetBackup MS SQL クライアントでリストアスクリプトの作成や編集を行う必要があります。

スクリプトで、DATABASE 行や NBIMAGE 行の SQL Server ホスト名または SQL Server データベース名を正しい名前に編集します。たとえば、デフォルトインスタンスを使っている場合にサーバーホスト名が「ACCT」でデータベース名が「DatabaseA」だとします。サーバーホスト名とデータベース名の末尾のスペースに注目してください。

次の行を変更します。

```
DATABASE "DatabaseA"  
NBIMAGE "ACCT.MSSQL7.ACCT.db.DatabaseA.~.7.001of001.20151118121736..C"
```

目的:

```
DATABASE "DatabaseA"  
NBIMAGE "ACCT.MSSQL7.ACCT.db.DatabaseA.~.7.001of001.20151118121736..C"
```

SQL Server のホスト名、データベース名、データベース論理名の末尾にスペースがあると移動操作は状態コード 5 またはエラー (-1) で失敗する

SQL Server のホスト名、データベース名、データベース論理名の末尾に 1 つ以上のスペースがあると移動操作は状態コード 5 またはエラー (-1) で失敗します。移動操作を正常に実行するには、NetBackup MS SQL Client で移動スクリプトの作成や編集を行う必要があります。

この問題の回避策は、Veritas のサポート Web サイトにある次の TechNote を参照してください。

<http://www.veritas.com/docs/000099850>

可用性グループのレプリカを検出または参照できない

読み取りスケール可用性グループのデータベースを検出して参照できるようにするには、**Microsoft SQL Server Native Client** バージョン 11.0.7462 以降の ODBC ドライバが可用性グループのレプリカにインストールされている必要があります。SQL Server インテリジェントポリシーからデータベースを参照する場合、**NetBackup** 管理コンソールで終了状態 114 を受信します。Web UI では、読み取りスケール可用性グループは検出されませんが、エラーメッセージは表示されません。

SQL Server のディザスタリカバリについて

SQL Server には、一時的な軽度の問題を自動的に修正する機能があります。ただし、この自動リカバリ機能は、ほとんどの障害に対応できません。たとえば、データベースの破損の程度が深刻である場合や、重大な障害が発生した場合は、システム管理者がリカバリを開始します。

ユーザー主導リカバリでは、システムの完全バックアップからサーバー全体 (SQL Server データベースを含む) をリストアできます。または、リカバリに SQL Server データベースのみの、新しくインストールした SQL Server または利用可能な他の SQL Server へのリストアを含めることができます。

サーバー全体をリストアすると、障害の発生時にそのサーバーに存在していた他のアプリケーションおよびデータもリカバリできるという利点があります。リストアは、次のいずれかの方法で行います。

- サーバーの手動リカバリ: システムの完全バックアップからサーバーを手動でリストアします。
p.147 の「[SQL Server のディザスタリカバリの準備](#)」を参照してください。
- **NetBackup Bare Metal Restore**。BMR では、オペレーティングシステム、システム構成およびすべてのシステムファイルとデータファイルがリストアされ、システムリカバリが自動的行われます。詳しくは『[NetBackup Bare Metal Restore 管理者ガイド](#)』を参照してください。

サーバーのリカバリが完了するか、または新しくインストールしたサーバーが利用可能になると、SQL Server データベースのリカバリを開始できます。

SQL Server のディザスタリカバリの準備

SQL Server のディザスタリカバリ計画を作成する場合は、master データベースの破損からリカバリする方法を検討する必要があります。ホストマシンの損失についても検討する必要があります。master データベースが破損すると、SQL Server は起動されません。障害の発生時には、システムデータベースを再構築する必要がある場合もあります。ただし、このプロセスでは、アプリケーションデータベースのスキーマ情報は再作成されま

せん。データベース図式をリカバリするには、**NetBackup MS SQL Client** を使用して **master** データベースの最新のバックアップをリストアします。

SQL Server のディザスタリカバリでは、その他のデータ損失からのリカバリ方針が決定されている必要があります。データ損失には、ディスクエラー、ソフトウェアのエラー、人為的なミスなどが含まれます。ディザスタリカバリの準備として、**master** データベースを頻繁にバックアップする必要があります。データベースを追加または削除した後や、スキーマ定義が生成される操作を実行した後は、頻繁にバックアップを行います。

ディザスタリカバリの後の SQL Server のデータベースのリカバリ

ディザスタリカバリする場合、新しくインストールした **SQL Server** にリストアすることをお勧めします。ただし、アクティブな他のデータベースが存在する既存の **SQL Server** をリストアできます。サーバーは、同じハードウェアプラットフォームの同じバージョンの **Windows** で実行されている必要があります。SQL Server のバージョンと SQL Server の **Service Pack** レベルも元のサーバーと同じである必要があります。

SQL Server データベースをリカバリする方法

- 1 既存の **SQL Server** にリストアする場合は、次のいずれかを選択します。
 - 新しい **SQL Server** インストールの場合、またはマスターデータベースが完全な状態であるときは、手順 4 に進みます。
 - マスターデータベースが破損している場合は、まずマスターデータベースを再構築する必要があります。2 に進みます。

- 2 マスターデータベースを再構築する方法の手順については、次の記事を参照してください。正しい **SQL Server** バージョンを選択するには[その他のバージョン (Other Versions)]ドロップダウンリストをクリックします。

<http://msdn.microsoft.com/en-us/library/ms144259.aspx>

コマンドプロンプトでデフォルトインスタンスのシステムデータベースを再構築する方法について説明した情報を検索します。

- 3 再構成が完了したら、**SQL Server** サービスを再起動します (必要な場合)。
- 4 マスターデータベースのリストアを開始するには、シングルユーザーモードで **SQL Server** を開始します。

シングルユーザーモードで **SQL Server** を開始する手順は、次の記事で説明されています。

<http://msdn.microsoft.com/en-AU/library/ms188236.aspx>

正しい **SQL Server** バージョンを選択するには[その他のバージョン (Other Versions)]ドロップダウンリストをクリックします。

- 5 **NetBackup MS SQL Client** インターフェースを開きます。
- 6 リストア操作に必要なすべてのメディアを検索します。

- 7 [ファイル (File)]、[SQL Server オブジェクトのリストア (Restore SQL Server objects)]の順に選択します。
- 8 リストアする **master** データベースのコピーを含むバックアップイメージを選択します。
この時点では **master** データベースのみを選択します。
- 9 [リストア (Restore)]をクリックします。
- 10 リストアの完了後、SQL Server サービスを再起動します。
- 11 残りの SQL Server データベースのリストアを続行します。

SQL データベース、差分、トランザクションログ、ファイルおよびファイルグループをリストアする手順に従います。

すべてのリストア操作が正常に完了したら、SQL Server データベースのリカバリは完了です。

リカバリの完了後は、Veritas はできるだけ早くデータベースの完全バックアップを実行することをお勧めします。