

# NetBackup™ Web UI Microsoft SQL Server 管理 者ガイド

リリース 9.0

**VERITAS™**

# NetBackup Web UI Microsoft SQL Server 管理者ガイド

最終更新日: 2021-02-01

## 法的通知と登録商標

Copyright © 2021 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](mailto:CustomerCare@veritas.com)

日本

[CustomerCare\\_Japan@veritas.com](mailto: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](mailto: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](https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf)

# 目次

第 1 章	NetBackup Web ユーザーインターフェースの概要	7
	NetBackup Web UI について	7
	用語	9
	NetBackup Web UI へのサインイン	11
	NetBackup Web UI からのサインアウト	12
第 2 章	NetBackup for SQL Server について	14
	NetBackup for SQL Server の概要	14
第 3 章	インストールとホストの構成	17
	NetBackup for SQL Server のインストールの計画	17
	SQL Server ホストとユーザー権限の構成	18
	vSphere 用の Veritas VSS プロバイダのインストール	19
	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	20
	SQL Server のローカルセキュリティの権限の構成	22
第 4 章	監視と通知	23
	NetBackup ダッシュボード	23
	ジョブの監視	24
	ジョブリストのジョブフィルタ	24
第 5 章	SQL Server の検出とクレデンシャルの管理	26
	SQL Server オブジェクトの検出について	26
	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	27
	オンデマンドでのデータベースの検出	28
	読み取りスケール可用性グループの検出	28
	SQL Server 資産の参照	28
	SQL Server クレデンシャルについて	31
	SQL Server インスタンスまたはレプリカへのクレデンシャルの追加	33
	SQL Server のクレデンシャルの管理	35

	SQL Server インスタンスの削除 .....	35
	SQL Server インスタンスの手動での追加 .....	36
<b>第 6 章</b>	<b>SQL Server の保護計画の管理 .....</b>	<b>37</b>
	SQL Server 可用性グループの保護について .....	37
	SQL Server 資産を保護するための保護計画の作成 .....	38
	スケジュールと保持 .....	41
	パフォーマンスチューニングおよび設定のオプション .....	41
	コピーまたはクローキングした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 .....	46
	スナップショット方式 .....	46
	NetBackup ドメインをまたぐ SQL Server 可用性グループの保護 .....	48
<b>第 7 章</b>	<b>SQL Server の保護 .....</b>	<b>51</b>
	保護計画への SQL Server 資産の追加 .....	51
	Microsoft SQL Server 資産の保護設定の編集 .....	54
	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 .....	55
	SQL Server 資産の保護の削除 .....	55
<b>第 8 章</b>	<b>SQL Server のリストア .....</b>	<b>57</b>
	SQL Server のリストアの要件 .....	57
	完全データベースリカバリの実行 .....	58
	1 つのリカバリポイントのリカバリ .....	61
	SQL Server のリストアオプション .....	64
	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 .....	65
	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 .....	67
<b>第 9 章</b>	<b>SQL Server でのインスタントアクセスの使用 .....</b>	<b>70</b>
	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 .....	70
	インスタントアクセスのハードウェア構成の必要条件 .....	72
	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 .....	72
	SQL Server インスタントアクセス用の Samba ユーザーの構成 .....	73
	インスタントアクセスデータベースの構成 .....	74
	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 .....	76
	インスタントアクセスデータベースの削除 .....	77
	NetBackup for SQL Server インスタントアクセスのオプション .....	78
	NetBackup for SQL Server の用語 .....	79
	よく寄せられる質問 .....	80

第 10 章	VMware バックアップを使用した SQL Server の保護 .....	84
	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 .....	84
	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 .....	85
	バックアップオプション (Backup options) と詳細オプション (Advanced options) .....	86
	バックアップからのディスクの除外 .....	88
	スナップショットの再試行オプション (Snapshot retry options) .....	89
	VMware バックアップを使用した SQL Server データの保護 .....	90
	VMware バックアップからの SQL Server データベースのリストア .....	91
第 11 章	トラブルシューティング .....	92
	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 .....	92
	SQL Server の VMware バックアップとリストアのトラブルシューティング .....	93
	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 .....	95

# NetBackup Web ユーザー インターフェースの概要

この章では以下の項目について説明しています。

- [NetBackup Web UI について](#)
- [用語](#)
- [NetBackup Web UI へのサインイン](#)
- [NetBackup Web UI からのサインアウト](#)

## NetBackup Web UI について

NetBackup Web ユーザーインターフェースは、次の機能を提供します。

- Chrome や Firefox などの Web ブラウザからマスターサーバーにアクセスする機能。Web UI でサポートされるブラウザについて詳しくは、[NetBackup ソフトウェア互換性リスト](#)を参照してください。  
NetBackup Web UI は、ブラウザによって動作が変わる場合があります。日付選択などの一部の機能は、一部のブラウザでは利用できないことがあります。こうした違いは、NetBackup の制限によるものではなく、ブラウザの機能によるものです。
- 重要な情報の概要を表示するダッシュボード。
- 役割ベースのアクセス制御 (RBAC) により、管理者は NetBackup へのユーザーアクセスを構成し、セキュリティ、ストレージ管理、または作業負荷の保護などのタスクを委任できます。
- NetBackup セキュリティ設定、証明書、API キー、ユーザーセッションの管理。
- 資産の保護は、保護計画、ジョブ管理、資産の保護状態の可視性を通じて実現します。また、ポリシー管理は、限られた数のポリシー形式でも利用できます。

- 作業負荷管理者は、保護計画を作成し、SLO を満たす保護計画に資産をサブスクライブし、保護状態を監視し、仮想マシンのセルフサービスリカバリを実行できます。Web UI は次の作業負荷をサポートします。
  - クラウド
  - Microsoft SQL Server
  - Oracle
  - Red Hat Virtualization (RHV)
  - VMware
- 使用状況レポートは、マスターサーバー上のバックアップデータのサイズを追跡します。また、Veritas NetInsights コンソールに簡単に接続して、NetBackup ライセンスを表示および管理できます。

---

メモ: NetBackup Web UI は、1280x1024 以上の画面解像度で最適に表示されます。

---

## NetBackup Web UI のアクセス制御

NetBackup では、役割ベースのアクセス制御を使用して Web UI へのアクセス権を付与します。アクセス制御は、役割を通じて実行されます。

- 役割は、ユーザーが実行できる操作と、作業負荷資産、保護計画、またはクレデンシャルに必要なアクセス権を定義します。単一のユーザーに複数の役割を設定でき、ユーザーアクセスを完全かつ柔軟にカスタマイズできます。
- RBAC は、Web UI と API でのみ利用可能です。NetBackup のその他のアクセス制御方法は、拡張監査 (EA) を除いて、Web UI と API ではサポートされません。

## NetBackup ジョブおよびイベントの監視

NetBackup Web UI を使用すると、管理者はより簡単に NetBackup 操作とイベントを監視し、注意が必要な問題を特定できます。

- ダッシュボードには、NetBackup ジョブ、証明書、トークン、セキュリティイベント、使用状況レポートの概要が表示されます。表示されるダッシュボードウィジェットは、ユーザーの RBAC の役割と権限によって異なります。
- ジョブが失敗したときに管理者が通知を受信するように電子メール通知を設定できます。NetBackup は、受信電子メールを受け取ることができる任意のチケットシステムをサポートします。



## 保護計画: スケジュール、ストレージ、およびストレージオプションを一元的に構成する場所

保護計画には、次の利点があります。

- バックアップのスケジュールに加えて、保護計画には、レプリケーションと長期保持のスケジュールも含めることができます。
- 利用可能なストレージから選択するときに、そのストレージで利用可能な追加機能を確認できます。
- デフォルトの作業負荷管理者は、バックアップ処理時間帯やバックアップ保持期間などの保護計画を作成して管理できます。  
役割の権限については、『NetBackup Web UI 管理者ガイド』を参照してください。
- デフォルトの作業負荷管理者は、資産またはインテリジェントグループを保護するために使用する保護計画を選択できます。

## セルフサービスリカバリ

NetBackup Web UI を使用すると、作業負荷管理者が VM またはデータベースを簡単にリカバリできるようになります。インスタントアクセス機能をサポートする作業負荷の場合、ユーザーはスナップショットをマウントして、VM のファイルやデータベースにすぐにアクセスできます。

# 用語

次の表では、新しい Web ユーザーインターフェースで導入された概念と用語について説明します。

表 1-1 Web ユーザーインターフェースの用語および概念

用語	定義
管理者	NetBackup と、NetBackup Web UI を含むすべてのインターフェースに対する完全なアクセス権を持つユーザーです。ルート、管理者、拡張監査のすべてのユーザーは、NetBackup の完全なアクセス権を持ちます。NetBackup Web UI の各ガイドでは、 <b>NetBackup 管理者</b> という用語は、NetBackup への完全なアクセス権を持つユーザーも指しますが、通常は NetBackup 管理コンソールのユーザーを指します。  「役割」も参照してください。
資産グループ	「インテリジェントグループ」を参照してください。
資産	物理クライアント、仮想マシン、データベースアプリケーションなどの保護対象データです。

用語	定義
今すぐバックアップ	資産のバックアップをすぐに作成します。 <b>NetBackup</b> は、選択した保護計画を使用して資産の完全バックアップを 1 回のみ実行します。このバックアップは、スケジュールバックアップには影響しません。
従来のポリシー	<b>NetBackup Web UI</b> では、レガシーポリシーが資産を保護することを示します。レガシーポリシーは、 <b>NetBackup</b> 管理コンソールで作成します。
外部証明書	<b>NetBackup</b> 以外のあらゆる CA から発行されたセキュリティ証明書です。
インテリジェントグループ	指定した条件 (クエリー) に基づいて、 <b>NetBackup</b> が保護対象資産を自動的に選択することを可能にします。インテリジェントグループは、本番環境の変更が含まれるように、自動的に最新の状態に維持されます。これらのグループは、資産グループとも呼ばれます。  VMware と RHV の場合、[インテリジェント VM グループ (Intelligent VM groups)] タブにこれらのグループが表示されます。
インスタントアクセス	<b>NetBackup</b> バックアップイメージから作成したインスタントアクセス VM やデータベースはほとんど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。 <b>NetBackup</b> は、バックアップストレージデバイスにスナップショットを直接マウントし、そのスナップショットを通常の VM またはデータベースとして扱います。
NetBackup 証明書	<b>NetBackup CA</b> から発行されたセキュリティ証明書です。
保護計画	保護計画は、バックアップを実行するタイミング、バックアップの保持期間、使用するストレージ形式を定義します。保護計画を設定したら、資産を保護計画にサブスクライブできます。
RBAC	役割ベースのアクセス制御です。管理者は、RBAC で設定されている役割を通じて、 <b>NetBackup Web UI</b> へのアクセスを委任または制限できます。  注意: RBAC で設定した役割は、 <b>NetBackup</b> 管理コンソールまたは CLI へのアクセスを制御しません。
役割	RBAC の場合、ユーザーが実行できる操作と、ユーザーがアクセスできる資産やオブジェクトを定義します。たとえば、特定のデータベースのリカバリを管理する役割と、バックアップおよびリストアに必要なクレンジンシャルを設定できます。
ストレージ	データのバックアップ、レプリケート、または複製 (長期保持用) 対象となるストレージです。

用語	定義
保護計画にサブスクライブする	保護計画にサブスクライブする資産または資産グループを選択する処理です。資産は、保護計画のスケジュールに従って保護されます。Web UI では、サブスクライブを「保護の追加」とも表記します。
保護計画からサブスクライブ解除する	サブスクライブ解除は、保護を解除する処理、または計画から資産や資産グループを削除する処理を指します。
作業負荷 (Workload)	資産のタイプです。たとえば、VMware、RHV、またはクラウドです。

## NetBackup Web UI へのサインイン

権限を持つユーザーは、NetBackup Web UI を使用して、NetBackup マスターサーバーに Web ブラウザからサインインできます。利用可能なサインインオプションは次のとおりです。

- 「ユーザー名とパスワードでサインインする」
- 「証明書またはスマートカードでサインインする」
- 「シングルサインオン (SSO) でサインインする」

### ユーザー名とパスワードでサインインする

認可済みのユーザーのみが NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

ユーザー名とパスワードを使用して NetBackup マスターサーバーにサインインするには

- 1 Web ブラウザを開き、次の URL に移動します。

`https://masterserver/webui/login`

`masterserver` は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。

- 2 クレデンシャルを入力して、[サインイン (Sign in)] をクリックします。

次に例を示します。

ユーザーの種類	使用する形式	例
ローカルユーザー	<code>username</code>	<code>jane_doe</code>
Windows ユーザー	<code>DOMAIN#username</code>	<code>WINDOWS#jane_doe</code>
UNIX ユーザー	<code>username@domain</code>	<code>john_doe@unix</code>

## 証明書またはスマートカードでサインインする

権限を持つユーザーである場合は、スマートカードまたはデジタル証明書を使用して NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

スマートカードにないデジタル証明書を使用するには、まずブラウザの証明書マネージャに証明書をアップロードする必要があります。詳しくはブラウザのマニュアルで手順を参照するか、証明書管理者にお問い合わせください。

証明書またはスマートカードでサインインするには

- 1 Web ブラウザを開き、次の URL に移動します。  
`https://masterserver/webui/login`  
*masterserver* は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。
- 2 [証明書またはスマートカードでサインイン (Sign in with certificate or smart card)] をクリックします。
- 3 ブラウザにプロンプトが表示されたら、証明書を選択します。

## シングルサインオン (SSO) でサインインする

NetBackup 環境内で SAML が ID プロバイダとして設定されている場合、シングルサインオン (SSO) オプションを使用して NetBackup Web UI にサインインできます。詳しくは、NetBackup セキュリティ管理者にお問い合わせください。

SSO を使用して NetBackup マスターサーバーにサインインするには

- 1 Web ブラウザを開き、次の URL に移動します。  
`https://masterserver/webui/login`  
*masterserver* は、サインインする NetBackup マスターサーバーのホスト名または IP アドレスです。
- 2 [シングルサインオンでサインイン (Sign in with single sign-on)] をクリックします。
- 3 管理者が指示する手順に従ってください。  
以降のログオンでは、NetBackup によって自動的にマスターサーバーへのサインインが行われます。

# NetBackup Web UI からのサインアウト

NetBackup は、24 時間 (ユーザーセッションで許可される最大時間) 後に Web UI からの自動サインアウトを強制的に実行します。その時間が経過すると、NetBackup は再びサインインを要求します。また、使用するサインインオプション (ユーザー名とパスワード、

スマートカード、またはシングルサインオン (SSO) を変更する場合にもサインアウトできます。

**NetBackup Web UI からサインアウトするには**

- ◆ 右上で、プロフィールアイコン、[サインアウト (Sign out)]の順にクリックします。

# 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。インスタンスは NetBackup 環境内で自動的に検出され、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。

NetBackup Web UI では、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
- SQL Server 資産を保護するための保護計画の選択
- データベースの復元
- 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。

**表 2-1** 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	<p>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。</p>
保護計画	<p>次の利点があります。</p> <ul style="list-style-type: none"> <li>■ 複数の SQL Server インスタンスまたはインスタンスデータベースを保護する単一の保護計画、または可用性グループまたは可用性データベースを保護する単一の計画を使用できます。インスタンスは複数のクライアントに分散できます。</li> <li>■ 同じポリシーに完全、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。</li> <li>■ 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。</li> <li>■ SQL Server コマンドに関する知識や、バ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バッチファイルを生成します。</li> </ul>
SQL Server 資産の管理	<p>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、SQL Server 資産を保護するために 1 つ以上の保護計画を選択できます。</p>
認証およびクレデンシャル	<p>SQL Server 保護計画では次がサポートされます。</p> <ul style="list-style-type: none"> <li>■ Windows 認証および Windows Active Directory 認証。</li> <li>■ 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。</li> </ul>

機能	説明
バックアップおよびリストア機能	<p>バックアップとリストアでは次の機能を利用できます。</p> <ul style="list-style-type: none"> <li>■ バックアップは、<b>NetBackup</b> 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。</li> <li>■ <b>NetBackup Web UI</b> 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: <b>Web UI</b> を使用した <b>SQL Server</b> リカバリでは、<b>SQL Server</b> クライアントがバージョン <b>8.3</b> 以降である必要があります。</li> <li>■ 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。</li> <li>■ 手動バックアップとコピーのみバックアップ。</li> <li>■ <b>SQL Server</b> クラスタと可用性グループを含む、高可用性 (<b>HA</b>) 環境のサポート。</li> <li>■ <b>SQL Server</b> 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)。</li> <li>■ バックアップ中に複数のストライプを使うための機能です。</li> <li>■ 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。</li> </ul>
ストリームベースのバックアップおよびリストア	<p><b>SQL Server</b> 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 <b>SQL Server</b> オブジェクトのバックアップとリストア</p>
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	<p><b>NetBackup</b> では、スナップショット方式を使用して <b>SQL Server</b> のバックアップを実行できます。</p> <p>また、<b>NetBackup</b> 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。<b>NetBackup</b> 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。</p>
SQL Server を保護する VMware バックアップのサポート	<p>スナップショットを使用した、<b>VMware</b> コンピュータのアプリケーションで一貫した完全バックアップのサポート。また、<b>NetBackup</b> 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。</p> <p>詳しくは、次の文書を参照してください。</p> <p><a href="#">『NetBackup for VMware 管理者ガイド』</a></p> <p><a href="#">『NetBackup 管理者ガイド Vol. 1』</a></p>



# 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](#)

## NetBackup for SQL Server のインストールの計画

[表 3-1](#) 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 3-1** 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。	<a href="#">NetBackup 互換性リスト</a> を参照してください。
手順 2	マスターサーバーに NetBackup for SQL Server の有効なライセンスと、使用する NetBackup のオプションまたはアドオンがあることを確認します。	

手順	処理	説明
手順 3	<p>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、<b>NetBackup クライアントソフトウェア</b>をインストールします。<b>NetBackup for SQL Server</b> エージェントは <b>NetBackup クライアントソフトウェア</b>とともにインストールされます。</p> <p><b>NetBackup 9.0 の NetBackup for SQL Server</b> に含まれる新しい機能を使用するには、<b>NetBackup for SQL Server クライアント</b>を <b>NetBackup 9.0</b> にアップグレードします。<b>NetBackup メディアサーバー</b>は <b>NetBackup for SQL Server クライアント</b>以上のバージョンを使用する必要があります。</p>	<p>次の点に注意してください。</p> <ul style="list-style-type: none"> <li>■ <b>SQL Server 可用性グループ</b>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。</li> <li>■ <b>SQL Server クラスタ環境</b>では、クラスタ内のそれぞれのノードに <b>NetBackup クライアント</b>をインストールします。各ノードに同じ <b>NetBackup</b> のバージョンがある必要があります。</li> <li>■ <b>VMware 環境</b>では、<b>SQL Server</b>を実行している仮想マシンに <b>NetBackup クライアントソフトウェア</b>をインストールします。</li> <li>■ 複数の <b>NIC</b>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 <b>NetBackup クライアント</b>をインストールします。</li> <li>■ <b>SQL Server クライアント</b>がマスター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 <b>NetBackup クライアント</b>をインストールする必要があります。</li> </ul>
手順 4	<p>読み取りスケール可用性グループを保護するには、<b>SQL Server Native Client</b>バージョン <b>11.0.7462</b>以降の <b>ODBC ドライバ</b>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。</p>	<p>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。</p>
手順 5	<p><b>NetBackup クラスタ</b>で <b>NetBackup for SQL Server</b>を使用するには、クラスタ環境がサポートされており、<b>NetBackup クラスタ</b>が正しく構成されていることを確認します。</p>	<p>次の必要条件を確認してください。</p> <ul style="list-style-type: none"> <li>■ <b>NetBackup サーバーソフトウェア</b>が <b>NetBackup クラスタ</b>内にインストールされ、動作するように構成されている。</li> <li>■ <b>NetBackup</b>のクライアントソフトウェアが、<b>NetBackup</b>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。</li> <li>■ <b>NetBackup サーバー</b>がある各ノードに <b>NetBackup for SQL Server</b>の有効なライセンスがある。</li> </ul> <p><a href="#">ソフトウェアの互換性リスト (SCL)</a>を参照してください。  <a href="#">『NetBackup インストールガイド』</a>を参照してください。  <a href="#">『NetBackup マスターサーバーのクラスタ化管理者ガイド』</a>を参照してください。</p>

## 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 3-2** 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。	p.19 の「 <a href="#">vSphere 用の Veritas VSS プロバイダのインストール</a> 」を参照してください。
手順 2	NetBackup がバックアップやリストアを実行する際に SQL Server にアクセスするように NetBackup Client Service および NetBackup Legacy Network Service を構成します。	p.20 の「 <a href="#">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</a> 」を参照してください。
手順 3	SQL Server クレデンシャル用に[これらの特定のクレデンシャルを使用 (Use these specific credentials)]オプションを使用する場合、ローカルシステム以外のアカウントには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。  p.22 の「 <a href="#">SQL Server のローカルセキュリティの権限の構成</a> 」を参照してください。
手順 4	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。マスターサーバーの[セキュリティ (Security)]、[ホスト (Hosts)]でこの構成を実行します。  <a href="#">ホストマッピングの構成</a> について詳しくは、『 <a href="#">NetBackup Web UI 管理者ガイド</a> 』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。

## 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 [コントロールパネル]で、[プログラムの追加と削除]または[プログラムと機能]を開きます。
- 2 [vSphere 用の Veritas VSS プロバイダ (Symantec VSS Provider for vSphere)]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 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。

**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ャルに [クライアントのローカルで定義されているクレデンシャルを使用 (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ャルに [これらの特定のクレデンシャルを使う (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す。
  - (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ャルに [クライアントのローカルで定義されているクレデンシャルを使用 (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ャルに [これらの特定のクレデンシャルを使う (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す。
  - (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アル用に[これらの特定のクレデンシアルを使用 (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.22 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アル用に[これらの特定のクレデンシアルを使用 (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。
  - 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。

# 監視と通知

この章では以下の項目について説明しています。

- [NetBackup ダッシュボード](#)
- [ジョブの監視](#)
- [ジョブリストのジョブフィルタ](#)

## NetBackup ダッシュボード

NetBackup ダッシュボードは、組織内のロールに関連する詳細情報のクイックビューを提供します。

表 4-1 NetBackup ダッシュボード

ダッシュボードウィジェット	説明
ジョブ	アクティブジョブやキューに投入済みのジョブの数、試行されたジョブや完了したジョブの状態などのジョブ情報を一覧表示します。
証明書	環境内の NetBackup のホスト ID ベースのセキュリティ証明書または外部証明書に関する情報を表示します。 外部証明書では、NetBackup 8.2 以降のホストに関する次の情報が表示されます。 <ul style="list-style-type: none"><li>■ ホストの合計。ホストの合計数です。ホストはオンラインになっており、NetBackup マスターサーバーと通信できる必要があります。</li><li>■ 不明。外部証明書が登録されていないホストの数です。</li><li>■ 有効。外部証明書が登録されているホストの数です。</li><li>■ 期限切れ。期限切れの外部証明書を持つホストの数です。</li></ul>
トークン	環境内の認証トークンに関する情報を表示します。

ダッシュボードウィジェット	説明
セキュリティイベント	[アクセス履歴 (Access history)]ビューには、ログオンイベントのレコードが含まれます。[監査イベント (Audit events)]ビューには、ユーザーが NetBackup マスターサーバーで開始したイベントが含まれます。
使用状況レポート	組織内の NetBackup マスターサーバーのバックアップデータのサイズを一覧表示します。このレポートは、容量ライセンスを追跡するために役立ちます。右上のドロップダウンリストを使用して、表示する期間とビューを選択します。サーバー名をクリックして、そのサーバーの特定の詳細を表示します。

## ジョブの監視

[ジョブ (Jobs)]ノードを使用して、NetBackup 環境のジョブを監視し、特定のジョブの詳細を表示します。

ジョブを監視するには

- 1 左側で、[アクティビティモニター (Activity monitor)]>[ジョブ (Jobs)]をクリックします。
- 2 表示するジョブの名前をクリックします。

[概要 (Overview)]タブで、ジョブに関する情報を表示します。

- [ファイルリスト (File List)]には、バックアップイメージに含まれているファイルが表示されます。
- [状態 (Status)]セクションには、ジョブに関連する状態と状態コードが表示されます。状態コード番号をクリックすると、この状態コードについてのベリタスナレッジベースの情報が表示されます。

『[NetBackup 状態コードリファレンスガイド](#)』を参照してください。

- 3 [詳細 (Details)]タブをクリックして、ジョブについて記録された詳細を表示します。ドロップダウンメニューを使用して、エラーの種類によってログをフィルタできます。

p.24 の「[ジョブリストのジョブフィルタ](#)」を参照してください。

## ジョブリストのジョブフィルタ

特定の状態のジョブを表示するために、ジョブをフィルタできます。たとえば、実行中のジョブまたは一時停止中のジョブをすべて表示できます。

ジョブリストをフィルタするには

- 1 [ジョブ (Jobs)]をクリックします。
- 2 ジョブリストの上にある[フィルタ (Filter)]オプションをクリックします。



- 3 [フィルタ (Filter)]ウィンドウでフィルタオプションを選択すると、表示されるジョブが動的に変わります。フィルタオプションは次のとおりです。
  - すべて (All)
  - 有効 (Active)
  - 完了 (Done)
  - 失敗 (Failed)
  - 未完了 (Incomplete)
  - 部分的に成功 (Partially Successful)
  - キューへ投入済み (Queued)
  - 成功 (Successful)
  - 一時停止 (Suspended)
  - 再試行を待機中 (Waiting for Retry)
- 4 [フィルタの適用 (Apply Filters)]をクリックします。
- 5 選択したフィルタを解除するには、[すべて消去 (Clear All)]をクリックします。

# SQL Server の検出とクレデンシヤルの管理

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 資産の参照](#)
- [SQL Server クレデンシヤルについて](#)
- [SQL Server インスタンスまたはレプリカへのクレデンシヤルの追加](#)
- [SQL Server のクレデンシヤルの管理](#)
- [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、そのマスター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 分ごとにマスターサーバーをポーリングして、期限の切れたデータがないかを確認します。

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、マスター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 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

## SQL Server クレデンシャルについて

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 5-1 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
<p>これらの特定のクレデンシャルを使用 (Use these specific credentials) (推奨)</p>	<ul style="list-style-type: none"> <li>■ 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。</li> <li>■ SQL Server 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。</li> </ul> <p>構成要件</p> <p>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。</p> <p>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。</p> <p>p.20 の「<a href="#">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</a>」を参照してください。</p> <p>p.22 の「<a href="#">SQL Server のローカルセキュリティの権限の構成</a>」を参照してください。</p>

クレデンシャルを登録するオプション	環境または構成
<p>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)</p>	<ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> </ul> <p>構成要件</p> <p>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。</p> <p>NetBackup サービスのログオンアカウントも構成する必要があります。</p> <p>p.20 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>

## 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。

# SQL Server インスタンスまたはレプリカへのクレデンシャルの追加

SQL Server 資産の完全な検出を許可するには、インスタンスまたはレプリカのサーバーの新しいクレデンシャルを追加するか、既存のクレデンシャルを選択する必要があります。使用する SQL Server クレデンシャルオプションの要件を確認します。

p.31 の「[SQL Server クレデンシャルについて](#)」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

既存の SQL Server クレデンシャルのリストから、インスタンスまたはレプリカに適用するクレデンシャルを選択できます。

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)]を選択し、[次へ (Next)]をクリックします。

- 5 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。  
NetBackup がクレデンシャルを検証します。
- 6 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。

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

インスタンスまたはレプリカに適用するクレデンシャルが利用できない場合は、それらを NetBackup に追加できます。

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 クレデンシャル名を入力します。
- 6 次のオプションのいずれかを選択します。
  - [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)]、[次へ (Next)]の順にクリックします。
  - これらの特定のクレデンシャルを使用 (Use these specific credentials)  
クレデンシャルに関連付けられている[ユーザー名 (User name)]、[パスワード (password)]、および[ドメイン (Domain)]を入力します。[次へ (Next)]をクリックします。

p.31 の「[SQL Server クレデンシャルについて](#)」を参照してください。

- 7 [アクセス権 (Permissions)]の画面には、クレデンシャルへのアクセス権を持つ役割が表示されます。
- 8 [次へ (Next)]をクリックします。

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。

## SQL Server のクレデンシャルの管理

適切な RBAC 権限を持つユーザーは、SQL Server インスタンスのクレデンシャルを表示および管理できます。

**SQL Server のクレデンシャルを編集するには**

- 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 編集するインスタンスまたはレプリカを選択して、[クレデンシャルの管理 (Manage credentials)]をクリックします。

## 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)]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 左側の[SQL Server]をクリックし、[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、追加のロール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.33 の「SQL Server インスタンスまたはレプリカへのクレデンシャルの追加」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](#)
- [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。
- 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.48 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。

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

可用性グループのバックアップには次の制限事項があります。

- **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バックアップ
  - VMware バックアップ
  - グループ化されたスナップショットバックアップ
  - 読み取り可能でないセカンダリレプリカのバックアップ  
レプリカへのユーザー接続を許可した場合は、**NetBackup** はそのレプリカのデータベースのみをバックアップできます。  
セカンダリレプリカが優先レプリカである場合にそれが読み取り不可である場合は、バックアップが失敗します。セカンダリレプリカが優先レプリカでない場合は、**NetBackup** はそのレプリカのバックアップを省略します。

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。
- 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 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。

**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。ユーザーがこの保護計画に資産をサブスクライブする際に、**NetBackup** はポリシーを自動的に作成します。このとき、ポリシー名に接頭辞が付加されます。

- 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設定できます。[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)]ウィンドウで、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.46 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あります。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る要因について詳しくは、『**NetBackup for Microsoft SQL Server 管理者ガイド**』も参照してください。

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。

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。

p.41 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 [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[ロール (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。

## スケジュールと保持

必要な RBAC 権限がある場合、資産を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。

表 6-1

オプション	説明
反復 (Recurrence) (間隔)	注意: この設定は、SQL Server のトランザクションログのスケジュールに対してのみ編集できます。 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)	注意: この設定は、SQL Server のトランザクションログのスケジュールに対してのみ編集できます。 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。
開始時間帯 (Start window)	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

必要な RBAC 権限がある場合、資産を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。

**表 6-2 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
ストライプあたりのクライアントバッファ (Client buffers per stripe)	<p>(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。<b>NetBackup</b> 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、<b>NetBackup</b> から <b>NetBackup</b> マスターサーバーへのデータ送信を高速化できます。</p> <p>このオプションのデフォルト値は 2 で、<b>Double Buffering</b> 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。</p>
最大転送サイズ (Maximum transfer size)	<p>(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、<b>SQL Server</b> 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、<b>SQL Server</b> 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。<math>64 \text{ KB} * 2^{\text{MAX\_TRANSFER\_SIZE}}</math> 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。</p>
並列バックアップ操作 (Parallel backup operations)	<p>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。</p>
VDI タイムアウト (秒) (VDI Timeout (seconds))	<p><b>SQL Server</b> 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。</p> <p>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。</p>
Microsoft SQL Server の圧縮を使用 (Use Microsoft SQL Server compression)	<p><b>SQL Server</b> 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。<b>SQL Server</b> の圧縮を有効にした場合、<b>NetBackup</b> の圧縮を有効にしないでください。</p> <p><b>SQL Server</b> 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。</p>
[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)]	<p><b>NetBackup</b> では、<b>NetBackup</b> 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。</p> <p><b>NetBackup</b> 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リプト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。</p>
コピーのみバックアップの作成	<p>このオプションでは、<b>SQL Server</b> によって帯域外 (アウトオブバンド) のバックアップが作成されるため、通常のバックアップシーケンスは妨げられません。</p> <p>p.46 の「コピーまたはクロッキングした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」を参照してください。</p>

フィールド	説明
<p>Microsoft SQL Server チェックサムの実行 (Perform Microsoft SQL Server checksum)</p>	<p>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。</p> <ul style="list-style-type: none"> <li>■ なし。バックアップチェックサムを無効にします。</li> <li>■ 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。 <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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。</li> </ul> </li> </ul>
<p>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)</p>	<p>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は、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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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。</li> </ul> <p>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。</p>

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)	<p>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、<b>NetBackup</b> 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。</p> <p>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、<b>SQL Server</b> 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。<b>NetBackup</b> 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。</p> <p>注意: <b>NetBackup</b> 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 <b>NetBackup</b> カタログに存在しないにもかかわらず、<b>SQL Server</b> が既存の完全 LSN を検出する場合、<b>NetBackup</b> 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、<b>NetBackup MS SQL Client</b> 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 <b>NetBackup</b> カタログにインポートできます。その場合は、<b>NetBackup MS SQL Client</b> 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。</p>

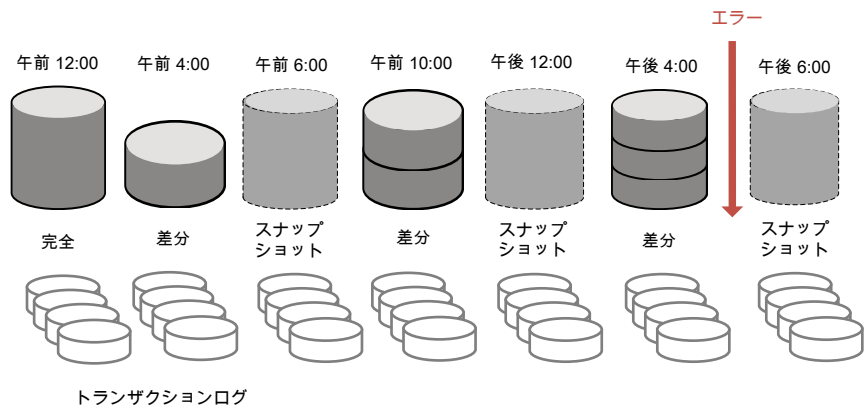
フィールド	説明
<p>可用性データベースのバックアッププリファレンス  <b>(Availability Database Backup Preference)</b></p>	<p>このオプションは、可用性グループのバックアップが発生する場所を決定します。データベースの設定とトランザクションログの設定を選択していることを確認します。</p> <ul style="list-style-type: none"> <li>■ なし (None)                      指定されたインスタンスでバックアップを実行します。このオプションは、個々の可用性データベースを保護する場合に使用します。                      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。</li> <li>■ 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せん。</li> <li>■ 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。</li> <li>■ 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。</li> </ul> <p>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</p> <p>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。</p> <ul style="list-style-type: none"> <li>■ [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。</li> <li>■ 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。</li> </ul>
<p>バックアップ後ログを切り捨て  <b>(Truncate logs after backup)</b></p>	<p>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。</p>

## コピーまたはクローキングした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となります。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



## 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。

表 6-3

方式	説明
自動	バックアップの開始時に、 <b>NetBackup</b> 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、 <b>NetBackup</b> は保護計画の資産に対して別の方式を選択します。
VSS	<p>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。</p> <p>プロバイダの形式 (Provider Type):</p> <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> </ul> <p>スナップショット属性 (Snapshot Attribute):</p> <ul style="list-style-type: none"> <li>■ 自動 (Automatic)。NetBackup が属性を選択します。</li> <li>■ 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。</li> <li>■ 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。</li> </ul>
VxVM	<p>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。</p> <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ ミラーの同期の完了を待機 (Wait for mirror sync completion)。このオプションを選択すると、ミラーの同期が完了するまでフルサイズインスタントスナップショットがバックアップに利用されないようにします。スナップショットディスクがソースと完全に同期される前にバックアップを開始し、サーバーがソースディスクへのアクセス権を持っていない場合、バックアップは失敗します。</li> <li>■ 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。</li> </ul>

# 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 Deduplication 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、次のようにします。

- [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マスターサーバーを選択します。マスターサーバーを選択し、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.41 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>

# 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。

- [保護計画への SQL Server 資産の追加](#)
- [Microsoft SQL Server 資産の保護設定の編集](#)
- [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 資産の保護の削除](#)

## 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 credenシヤルが設定されている必要があります。  
[p.33 の「SQL Server インスタンスまたはレプリカへの credenシヤルの追加」](#)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.18 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 credenシヤルが含まれる場合、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                  | <ul style="list-style-type: none"> <li>■ [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。</li> </ul>  |
| 個々のデータベース                           | <ul style="list-style-type: none"> <li>■ [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。</li> <li>■ [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。</li> </ul>  |
| 可用性グループ                             | <ul style="list-style-type: none"> <li>■ [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。</li> </ul>   |
| 個々の可用性データベース                        | <ul style="list-style-type: none"> <li>■ [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。</li> <li>■ [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。</li> </ul>   |
| SQL Server クラスタ                     | <ul style="list-style-type: none"> <li>■ [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。<br/>                     ホスト名は SQL Server クラスタの仮想名です。</li> </ul>  |
| SQL Server フェールオーバークラスタインスタンス (FCI) | <ul style="list-style-type: none"> <li>[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。</li> <li>■ 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。<br/>                     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マスター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。</li> <li>■ 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。<br/>                     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。</li> </ul> |

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、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.46 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 必要な役割の権限を持っている場合は、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.41 の「スケジュールと保持」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.41 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 資産の保護設定の編集

必要な役割の権限がある場合は、スケジュールやその他のオプションなど、保護計画の特定の設定を編集できます。

- p.41 の「[スケジュールと保持](#)」を参照してください。
- p.41 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 資産の保護設定を編集するには

- 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 必要な役割の権限を持っている場合は、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.41 の「[スケジュールと保持](#)」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.41 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。

## 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  NetBackup 管理コンソールで、従来のポリシーを使用してインスタンスや可用性グループがどのように保護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 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。



# 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](#)
- [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

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。
- NetBackup サービスが正しく構成されている必要があります。  
p.18 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。
- リストア中に指定される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ます、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。
- 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 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 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。

- セキュリティ管理者は、[セキュリティ (Security)]、[ホスト (Hosts)] 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。

## 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してリカバリ済みの状態または使用準備完了に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。

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 リストアするデータベースを見つけます。

スタンドアロンデータベース

データベースを見つけて選択します。

- [インスタンス (Instances)] タブで、リストアするデータベースを含むインスタンスをクリックします。
- [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。

SQL Server クラスタの一部であるデータベース

データベースを見つけて選択します。

- [インスタンス (Instances)] タブで、クラスタに属するインスタンスを選択します。ホスト名は SQL Server クラスタの仮想名です。
- [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。

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

[インスタンス (Instances)] タブで、次の手順を実行します。

- FCI の保護方法に応じて、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。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。
- [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。

複数の NIC を使用する SQL Server ホスト

[インスタンス (Instances)] タブで、次のいずれかを選択します。

- ホストの保護方法に応じて、インスタンス名を選択します。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インスタンス名。
- [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。

- 3 [リカバリポイント (Recovery points)] タブをクリックします。
- 4 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選択します。

- 5 [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。
- 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。

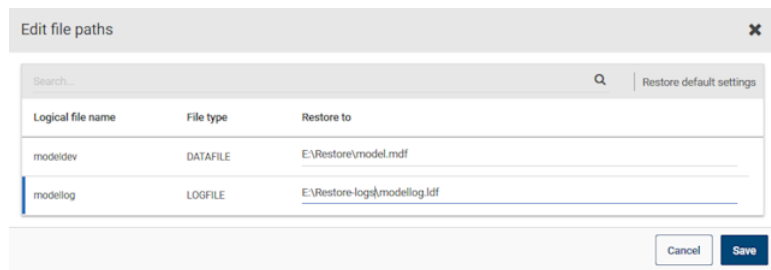
別のデータベースにリストアします。

[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。

<p>すべてを元のディレクトリにリストア (Restore everything to the original directory)</p>	<p>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。</p>
<p>すべてを異なるディレクトリにリストア (Restore everything to a different directory)</p>	<p>[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。</p>
<p>ファイルを別々のパスにリストア (Restore files to different paths)</p>	<p>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。</p>

別のパスに対するリストアの例:



- 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 [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。
- 11 その他のリカバリオプションを選択します。  
p.64 の「SQL Server のリストアオプション」を参照してください。
- 12 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.64 の「SQL Server のリストアオプション」を参照してください。
- 13 [次へ (Next)]をクリックします。
- 14 [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。
- 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 リストアするデータベースの名前を見つけます。

スタンドアロンデータベース データベースを見つけて選択します。

- [インスタンス (Instances)]タブで、リストアするデータベースを含むインスタンスをクリックします。
- [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。

SQL Server クラスタの一部であるデータベース データベースを見つけて選択します。

- [インスタンス (Instances)]タブで、クラスタに属するインスタンスを選択します。  
ホスト名は SQL Server クラスタの仮想名です。
- [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。

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 [インスタンス (Instances)]タブで、次の手順を実行します。

- FCI の保護方法に応じて、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。  
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。
- [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。

複数の NIC を使用する SQL Server ホスト [インスタンス (Instances)] タブで、次のいずれかを選択します。

- ホストの保護方法に応じて、インスタンス名を選択します。  
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インスタンス名。
- [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。

- 3 [リカバリポイント (Recovery points)] タブをクリックします。
- 4 リストアする完全、差分、またはトランザクションログを選択します。[処理 (Actions)] メニューで [1 つのリカバリポイントのリカバリ (Restore single recovery point)] を選択します。
- 5 (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)

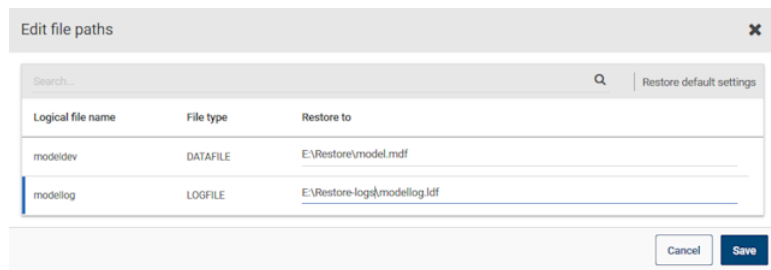
- トランザクションマーク以前にリストアするかどうかを選択します。
- トランザクションマークの名前を入力します。
- 特定の日付の後に発生するトランザクションマークを選択するには、[特定の日時後 (After specific date and time)] を選択します。次に、日付と時刻を指定します。

- 6 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できます。
  - 別のインスタンスにリストアするには、[インスタンス (Instances)] 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するには、[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するには、[データベース名 (Database name)] フィールドに名前を入力します。

7 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:



8 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。

9 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.64 の「SQL Server のリストアオプション」を参照してください。

10 [次へ (Next)]をクリックします。

11 [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。
- 12** 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)	<p>リストア後にデータベースの状態を選択します。</p> <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> </ul>



オプション	説明
一貫性チェック (Consistency check)	<p>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。</p> <ul style="list-style-type: none"> <li>■ 実行しない (Do not perform) 一貫性チェックを実行しません。</li> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> </ul>
既存のデータベースを上書きする (Overwrite the existing database)	<p>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。</p> <p>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。</p>
VDI タイムアウト (VDI timeout)	<p>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>

## 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

- 1 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。
- 2 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、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。
- 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.64 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。
- 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。

- |   |  |
|---|--|
| <p>選択したリカバリポイント<br/>(Recovery point selected)</p> | <p>指定された時間にデータベースをリストアします。</p>   |
| <p>指定した時点 (Point in time)</p>                     | <p>データベースのリストアを行う別の時点を選択します。</p>   |
| <p>トランザクションログマーク<br/>(Transaction log mark)</p>   | <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ トランザクションマークの名前を入力します。</li> <li>■ 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。</li> </ul> |

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.64 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アルを入力し、[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.64 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、RHEL 7.6 および RHEL 7.7 の最新のアプライアンスのオペレーティングシステムのバージョンと同じ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。これは、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。
  - ストレージの構成を開始する前に、新しい BYO nginx 構成エントリ /etc/nginx/conf.d/byo.conf が、元の /etc/nginx/nginx.conf ファイルの HTTP セクションに含まれることを確認します。
  - 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。
  - マスターサーバー、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。
  - 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構成の必要条件

表 9-1 ハードウェア構成の必要条件

CPU	メモリ	ディスク
<ul style="list-style-type: none"> <li>2.2 GHz 以上のクロックレート。</li> <li>64 ビットのプロセッサ。</li> <li>最小 4 コア。8 コアを推奨。</li> </ul> <p>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。</p>	<ul style="list-style-type: none"> <li>16 GB (8 TB から 32 TB のストレージの場合)。</li> <li>1 TB のストレージの場合は 1 GB の RAM。</li> <li>32 TB 以上のストレージの場合は 32 GB の RAM。</li> <li>ライブマウントごとに追加の 500 MB の RAM。</li> </ul>	<p>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ブール (MSDP) のハードウェアの必要条件を参照してください。</p>

## 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)
- 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マスターサーバーが **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マスターサーバーで **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 9.0** 以降では最初に、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** ユーザーを構成し、クライアントでクレデンシャルを入力する必要があります。この構成は、**NetBackup 9.0** にアップグレードする場合も必要です。

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** 共有に使用できます。この場合、共有へのアクセスにクレデンシャルは不要です。

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ために実行する手順を説明します。

**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
アプライアンスユーザーの場合	<p>アプライアンスの場合、ローカルユーザーは <b>Samba</b> ユーザーでもありません。</p> <p>ローカルユーザーを管理するには、<b>CLISH</b> にログオンし、<b>[Main]&gt;[Settings]&gt;[Security]&gt;[Authentication]&gt;[LocalUser]</b>の順に選択します。</p> <p><b>Samba</b> 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オンパスワードと同じです。</p>

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: <ol style="list-style-type: none"> <li>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 test_samba_user 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> </li> <li>新しい SMB パスワードを入力します。</li> <li>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。</li> </ol> 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: smbpasswd -a test_samba_user

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ヤ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。

## 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構成とデータベースの開始

完全バックアップ、トランザクションログバックアップまたは増分バックアップから、インスタントアクセスデータベースを構成できます。データベースを SQL Server インスタンスに自動的に追加するように選択できます。

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

- 左側の[Microsoft SQL Server]をクリックします。
- [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。
- [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。
- バックアップイメージを右クリックし、[処理 (Actions)]、[インスタントアクセスの構成 (Configure instant access)]をクリックします。

- 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 SQL Server インスタンスのユーザー名とパスワードを入力します。
- 10 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.78 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。
- 11 (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。
- 12 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。
- 13 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.76 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

完全バックアップからインスタントアクセスデータベースを構成できます。インスタントアクセスデータベースを作成した後に開始しない場合は、ホスト名を入力するか、インスタントアクセスデータベースを作成する名前を選択できます。インスタントアクセスデータベースが作成されると、データベースはインスタンスに追加されず、Samba 共有にエクスポートされます。

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 左側の[Microsoft SQL Server]をクリックします。
- 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右クリックし、[処理 (Actions)]、[インスタントアクセスの構成 (Configure instant access)] をクリックします。
- 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.76 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 左側の[Microsoft SQL Server]をクリックします。
- 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 左側の[Microsoft SQL Server]をクリックします。
- 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 行の右にある処理メニューで[削除 (Delete)]を選択します。
- 4 次のいずれかを実行します。
  - 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。 <ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> </ul>
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。 <ul style="list-style-type: none"> <li>■ 実行しない (Do not perform)                              一貫性チェックを実行しません。</li> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> <li>■ 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。</li> </ul>

オプション	説明
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.74 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 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。 <ol style="list-style-type: none"><li>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。</li><li>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。</li><li>3 コマンド <code>/usr/openshift/pdce/vpfs/bin/vpfs_config.sh --configure_byo</code> を実行します。</li></ol>
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。 <ol style="list-style-type: none"><li>1 Yum ツールを使用して、<code>policycoreutils</code> と <code>policycoreutils-python</code> パッケージをインストールします。</li><li>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。<ul style="list-style-type: none"><li>■ <code>semanage port -a -t http_port_t -p tcp 10087</code></li><li>■ <code>setsebool -P httpd_can_network_connect 1</code></li></ul></li><li>3 コマンド <code>/usr/openshift/pdce/vpfs/bin/vpfs_config.sh --configure_byo</code> を実行します。</li></ol>



適用対象	よく寄せられる質問	回答
BYO	<p>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。</p> <p>外部 CA (*.pem 証明書) で署名された証明書で置き換えることが必要な場合は、どのようにしたら良いですか。</p>	<p>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 に進みません。</p> <ol style="list-style-type: none"> <li>1 RSA の公開鍵と秘密鍵のペアを作成します。</li> <li>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。</li> <li>3 外部認証局が証明書を作成します。</li> <li>4 &lt;PDDE ストレージのパス &gt;/spws/var/keys/spws.cert を証明書に置き換え、&lt;PDDE ストレージのパス &gt;/spws/var/keys/spws.key を秘密鍵に置き換えます。</li> <li>5 次のコマンドを実行して、証明書を再ロードします。  /usr/opensv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</li> </ol>
BYO	<p>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。</p> <p>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。</p> <p>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。</p>	<p>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。</p> <p><a href="https://access.redhat.com/solutions/20107">https://access.redhat.com/solutions/20107</a></p>

適用対象	よく寄せられる質問	回答
BYO	<p>/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。</p> <pre>**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) **** /usr/opensv/netbackup/bin/nblibcurlcmd failed (1):</pre>	<p>次に示す順序で操作を実行します。</p> <ol style="list-style-type: none"> <li><b>1 NetBackup</b> マスターサーバーが起動しており、ファイアウォールが <b>NetBackup</b> マスター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。</li> <li><b>2</b> 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。  /usr/opensv/netbackup/bin/bpcintcmd -pn</li> <li><b>3 NetBackup</b> マスターサーバーを起動し、<b>NetBackup</b> マスター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。  /usr/opensv/pdde/vpfs/bin/vpfs_config.sh --configure_byo</li> </ol>
BYO	<p>MSSQL 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、<b>Samba</b> 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。</p> <p>次のリンク先に、クライアントの Windows バージョンとバックグラウンドの一覧が示されています。</p> <p><a href="https://support.microsoft.com/en-us/help/4046019/guest-access-in-smb2-disabled-by-default-in-windows-10-and-windows-ser">https://support.microsoft.com/en-us/help/4046019/guest-access-in-smb2-disabled-by-default-in-windows-10-and-windows-ser</a></p>	<p>次に示す順序で操作を実行します。</p> <ol style="list-style-type: none"> <li><b>1 Samba</b> 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。 <ul style="list-style-type: none"> <li>■ 次の <b>Samba</b> 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</li> <li>■ <b>Samba</b> のユーザークレデンシアルを作成します。 <ul style="list-style-type: none"> <li>■ smbpasswd -a spws Samba ユーザー spws の Samba パスワードを設定</li> <li>■ smbpasswd -e spws Samba ユーザー spws を有効化</li> </ul> </li> </ul> </li> <li><b>2</b> 以前のクレデンシアルを使用して <b>Samba</b> 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 クレデンシアルを保存します。</li> </ol>

適用対象	よく寄せられる質問	回答
<p>アプライアンス</p>	<p>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。</p>	<p>次に示す順序で操作を実行します。</p> <ol style="list-style-type: none"> <li>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、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 &gt; Settings &gt; Security &gt; Authentication &gt; LocalUser</li> <li>2 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のクレデンシアルを保存します。</li> </ol>

# 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 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。

- 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。
- 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用することができます。

### 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](https://www.veritas.com/content/support/en_US/doc/NB_70_80_VE)

## Veritas VSS プロバイダ

p.19 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。

# 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 保護計画は、仮想マシン上の SQL Server データを保護できます。ユーザーはその後、保護計画に資産をサブスクライブできます。保護計画を作成する前に、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.20 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.22 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、セキュリティ管理者または類似の 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.41 の「スケジュールと保持」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

<p>バックアップストレージ (Backup storage)</p>	<p>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。</p>	<p>[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。</p>
-------------------------------------	---	--

- 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.86 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。

(オプション) 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る場合は、[ログを切り捨てる (Truncate logs)] を選択します。

- 10 [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 [ロール (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。

- 11 [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。

## 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 10-1 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。
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.88 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 10-2 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。

オプション	説明
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。  Microsoft Exchange Server または Microsoft SharePoint Server の NetBackup 8.3 以前のアプリケーションデータは、NetBackup の [バックアップ、アーカイブおよびリストア (Backup, Archive, and Restore)] インターフェースでリストアする必要があります。Microsoft SQL Server のデータは、NetBackup MS SQL Client を使用してリストアする必要があります。詳しくは、NetBackup データベースエージェントのマニュアル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.89 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 10-3** 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。
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。



除外オプション	説明
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)	<p>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。</p> <p>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。</p> <p>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。『<a href="#">NetBackup Plug-in for VMware vSphere Web Client ガイド</a>』または『<a href="#">NetBackup Plug-in for VMware vSphere Client (HTML5) ガイド</a>』を参照してください。</p>
除外する特定のディスク (Specific disks to be excluded)	<p>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。</p> <p>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。</p>

## 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 10-4 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。
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リブします。保護計画に資産をサブスクリブするときに、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

- 1 左側の [VMware] をクリックします。
- 2 [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。
- 3 保護計画を選択し、[次へ (Next)] をクリックします。
- 4 必要な役割の権限を持っている場合は、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.41 の「[スケジュールと保持](#)」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.86 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.86 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ために NetBackup MS SQL Client を使用する方法について説明します。NetBackup Web UI では現在、VMware バックアップからの個々の SQL Server データベースのリストアをサポートしていません。

### 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 NetBackup MS SQL Client を起動します。
- 2 リストアするバックアップイメージを表示します。
- 3 データベースインスタンスとデータベースを展開します。
- 4 リストアするデータベースイメージを選択します。

SQL Server の VMware バックアップでは、[リカバリ済み (Recovered)]リカバリオプションのみを利用できます。

- 5 [リストア (Restore)]をクリックします。

# 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。

- [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](#)
- [SQL Server の VMware バックアップとリストアの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](#)

## 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>。	<ul style="list-style-type: none"> <li>■ 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。</li> <li>■ 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>p.22 の「<a href="#">SQL Server のローカルセキュリティの権限の構成</a>」を参照してください。</p> </li> </ul>
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。	<p>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> <p>p.20 の「<a href="#">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</a>」を参照してください。</p>

## SQL Server の VMware バックアップとリストアの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 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 ポリシーを使用する SQL Server の保護での問題

問題	説明
データベースのバックアップが失敗する。	<p>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に存在する場合にのみカタログ化され、保護されます。Raw デバイスマッピング (RDM)、独立とマーク付けされている仮想マシンディスク (vmdk) ボリューム、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、または除外された Windows ブートディスクはサポートされていません。</p> <p>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。</p>
ASC ジョブが状態 1 (部分的に成功) を生成する。	<p>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。</p> <p>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。</p>
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。	<p>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。</p> <p>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。</p> <p>[仮想マシンの静止 (Virtual machine quiesce)] オプションを無効にしました。</p> <p>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。</p> <p>[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。</p> <p>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。『<a href="#">NetBackup for VMware 管理者ガイド</a>』を参照してください。</p> <p>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。</p>

問題	説明
バックアップから仮想マシン全体をリカバリできますが、データベースを個別にリカバリすることはできない。	仮想マシンのバックアップからデータベースをリカバリするための[Microsoft SQL Server (Microsoft SQL Server)]を選択していない

## 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。