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

リリース 8.3

VERITAS™

NetBackup Web UI Microsoft SQL Server 管理者ガイド

最終更新日: 2020-09-21

法的通知と登録商標

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

テクニカルサポート

テクニカルサポートはグローバルにサポートセンターを管理しています。すべてのサポートサービスは、サポート契約と現在のエンタープライズテクニカルサポートポリシーに応じて提供されます。サポート内容およびテクニカルサポートの利用方法に関する情報については、次のWebサイトにアクセスしてください。

https://www.veritas.com/support

次の URL で Veritas Account の情報を管理できます。

https://my.veritas.com

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

世界共通 (日本を除く)	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

マニュアル

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

https://sort.veritas.com/documents

マニュアルに対するご意見

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

目次

1

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。

- Web UI について
- 用語
- Web UI へのサインイン
- Web UI からのサインアウト

Web UI について

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、ソフトウェア互換性リストを参照してください。
- 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 へのユーザーアクセスを構成し、セキュリティ、バックアップ管理、または作業負荷の保護などのタスクを委任できます。
- 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、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、ライセンスを表示および管理できます。

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

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。
  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。アクセス制御 (NBAC) が有効な場合は、Web UI を使用できません。

ジョブおよびイベントの監視

Web UIを使用すると、管理者はより簡単に 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、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。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。
- 作業負荷管理者は、必要な RBAC 権限を使用して、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詳しくは、『 Web UI 管理者ガイド』を参照してください。
- 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	と、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、の完全なアクセス権を持ちます。Web UI の各ガイドでは、*管理者*という用語は、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 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。
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。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	Web UI 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、管理コンソールで作成します。

用語	定義
外部証明書	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、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	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。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	NetBackup CA 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、Web UI 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、管理コンソールまたは CLI へのアクセスを制御しません。Web UI は、アクセス制御 (NBAC) ではサポートされておらず、NBAC が有効になっている場合は使用できません。
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デ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。
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。

Web UI へのサインイン

権限を持つユーザーは、Web UI を使用して、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 Web UI にサインインできます。詳しくは、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 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 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	*username*	jane_doe
Windows ユーザー	*DOMAIN¥username*	WINDOWS¥jane_doe
UNIX ユーザー	*username@domain*	john_doe@unix

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 Web UI にサインインできます。詳しくは、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 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

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 Web UI にサインインできます。詳しくは、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 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 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、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。

Web UI からのサインアウト

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、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。

Web UI からサインアウトするには

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

2

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。

の概要

Web UI では、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。インスタンスは環境内で自動的に検出され、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。

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
- 資産を保護するための保護プランの選択
- 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、を「」と記載します。は「 for 」と記載します。

表 2-1 の機能

機能	説明
保護計画	次の利点があります。 ■ 複数の 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。 ■ 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。 ■ 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。 ■ 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、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。
資産の管理	は自動的に環境内の 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、作業負荷管理者は、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。
認証およびクレデンシャル	保護計画は次をサポートします。 ■ Windows 認証および Windows Active Directory 認証。 ■ 適切に構成すると、サービスアカウントをクライアント上で の特権ユーザーとして実行する必要がなくなります。
バックアップおよびリストア機能	バックアップとリストアでは次の機能を利用できます。 ■ バックアップは、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。 ■ Web UI は、1 つのインターフェースからデータベースとトランザクションログのバックアップとリストアをサポートします。 注意: Web UI を使用した リカバリでは、クライアントがバージョン 8.3 以降である必要があります。 ■ 完全バックアップ、差分バックアップ、トランザクションログバックアップのバックアップスケジュール。 ■ 手動バックアップとコピーのみバックアップ。 ■ クラスタと可用性グループを含む、高可用性 (HA) 環境のサポート。 ■ オブジェクトの別の場所へのリストア (リダイレクトリストア)。 ■ バックアップ中に複数のストライプを使うための機能です。 ■ バックアップのパフォーマンスを改善できるチューニングオプション。
ストリームベースのバックアップおよびリストア	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った、ストリームベースでの オブジェクトのバックアップとリストア。

機能	説明
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	では、スナップショット方式を使用して のバックアップを実行できます。 また、NetBackup バックアップイメージから、インスタントアクセスデータベースを作成できます。データベースは瞬時に利用可能になるため、ほぼゼロのリカバリ時間目標を達成できます。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。
を保護する VMware バックアップのサポート	スナップショットを使用した、VMware コンピュータのアプリケーションで一貫した完全バックアップのサポート。また、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。 詳しくは、次の文書を参照してください。 『 for VMware 管理者ガイド』 『 管理者ガイド Vol. 1』

3

Microsoft SQL Server の管理

この章では以下の項目について説明しています。

オブジェクトの検出について

による検出を定期的に実行して、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。 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 (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、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、『 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、は、詳細検出データが再送信されたときに、次回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

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)]、[]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

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)]、[]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。

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。

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。

インスタンスを参照するには

1. 左側で[作業負荷 (Workloads)]、[]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

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。

可用性グループを参照するには

1. 左側で[作業負荷 (Workloads)]、[]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

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。

データベースを参照するには

1. 左側で［作業負荷 (Workloads)］、［］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

インスタンスまたはレプリカへのクレデンシャルの選択または追加

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クレデンシャルを選択または追加する必要があります。使用するクレデンシャルオプションの要件を確認します。

p.21 の「 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にクレデンシャルを選択または追加するには

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。

   可用性グループの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。
4. 次のいずれかのオプションを選択します。資産にクレデンシャルを選択または追加できるようにするには、特定の RBAC 権限が必要です。

   詳しくは、『 Web UI 管理者ガイド』を参照するか、管理者にお問い合わせください。

既存のクレデンシャルから選択してください (Select from existing credentials)	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。
クレデンシャルを追加 (Add credentials)	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。

5. ［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。

必要な RBAC 権限を持っている場合は、次の操作が可能です (複数の操作も可能)。

- 別の RBAC の役割を追加してクレデンシャルのアクセス権を付与する
- クレデンシャルの役割の権限を編集する
- 役割を削除する

6 [次へ (Next)]をクリックします。クレデンシャルの設定を確認し、[完了 (Finish)]をクリックします。

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。

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。

クレデンシャルについて

を保護するには、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。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 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 3-1 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 (Option to register credentials)	環境または構成
これらの特定のクレデンシャルを使用 (Use these specific credentials) (推奨)	■ DBA が ユーザークレデンシャルを 管理者に提供する。 ■ DBA がクライアント上で特権のある ユーザーとして サービスを実行することを要求しない。 構成要件 クレデンシャルを登録するために使用されるユーザーアカウントは、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。 サービスは、ローカルシステムログオンアカウントを使用できます。別のログオンアカウントを使用する場合は、そのアカウントにも特定のローカルセキュリティ権限が必要です。

クレデンシャルを登録するオプション (Option to register credentials)	環境または構成
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)	■ サービスはクライアント上で特権のある ユーザーとして動作する。 ■ 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。 ■ 管理者が クレデンシャルへのアクセス権を持っていない。 構成要件 クレデンシャルを登録するために使用されるユーザーアカウントは、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。 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。

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

が 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 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 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。

が複数の NIC を使用する ホストを検出すると、[インスタンス (Instances)]タブで 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 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 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 クラスタでは、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。

詳しくは、『 for Web UI 管理者ガイド』を参照するか、管理者にお問い合わせください。

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

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、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。

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 クラスタの一部である場合、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。 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。

『 for Microsoft SQL Server 管理者ガイド』を参照してください。

SQL Server のバックアップとリストアのための サービスの設定

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

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「sysadmin」ロールが必要です。
- 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、sysadmin ロールを 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。

のバックアップとリストアのために サービスを設定するには

1. sysadmin ロール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、Client Service を開きます。
3. [ローカルシステムアカウント (Local System account)]または 管理者アカウントが設定されていることを確認します。

   [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)]設定を使ってインスタンスを登録する場合は、両方のサービスが同一のログオンアカウントを使う必要があります。[これらの特定のクレデンシャルを使う (Use these specific credentials)]設定を使ってインスタンスを登録する場合は、これらのサービスで同じログオンアカウントを使うか、別々のログオンアカウントを使うことができます。
4. Legacy Network Service を開きます。

5 [ローカルシステムアカウント (Local System account)]または 管理者アカウントが設定されていることを確認します。

[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)]設定を使ってインスタンスを登録する場合は、両方のサービスが同一のログオンアカウントを使う必要があります。[これらの特定のクレデンシャルを使う (Use these specific credentials)]設定を使ってインスタンスを登録する場合は、これらのサービスで同じログオンアカウントを使うか、別々のログオンアカウントを使うことができます。

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 [これらの特定のクレデンシャルを使用 (Use these specific credentials)]オプションを選択する場合、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。

p.24 の「 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。

のローカルセキュリティの権限の構成

[これらの特定のクレデンシャルを使用 (Use these specific credentials)]オプションを使ってクレデンシャルを作成する場合、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。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 この変更を有効にするために、グループポリシーの更新コマンド (グループポリシーの更新) を実行します。

```
gpupdate /Force
```

5 Client Service と 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 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。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。

クレデンシャルの管理

適切な RBAC 権限を持つユーザーは、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。

クレデンシャルを編集するには

1 左側で[作業負荷 (Workloads)]、[]、[インスタンス (Instances)]タブの順にクリックします。

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。

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。

インスタンスを削除するには

1 左側の[]をクリックし、[インスタンス (Instances)]タブをクリックします。

2 インスタンスのチェックボックスに移動してチェックマークを付けます。

3 [削除 (Remove)]をクリックします。

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

インスタンスの手動での追加

新たに検出された 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。

インスタンスを手動で追加するには

1. 左側の[]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。
   - クラスタの場合、ホスト名は 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、ホスト名はホストまたは仮想 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、クラスタの仮想名を入力します。
     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.20 の「 インスタンスまたはレプリカへのクレデンシャルの選択または追加」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。

4

Microsoft 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。

資産の保護

次の手順を使用して、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。

- 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。
- 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。

資産を保護するには

1 左側で[作業負荷 (Workloads)]、[]の順にクリックします。

2 保護する資産 (複数可) を選択します。

インスタンス内のすべてのデータベース	■ [インスタンス (Instances)]タブで、保護するインスタンスのチェックボックスにチェックマークを付けます。
個々のデータベース	■ [インスタンス(Instances)]タブで、保護するデータベースを含むインスタンスのチェックボックスにチェックマークを付けます。 ■ [データベース (Databases)]タブで、1 つ以上のデータベースのチェックボックスにチェックマークを付けます。
可用性グループ	■ [可用性グループ (Availability groups)]タブで、可用性グループ名のチェックボックスにチェックマークを付けます。
個々の可用性データベース	■ [可用性グループ (Availability groups)]タブで、保護するデータベースを含む可用性グループの名前をクリックします。 ■ [データベース (Databases)]タブで、1 つ以上のデータベースのチェックボックスにチェックマークを付けます。
クラスタ	■ [インスタンス (Instances)]タブで、クラスタに属するインスタンスのチェックボックスにチェックマークを付けます。 ホスト名は クラスタの仮想名です。
フェールオーバークラスタインスタンス (FCI)	[インスタンス (instance)]タブで、クラスタまたはクラスタ内のノードを保護する必要があるかどうかに応じて、インスタンス名を選択します。 ■ ホスト名が FCI のクラスタ名である場合のインスタンス名。 バックアップはアクティブノードで試行されます。両方のノードが同じ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。 ■ ホスト名が FCI の物理ノード名のいずれかである場合のインスタンス名。 正常にバックアップを作成するには、このノードがクラスタ内のアクティブノードである必要があります。バックアップはクラスタ名に基づいてカタログ化されます。
複数の NIC を使用する 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 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 のプライベートインターフェース名である場合に、複数の NIC を使用する 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.35 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.30 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.31 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。

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.30 の「スケジュールと保持」を参照してください。
- p.31 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。

資産の保護設定を編集するには

1. 左側で[作業負荷 (Workloads)]、[]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.30 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.31 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。

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 4-1

オプション	説明
反復 (Recurrence) (間隔)	注意: この設定は、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、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 4-2 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)	(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。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、から マスターサーバーへのデータ送信を高速化できます。 このオプションのデフォルト値は 2 で、Double Buffering を有効にします。この値を大きくすると、パフォーマンスがわずかに向上する場合があります。範囲は 1 から 32 です。
最大転送サイズ (Maximum transfer size)	(ストリームベースのバックアップのみ) このオプションは、SQL Server バックアップイメージの読み込みと書き込みに使われるバッファサイズです。通常、この値を大きくすると、SQL Server のパフォーマンスが向上します。このオプションは、個々のバックアップ操作に対して設定できます。64 KB * 2^MAX_TRANSFER_SIZE のように計算されます。64 KB から 4 MB の範囲でサイズを指定できます。デフォルトは 4 MB です。
並列バックアップ操作 (Parallel backup operations)	このオプションでは、データベースインスタンスごとの、同時に開始するバックアップ処理の数を指定します。範囲は 1 から 32 です。デフォルトは 1 です。
VDI タイムアウト (秒) (VDI Timeout (seconds))	SQL Server 仮想デバイスインターフェースのタイムアウト間隔を指定します。選択した間隔は、データベースとトランザクションログのバックアップとリストアに適用されます。 バックアップのデフォルト値は 300 です。リストアジョブのデフォルト値は 600 です。範囲は 300 から 2147483647 です。

フィールド	説明
Microsoft SQL Server の圧縮を使用 (Use Microsoft SQL Server compression)	SQL Server を使用してバックアップイメージを圧縮するには、このオプションを有効にします。SQL Server の圧縮を有効にした場合、 の圧縮を有効にしないでください。 SQL Server の圧縮は、スナップショットバックアップではサポートされません。
[利用できないデータベース(オフライン、リストア中など) をスキップ (Skip unavailable (offline, restoring, etc.) databases)]	では、 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。 では、利用できないデータベースのバックアップがスキップされますが、保護計画にサブスクライブされたその他のデータベースのバックアップは続行されます。バックアップは状態 0 で完了し、ジョブの詳細にデータベースがスキップされたことが示されます。
コピーのみバックアップの作成	このオプションでは、SQL Server 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。
Microsoft SQL Server チェックサムの実行 (Perform Microsoft SQL Server checksum)	SQL Server のバックアップチェックサムに、次のオプションのいずれかを選択してください。 ■ なし。バックアップチェックサムを無効にします。 ■ バックアップの前にチェックサムを検証するには、次のオプションのいずれかを選択してください。これらのオプションでは、バックアップ操作またはリストア操作でパフォーマンスが低下することに注意してください。 ■ エラー時続行 (Continue on error)。バックアップ時に検証エラーが発生した場合でも、バックアップは続行します。 ■ エラーによる失敗 (Fail on error)。バックアップ時に検証エラーが発生した場合、バックアップは停止されます。
増分バックアップを完全バックアップに変換 (Convert incremental backup to full backup)	データベースに対して以前の完全バックアップが存在しない場合は、は差分バックアップを完全バックアップに変換します。 エージェントは、各データベースの完全バックアップが存在するかどうかを判断します。以前の完全バックアップが存在する場合は、差分バックアップが次のように完全バックアップに変換されます。 ■ 差分バックアップのデータベースを選択すると、バックアップは完全データベースバックアップに変換されます。 ■ スナップショットバックアップポリシーの場合は、差分バックアップから完全バックアップに正常に変換させるために[完全 (Full)]スケジュールが必要です。 注意: 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 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、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、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、 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 カタログにインポートできます。その場合は、MS SQL Client を使用して完全と差分の両方のバックアップをリストアできます。

フィールド	説明
トランザクションログバックアップを完全バックアップに変換 (Convert transaction log backup to full backup)	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、はトランザクションバックアップを完全バックアップに変換します。 このオプションでは、完全リカバリデータベースが単純リカバリモデルに切り替えられ、完全リカバリモデルに戻されたかどうかも検出されます。このシナリオでは、ログチェーンは分割され、SQL Server は、以降のログバックアップを作成するには、その前に差分バックアップを必要とします。がこの状況を検出した場合は、バックアップはデータベースの差分バックアップに変換されます。 注意: 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 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、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、MS SQL Client を使用した差分バックアップとログバックアップのリストアが可能です。または、バックアップが期限切れになっている場合、完全バックアップを カタログにインポートできます。その場合は、MS SQL Client を使用して完全バックアップ、差分バックアップ、ログバックアップをリストアできます。

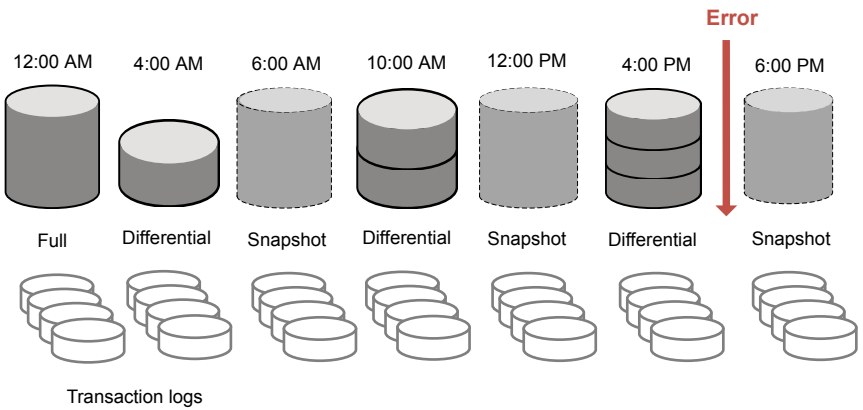
フィールド	説明
可用性データベースのバックアッププリファレンス (Availability Database Backup Preference)	このオプションは、可用性グループのバックアップが発生する場所を決定します。データベースの設定とトランザクションログの設定を選択していることを確認します。 ■ なし (None) 指定されたインスタンスでバックアップを実行します。このオプションは、個々の可用性データベースを保護する場合に使用します。 注意: 可用性グループを保護する場合は、このオプションを選択しないでください。 ■ プライマリレプリカを保護する (Protect primary replica)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

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を保護する場合は、次のスナップショットバックアップが作成された後、前回のスナップショットバックアップが期限切れになります。最後のバックアップより前の指定した時点へのリストアが必要な場合、差分バックアップは、存在しなくなったスナップショットバックアップに基づくことになります。または、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が終了するまでエラーが検出されない場合は、リストアに利用可能なスナップショットバックアップがありません。図 4-1を参照してください。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 4-1　　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、『 Snapshot Client 管理者ガイド』を参照してください。

表 4-3

方式	説明
自動	バックアップの開始時に、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、は保護計画の資産に対して別の方式を選択します。
VSS	VSS は Windows のボリュームシャドウコピーサービスを使用します。VSS はローカルバックアップに使用され、選択される実際のスナップショット方式は、クライアント上に構成されているスナップショットプロバイダによって異なります。 プロバイダの形式 (Provider Type): ■ 自動 (Automatic)。は、利用可能なプロバイダをハードウェア、ソフトウェア、システムの順に選択します。 ■ システム (System)。ブロックレベルのコピーオンライトスナップショットに Microsoft システムプロバイダを使用します。 ■ ソフトウェアプロバイダを使用し、ファイルシステムと Volume Manager の間のソフトウェアレベルの I/O 要求をインターセプトします。 ■ ディスクアレイ用のハードウェアプロバイダを使用します。 スナップショット属性 (Snapshot Attribute): ■ 自動 (Automatic)。が属性を選択します。 ■ 差分 (Differential)。コピーオンライト形式のスナップショットを使用します。 ■ プレックス (Plex)。クローンまたはミラー形式のスナップショットを使用します。
VxVM	Volume Manager ボリュームに構成されている任意のデータを含むスナップショットの場合。 ■ バックグラウンドでミラーを再同期化する (Resynchronize mirror in background)。バックアップリソースをより効率的に使用できるようにするには、このオプションを選択します。2 つのバックアップで同じテープドライブが必要な場合、最初のジョブの再同期化操作が完了していない場合でも、2 番目のジョブを開始できます。 ■ ミラーの同期の完了を待機 (Wait for mirror sync completion)。このオプションを選択すると、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。 ■ 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。

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)]、[]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 4-4　　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 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

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ライブを解除できます。資産のサブスクライブが解除されると、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ライブを解除するときに、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ライブされており、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ライブ解除されます。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 左側の[]をクリックします。

2 サブスクライブ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。

5

Microsoft 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。

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。

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 権限を持っている必要があります。
- が宛先クライアントと通信できる必要があります。

データベースの完全リカバリを実行するには

1. 左側で[作業負荷 (Workloads)]、[]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。

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 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。

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 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 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 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。

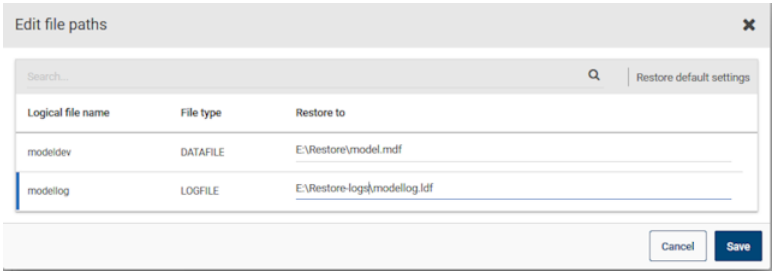
7 リカバリするホスト、インスタンス、データベースを選択します。次のオプションがあります。

- 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。

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

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

別のパスに対するリストアの例:



9 リ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。

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.45 の「 リストアのオプション」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.45 の「 リストアのオプション」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。
- 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)]、[]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。
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 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。

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 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 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 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。

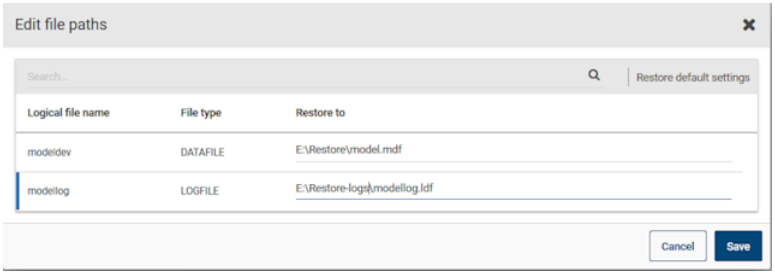
6 リカバリするホスト、インスタンス、データベースを選択します。次のオプションがあります。

- 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。

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.45 の「 リストアのオプション」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。

リストアのオプション

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 5-1 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)	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。

オプション	説明
リストア後のデータベースのリカバリ状態 (Database recovery state after restore)	リストア後にデータベースの状態を選択します。 ■ リカバリ (Recover) リストアシーケンスの最後のイメージをリストアし、データベースを使用できるようにします。 ■ リストアしています (Restoring) 中間バックアップイメージをリストアします。データベースはロード状態のままになるため、追加のバックアップイメージをリストアして適用できます。 ■ スタンバイ (Standby) トランザクションログおよびデータベースのリストア時に、スタンバイデータベースを作成して保持します。このオプションを選択する場合は、スタンバイの取り消しログが必要です。このログは、デフォルトではプライマリデータファイルと同じディレクトリにあります。サービスを実行するアカウントには SQLStandBy フォルダのフルアクセス権が必要です。
一貫性チェック (Consistency check)	リストア後に実行する一貫性チェック。一貫性チェックの出力は、クライアントの進捗ログに書き込まれます。 ■ 実行しない (Do not perform) 一貫性チェックを実行しません。 ■ インデックスを含む完全チェック (Full check, including indexes) 一貫性チェックにインデックスを含めます。エラーはログに記録されます。 ■ インデックスを含まない完全チェック (Full check, excluding indexes) 一貫性チェックからインデックスをエクスクルードします。インデックスをチェックしない場合、一貫性チェックの実行速度は大幅に向上しますが、完全にはチェックされません。一貫性チェックでは、各ユーザー表のデータページおよびクラスタ化インデックスページだけが対象となります。クラスタ化されていないインデックスページの一貫性はチェックされません。 ■ カタログのチェック (Check catalog) 指定したデータベースのシステムテーブル内およびシステムテーブル間の一貫性をチェックします。 ■ 物理チェックのみ (Physical check only) オーバーヘッドの少ない データベースの物理的な一貫性をチェックします。このオプションでは、ページヘッダーおよびレコードヘッダーの物理構造の整合性のみを検証します。また、ページのオブジェクト ID やインデックス ID と割り当て構造の間の一貫性もチェックします。
既存のデータベースを上書きする (Overwrite the existing database)	は、データベースまたはデータベースファイルがすでに存在する場合は、それらのファイルを上書きできます。 この操作が実行できない場合は、必要な RBAC 権限について 管理者にお問い合わせください。
VDI タイムアウト (VDI timeout)	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。

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)]、[]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。
     - [次へ (Next)]をクリックします。

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 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.45 の「 リストアのオプション」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、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 Web UI で[作業負荷 (Workloads)]、[]を選択します。

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。

- 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。

9 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.45 の「 リストアのオプション」を参照してください。

10 [次へ (Next)]をクリックします。次に、[リカバリの開始 (Start recovery)]をクリックします。

11 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。

12 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。

13 Web UI で[作業負荷 (Workloads)]、[]を選択します。

14 [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。

15 [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。

16 [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。

17 [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。

18 [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。

19 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。

20 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.45 の「 リストアのオプション」を参照してください。

21 [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。

22 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。

23 可用性グループの追加レプリカに対して、手順 12 から手順 22 を繰り返します。

6

インスタントアクセス

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

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ていることを確認します。
  - `policycoreutils` と `policycoreutils-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 6-1 ハードウェア構成の必要条件

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

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 Microsoft SQL Server のバックアップでは、Microsoft SQL インスタントアクセスはサポートされません。
  - アプリケーション認識バックアップ (VMware)
  - ストリームベースのバックアップ
  - NBU バックアップ圧縮
  - レガシー SQL Server バックアップ (BCH バックアップ)
  - 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)])
  - MSSQL DB ミラーリング (スタンドアロンの IA DB としての作成のみサポート)
  - MSSQL クラスタ設定 (スタンドアロンの IA DB としての作成のみサポート)
- 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、確実にインスタントアクセスを有効化するには、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/openv/netbackup/bin/nbwmc stop
  - /usr/openv/netbackup/bin/nbwmc start

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

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. (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.57 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.56 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、または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.56 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す。

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 6-2　　リカバリオプション

オプション	説明
リストア後のデータベースのリカバリ状態 (Database recovery state after restore)	リストア後にデータベースの状態を選択します。 ■ リカバリ (Recover) リストアシーケンスの最後のイメージをリストアし、データベースを使用できるようにします。 ■ リストアしています (Restoring) 中間バックアップイメージをリストアします。データベースはロード状態のままになるため、追加のバックアップイメージをリストアして適用できます。 ■ スタンバイ (Standby) トランザクションログおよびデータベースのリストア時に、スタンバイデータベースを作成して保持します。このオプションを選択する場合は、スタンバイの取り消しログが必要です。このログは、デフォルトではプライマリデータファイルと同じディレクトリにあります。 サービスを実行するアカウントには `SQLStandBy` フォルダのフルアクセス権が必要です。

オプション	説明
一貫性チェック (Consistency check)	リストア後に実行する一貫性チェック。一貫性チェックの出力は、クライアントの進捗ログに書き込まれます。 ■ 実行しない (Do not perform) 一貫性チェックを実行しません。 ■ インデックスを含む完全チェック (Full check, including indexes) 一貫性チェックにインデックスを含めます。エラーはログに記録されます。 ■ インデックスを含まない完全チェック (Full check, excluding indexes) 一貫性チェックからインデックスをエクスクルードします。インデックスをチェックしない場合、一貫性チェックの実行速度は大幅に向上しますが、完全にはチェックされません。一貫性チェックでは、各ユーザー表のデータページおよびクラスタ化インデックスページだけが対象となります。クラスタ化されていないインデックスページの一貫性はチェックされません。 ■ カタログのチェック (Check catalog) 指定したデータベースのシステムテーブル内およびシステムテーブル間の一貫性をチェックします。 ■ 物理チェックのみ (Physical check only) オーバーヘッドの少ない データベースの物理的な一貫性をチェックします。このオプションでは、ページヘッダーおよびレコードヘッダーの物理構造の整合性のみを検証します。また、ページのオブジェクト ID やインデックス ID と割り当て構造の間の一貫性もチェックします。
VDI タイムアウト (VDI timeout)	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。

for SQL Server の用語

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

表 6-3 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。

用語	定義
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 6-4

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。	次の手順を順番に実行します。 **1** 必要な nginx サービスのバージョンをインストールします。 **2** 新しい BYO nginx 構成エントリ `/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ていることを確認します。 **3** 次のコマンドを実行します。`/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

適用対象	よく寄せられる質問	回答
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 vpfs-config.log 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てください。 **1** Yum ツールを使用して、policycoreutils と policycoreutils-python パッケージをインストールします。 **2** Nginx の SELinux に必要な次のルールを追加し、10087 ポートにバインドします。 ■ semanage port -a -t http_port_t -p tcp 10087 ■ setsebool -P httpd_can_network_connect 1 **3** 次のコマンドを実行します。/usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo
BYO	BYO のインスタントアクセスでは、デフォルトで自己署名証明書が使用され、*.pem 外部証明書のみがサポートされます。 外部 CA (*.pem 証明書) で署名された証明書で置き換えることが必要な場合は、どのようにしたら良いですか。	外部証明書を構成するには、次の手順を実行します。新しい証明書がすでに生成されている場合 (証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります) は、手順 4 に進みます。 **1** RSA の公開鍵と秘密鍵のペアを作成します。 **2** 証明書の署名要求 (CSR) を作成します。 証明書にはメディアサーバーの長いホスト名と短いホスト名が含まれている必要があります。 **3** 外部認証局が証明書を作成します。 **4** <PDDE ストレージのパス>/spws/var/keys/spws.cert を証明書に置き換え、<PDDE ストレージのパス>/spws/var/keys/spws.key を秘密鍵に置き換えます。 **5** 次のコマンドを実行して、証明書を再ロードします。 /usr/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo

適用対象	よく寄せられる質問	回答
BYO	GNOME のインスタントアクセスライブマウント共有で、メディアの自動マウントを無効にする方法を教えてください。 自動マウントが有効になっている場合、ソースフォルダは GNOME のライブマウント共有からマウントされ、小さなディスクが表示されます。このシナリオでは、インスタントアクセス機能が正しく動作しません。 マウントされたディスクコンテンツソースは、ライブマウント共有配下の `.../meta_bdev_dir/...` フォルダにあり、マウントターゲットは `/run/media/...` フォルダにあります。	次のガイドラインに従って、GNOME 自動マウントを無効にします。 https://access.redhat.com/solutions/20107

BYO	`/var/log/vpfs/vpfs-config.log` ファイルの次の問題は、どうすれば解決できますか。
	
	`**** Asking the NetBackup Webservice to trust the MSDP webserver (spws) ****`
	`/usr/openv/netbackup/bin/nblibcurlcmd failed (1):`
		次の手順を順番に実行します。
		
		1 NetBackup マスターサーバーが起動しており、ファイアウォールが NetBackup 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。
		
		2 ストレージサーバーで次のコマンドを実行して、接続状態を確認します。
		
		`/usr/openv/netbackup/bin/bpclntcmd -pn`
		
		3 NetBackup マスターサーバーを起動し、NetBackup 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/openv/pdde/vpfs/bin/vpfs_config.sh --configure_byo`

適用対象	よく寄せられる質問	回答
BYO	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、Samba 共有にのホストベースの認証を有効にしてログオンをセキュリティで保護する方法を教えてください。 次のリンク先に、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。 https://support.microsoft.com/en-us/help/4046019/guest-access-in-smb2-disabled-by-default-in-windows-10-and-windows-ser	次の手順を順番に実行します。 1 Samba 共有のエクスポート元のストレージサーバーで、1 回限りの操作として次の操作を行います。 ■ 次の Samba オプションを上書きしてゲストログインを無効にします。 `map to guest = Never` ■ Samba のユーザークレデンシャルを作成します。 ■ `smbpasswd -a spws` Samba ユーザー (spws) の Samba パスワードを設定 ■ `smbpasswd -e spws` Samba ユーザー (spws) を有効化 2 以前のクレデンシャルを使用して Samba 共有にアクセスする各 Windows クライアントのクレデンシャルマネージャで、spws クレデンシャルを保存します。
アプライアンス	MSSQL インスタントアクセスが NetBackup Appliance と Windows クライアントで機能するように、Samba 共有のホストベースの認証を有効にしてログオンをセキュリティで保護する方法を教えてください。	次の手順を順番に実行します。 1 Samba 共有のエクスポート元のストレージサーバーで 1 回限りの操作として、Samba の新しいローカルユーザーのクレデンシャルを次の Appliance CLISH パスで作成します。 Main > Settings > Security > Authentication > LocalUser 2 以前のクレデンシャルを使用して Samba 共有にアクセスする各 Windows クライアントのクレデンシャルマネージャで、新しいローカルユーザークレデンシャルを保存します。