IBM Spectrum Protect Plus
バージョン 10.1.4

インストールおよびユーザーズ・ガイド

お願い

本書および本書で紹介する製品をご使用になる前に、315 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM Spectrum Protect Plus (製品番号 5737-F11) のバージョン 10、リリース 1、モディフィケーション 4、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに 適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典：
IBM Spectrum Protect Plus
Version 10.1.4
Installation and User's Guide

発行：
日本アイ・ビー・エム株式会社

担当：
トランスレーション・サービス・センター

© Copyright International Business Machines Corporation 2017, 2019.

目次

本書について

本書は、IBM Spectrum Protect Plus の概要、プランニング、インストール、およびユーザー指示について記載しています。

本書の対象読者

本書は、サポートされている環境のいずれかにおいて、IBM Spectrum Protect Plus を使用したバックアップおよびリカバリー・ソリューションの実装を担当する管理者およびユーザーを対象にしています。

本書では、読者が IBM Spectrum Protect Plus をサポートするアプリケーションについて理解していることを前提としています (11 ページの『システム要件』を参照)。

資料

IBM Spectrum Protect 製品ファミリーには、IBM Spectrum Protect Plus、IBM Spectrum Protect for Virtual Environments、IBM Spectrum Protect for Databases、および IBM® のその他のいくつかのストレージ管理製品が含まれます。

IBM 製品資料を確認するには、IBM Knowledge Center を参照してください。

© Copyright IBM Corp. 2017, 2019

バージョン 10.1.4 の新機能

IBM Spectrum Protect Plus バージョン 10.1.4 には、新機能と更新が導入されています。

このリリースと前のバージョン 10 リリースの新機能と更新内容のリストについては、IBM Spectrum Protect Plus updates を参照してください。

この製品資料での新規情報および変更された情報は、変更箇所の左側に縦棒 (|) を付けて示しています。

© Copyright IBM Corp. 2017, 2019

製品開発への参加

設計チームや開発チームと洞察を共有することで、今後の IBM Storage 製品に影響を与えることができます。参加するには、スポンサー・ユーザー・プログラムまたはベータ・プログラムにご加入ください。

スポンサー・ユーザー・プログラム

IBM Storage スポンサー・ユーザー・プログラムでは、設計者や開発者と直接的に協力して、ご使用の製品の方向性に影響を与えることができます。

IBM では、お客様が経験や専門知識を共有されることを歓迎しています。このプログラムに参加することで、お客様とお客様のビジネスにとって重要な新しい製品機能を検討し、場合によっては実装する上で IBM を支援できます。

IBM Spectrum Protect Plus などの IBM Storage ソフトウェア製品を使用されていますか?

ビジョンを共有する準備はできていますか?

それでは、スポンサー・ユーザー・プログラムに登録して、製品イノベーションのプロセスにご参加ください。さらに、スポンサー・ユーザーは、今後のストレージ・リリースをプレビューして、ベータ・プログラムに参加し、新しい製品機能をテストすることができます。

スポンサー・ユーザー・プログラムに参加したり、追加情報を入手したりするには、以下のフォームに入力してください。

IBM Storage Sponsor User

お客様の情報の機密性は保たれ、情報は、製品開発の目的でのみ、IBM の設計チームと開発チームによって使用されます。

ベータ・プログラム

IBM Spectrum Protect Plus ベータ・プログラムを使用すると、今後予定されている製品の機能を一目で把握できます。また設計変更に影響を与える機会が提供されます。ご使用の環境で新規ソフトウェアをテストして、製品開発プロセスにお客様の声を直接届けることができます。

ベータ・プログラムは、顧客、IBM ビジネス・パートナー、および IBM の従業員など幅広い参加者を募っています。

このプログラムは以下のような利点があります。

早期コードにアクセスし、新しい製品機能や機能拡張を評価する
製品リリースの一般出荷開始日より前にベータ・コードにアクセスして、新機能と機能拡張が組織に適しているかどうかを判別できます。コードのダウンロード後、ご使用の環境で新規ソフトウェアを実行および検証できます。そして、コードが使用可能になる前に不明な点を特定して解決できるため、時間の節約につながり、後から発生する実動上の問題を防ぎます。コードが使用可能になると、それをインストールして、新機能を利用できます。

設計チームや開発チームとの対話
製品設計担当者、アーキテクト、開発者、およびテスターは、ベータ・リリースの計画を支援し、その参加者をサポートします。こういった専門家が、お客様の問題を解決できるように支援できます。

IBM リファレンス・カスタマーになる
ベータ版でお客様が有意義な体験ができた場合、IBM はお客様をリファレンス・プログラムの参加に招待します。IBM マーケティング・チームは、お客様の初期コードの適用や使用に関する成功事例を他の潜在的なベータ・テスターが把握できるメッセージを、お客様が作成する際にお手伝いをします。

© Copyright IBM Corp. 2017, 2019

連絡先と情報の登録

ベータ・プログラムの詳細は、Mary Anne Filosa (mailto:mfilosa@us.ibm.com) にご連絡ください。

IBM Spectrum Protect Plus Beta Program Signup Form に入力することで登録できます。

第 1 章 IBM Spectrum Protect Plus の概要

IBM Spectrum Protect Plus は、仮想環境とデータベース・アプリケーション向けのデータ保護および可用性のソリューションです。数分で導入して、1 時間以内にご使用の環境を保護することができます。

IBM Spectrum Protect Plus は、スタンドアロン・ソリューションとして実装するか、クラウド・ストレージまたはリポジトリー・サーバー (IBM Spectrum Protect サーバー など) に組み込んで、長期保管のためにコピーをオフロードできます。

製品のコンポーネント

IBM Spectrum Protect Plus ソリューションは、ストレージ・コンポーネントとデータ移動コンポーネントを組み込んだ、自己完結型仮想アプライアンスとして提供されています。

コンポーネント要件のサイジング : 一部の環境では、より多くのワークロードをサポートするために、これらのコンポーネントのインスタンス数を増やす必要があります。IBM Spectrum Protect Plus 環境におけるコンポーネントのサイジング、ビルド、および統合のガイダンスについては、IBM Spectrum Protect Plus Blueprints を参照してください。

IBM Spectrum Protect Plus の基本コンポーネントは次のとおりです。

IBM Spectrum Protect Plus サーバー
このコンポーネントはシステム 全体を管理します。このサーバーは、リストア・ポイント、構成、許可、カスタマイズなどのシステムの 各種側面を追跡する複数のカタログで構成されます。 通常、デプロイメントが複数のロケーションにまたがる場合であっても、1 つのデプロイメントに 1 つの IBM Spectrum Protect Plus アプライアンスがあります。

IBM Spectrum Protect Plus サーバーには、vSnap サーバーと VMware vStorage API for Data Protection (VADP) プロキシー・サーバーが搭載されています。小規模なバックアップ環境の場合、これらのサーバーで十分です。しかし、大規模な環境では、もっと多くのサーバーが必要になる場合があります。

内蔵の vSnap サーバーを使用すると、少数の仮想マシンのバックアップとリストアを行うことができ、IBM Spectrum Protect Plus 操作を評価できます。データのバックアップとリストアを行うための要件が増えるにつれて、外部 vSnap サーバーを追加して vSnap ストレージを拡張できます。外部 vSnap サーバーを環境に追加すると、IBM Spectrum Protect Plus アプライアンスの 負荷を軽減できます。

サイト
このコンポーネントは、環境内のデータ配置の管理に使用される IBM Spectrum Protect Plus ポリシー構造です。サイトは、データセンターなどの物理的なものでも、部門や組織などの論理的なものでもかまいません。IBM Spectrum Protect Plus コンポーネントは、データ・パスをローカライズし、最適化するためにサイトに割り当てられます。1 つのデプロイメントには、物理ロケーションあたり 1 つ以上のサイトが常にあります。推奨される方法では、vSnap サーバーと VADP プロキシーを一緒に 1 つのサイトに配置して、サイトへのデータ移動をローカライズします。サイトへのバックアップ・データの配置は、SLA ポリシーによって制御されます。

vSnap サーバー (vSnap server)
このコンポーネントは、データ保護または再使用のために実動システムからデータを受信するディスク・ストレージのプールです。vSnap サーバーは 1 つ以上のディスクで構成され、スケールアップ (ディスクを追加して容量を増やす) またはスケールアウト (全体的なパフォーマンスを上げるために複数の vSnap サーバーを導入する) することができます。各サイトには vSnap サーバーを 1 つ以上組み込むことができます。

vSnap プール
このコンポーネントは、vSnap サーバー・コンポーネントで使用される、ストレージ・スペースのプールにディスクを論理的に編成したものです。このコンポーネントはストレージ・プールとも呼ばれます。

© Copyright IBM Corp. 2017, 2019

VADP プロキシー (VADP proxy)
このコンポーネントは、VMware 仮想マシンを保護するために vSphere データ・ストアからデータを移動するものであり、VMware リソースの保護のみに必要です。各サイトには VADP プロキシーを 1 つ以上組み込むことができます。

ユーザー・インターフェース

IBM Spectrum Protect Plus は、構成、管理、およびモニターの各タスクのために以下のインターフェースを提供します。

IBM Spectrum Protect Plus ユーザー・インターフェース
IBM Spectrum Protect Plus ユーザー・インターフェースは、データ保護操作を構成、管理、およびモニターするための 1 次インターフェースです。

このインターフェースの 主なコンポーネントはダッシュボードであり、環境の正常性に関する要約情報を表示します。ダッシュボードについて詳しくは、3 ページの『製品ダッシュボード』を参照してください。

ユーザー・インターフェースのメニュー ・バーには、次の項目があります。

アラート・アイコン 	このアイコンをクリックすると、「**アラート**」ウィンドウが開きます。アラートの詳細については、4 ページの『アラート』を参照してください。
ヘルプ・アイコン 	このアイコンをクリックすると、オンライン・ヘルプ・システムが開きます。
ユーザー・メニュー	このメニューは、ログオンしているユーザーの名前を表示します。このメニューから、製品情報や資料、ログ、およびユーザー・サインアウト・オプションにアクセスできます。

vSnap コマンド・ライン・インターフェース
vSnap コマンド・ライン・インターフェースは、データ保護タスクを管理するための 2 次インターフェースです。このコマンド・ライン・インターフェースにアクセスするには、**vsnap** コマンドを実行します。このコマンドは、ユーザー ID `serveradmin`、または vSnap 管理特権を持つその他のオペレーティング・システム・ユーザーによって呼び出すことができます。

管理コンソール
管理コンソールは、ソフトウェア・パッチおよび更新のインストール、ならびにその他の管理タスクの実行に使用されます。管理タスクとは、セキュリティー証明書の管理、IBM Spectrum Protect Plus の開始と停止、アプリケーションのタイム・ゾーンの変更などです。

デプロイメントの例

以下の図は、2 つのアクティブなロケーションにデプロイされている IBM Spectrum Protect Plus を示しています。各ロケーションには、保護が必要なインベントリーがあります。ロケーション 1 には、1 つの vCenter サーバーと 2 つの vSphere データ・センター (および仮想マシンのインベントリー) があり、ロケーション 2 には単一のデータ・センター (および仮想マシンの小規模なインベントリー) があります。

IBM Spectrum Protect Plus サーバーは 1 つのサイトのみにデプロイされます。保護された vSphere リソースのコンテキストでデータ移動をローカライズするために、VADP プロキシーと vSnap サーバー (および対応するディスク) が各サイトにデプロイされます。

2 つのサイトの vSnap サーバー間で行われるように、双方向の複製が構成されます。

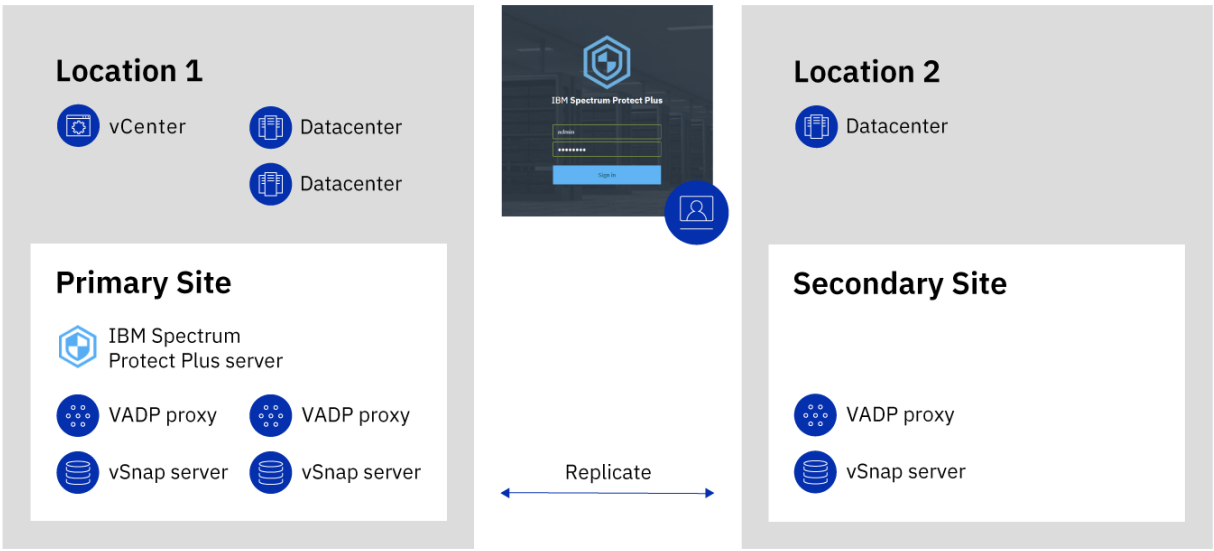


図 *1. 2* つの地理的ロケーションにおける *IBM Spectrum Protect Plus* デプロイメント

製品ダッシュボード

IBM Spectrum Protect Plus ダッシュボードには、仮想環境の正常性に関する要約が次の 3 つのセクションに表示されます。すなわち、「**ジョブと操作**」、「**宛先**」、および「**範囲**」です。

ジョブと操作

「**ジョブと操作**」セクションには、選択した期間のジョブ・アクティビティーの 要約が表示されます。期間をドロップダウン・リストから選択します。このセクションには、以下の情報が表示されます。

現在実行中

「**現在実行中**」セクションには、実行中のジョブの総数、および IBM Spectrum Protect Plus 仮想アプライアンスにおける中央演算処理装置 (CPU) 使用量のパーセンテージが表示されます。このパーセンテージは、10 秒ごとに最新表示されます。

ジョブの実行に関する詳しい情報を表示するには、「**表示**」をクリックします。

ヒストリー

「**ヒストリー**」セクションには、選択した期間内に完了したジョブの総数が表示されます。この数には、実行中のジョブは含まれません。

このセクションには、選択した期間にわたるジョブの成功率も表示されます。成功率は、以下の式を使用して計算されます。

100 x 成功したジョブ数 / ジョブの総数 = 成功率

完了したジョブは、以下のジョブ状況で表示されます。

成功
警告もクリティカル・エラーもなく完了したジョブの数。

失敗
クリティカル・エラーを出して失敗したか、完了できなかったジョブの数。

警告
部分的に完了したか、スキップされたか、またはその他の状況で警告が表示されたジョブの数。

ジョブのヒストリーに関する詳しい情報を表示するには、「**表示**」をクリックします。

宛先

「**宛先**」セクションには、バックアップ操作に使用されるデバイスの要約が表示されます。このセクションには、以下の情報が表示されます。

容量の要約
「**容量の要約**」セクションには、IBM Spectrum Protect Plus から使用できる vSnap サーバーの現在の使用状況や可用性が表示されます。

vSnap サーバーに関する情報を表示するには、「**表示**」をクリックします。

デバイス状況
「**デバイス状況**」セクションには、使用可能なデバイスの総数が表示されます。

オフラインであるか、またはその他の理由で使用できないデバイスの数は、「**非アクティブ**」フィールドに表示されます。

フル稼働しているデバイスの数は、「**フル**」フィールドに表示されます。

データの分解
「**データの分解**」セクションには、データ重複排除率とデータ圧縮率が表示されます。

データ重複排除率は、重複が除去された後でデータの保管に必要な物理スペースと比較した、保護されたデータの量です。この比率は、圧縮率に加えて実現された追加のスペース節約を表します。重複排除が無効になっている場合、この比率は 1 です。

範囲

「**範囲**」セクションには、IBM Spectrum Protect Plus によってインベントリーに入れられたリソースと、それらのリソースに割り当てられている SLA ポリシーの要約が表示されます。このセクションには、以下の情報が表示されます。

ソース保護
「**ソース保護**」セクションには、IBM Spectrum Protect Plus カタログのインベントリーに入れられた、仮想マシンやアプリケーション・サーバーなどのソース・リソースの総数が表示されます。保護されているリソースと保護されていないリソースの数が表示されます。

このセクションには、リソースの総数に対する、IBM Spectrum Protect Plus で保護されているリソースの比率 (パーセント表示) も表示されます。

ポリシー
「**ポリシー**」セクションには、SLA ポリシーの総数と、関連した保護ジョブが表示されます。

このセクションには、最も大きいカウント数が割り当てられているリソースがある 3 つの SLA ポリシーも表示されます。

すべての SLA ポリシーに関する詳しい情報を表示するには、「**表示**」をクリックします。

アラート

「**アラート**」メニューには、IBM Spectrum Protect Plus 環境における現在および最近の警告とエラーが表示されます。アラート数は赤い円に入れて表示され、アラートを表示できることを示します。

アラート・リストを表示するには、「**アラート**」メニューをクリックします。リスト内の各項目には、状況アイコン、アラートの要約、関連した警告またはエラーが発生した時間、および関連したログを表示するリンクが含まれます。

アラート・リストには、以下のアラート・タイプがあります。

アラート・タイプ

ジョブ失敗
ジョブが失敗したときに表示されます。

ジョブの部分的成功
ジョブが部分的に成功したときに表示されます。

システム・ディスク・スペース不足
空きディスク・スペース量が 10% 以下になったときに表示されます。

vSnap ストレージ・スペース不足
空きディスク・スペース量が 10% 以下になったときに表示されます。

システム・メモリー不足
メモリー使用量が 95% を超えたときに表示されます。

システム CPU 使用率が高い
プロセッサー使用率が 95% を超えたときに表示されます。

ハイパーバイザー VM が見つからない
VM が検出されないときに表示されます。

複製ストレージ・スナップショットのロック状態例外
複製ストレージ・スナップショットがロックされているときに表示されます。複製の保存設定を増やすか、ポリシーの複製頻度を増やしてください。

オフロード・ストレージ・スナップショットのロック状態例外
最新のオフロード・ストレージ・スナップショットがロックされているときに表示されます。オフロードの保存設定を増やすか、ポリシーのオフロード頻度を増やしてください。

SQL ログ・バックアップ失敗
データベースのログ・バックアップが失敗したときに表示されます。

SQL ログ SMO バックアップ障害
サーバー管理オブジェクトのトランザクション・ログ・バックアップ障害が発生した場合に表示されます。

SQL ログ・サイズが大きすぎる
トランザクション・ログ・サイズがディスク上の使用可能スペースよりも大きい場合に表示されます。

SQL ログの残りスペースが少ない
トランザクション・ログ・バックアップのステージング・ディレクトリーのディスク・スペースが少なくなったときに表示されるアラートで、残りのスペース容量を表示します。

役割ベースのアクセス制御

役割ベースのアクセス制御は、IBM Spectrum Protect Plus ユーザー・アカウントから使用できるリソースと許可を定義します。

役割ベースのアクセスは、必要な機能やリソースのみにユーザーがアクセスできるようにします。例えば、役割により、ユーザーはハイパーバイザー・リソースのバックアップ・ジョブとリストア・ジョブを実行できますが、ユーザー・アカウントの作成や変更などの管理タスクは実行できません。

この資料で説明しているタスクを実行するには、ユーザーは、必要な許可がある役割に属する必要があります。タスクを開始する前に、ご使用のユーザー・アカウントが、必要な許可がある役割に属していることを確認してください。

ユーザー・アクセスのセットアップと管理を行うには、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。

バックアップ・ストレージ・データの複製

バックアップ・データの複製を有効にすると、vSnap サーバーからのデータが、別の vSnap サーバーに非同期で複製されます。例えば、1 次サイト上の vSnap サーバーから、2 次サイト上の vSnap サーバーにバックアップ・データを複製できます。

バックアップ・ストレージ・データの複製の有効化

バックアップ・ストレージ・データの複製を有効にするには、以下のアクションを実行します。

1. vSnap サーバー間の複製パートナーシップを確立します。複製パートナーシップは、登録された vSnap サーバーの「管理」ペインで確立されます。「**ストレージ・パートナーの構成**」セクションで、別の登録済み vSnap サーバーを、複製操作のターゲットの役目をするストレージ・パートナーとして選択します。

   パートナー・サーバー上のプールが、1 次サーバーのプールからの複製データを十分に保持できる大きさであることを確認してください。

2. バックアップ・ストレージ・データの複製を有効にします。複製機能は、SLA ポリシーとも呼ばれるバックアップ・ポリシーを使用して有効になります。これらのポリシーは、バックアップ操作の頻度やバックアップの保存ポリシーを始めとする、バックアップ・ジョブに適用されるパラメーターを定義します。SLA ポリシーについて詳しくは、89 ページの『第 6 章 バックアップ操作用の SLA ポリシーの管理』を参照してください。

   バックアップ・ストレージ複製オプションは、SLA ポリシーの「**操作の保護**」 > 「**複製ポリシー**」セクションで定義できます。オプションには、複製の頻度、ターゲット・サイト、複製の保存があります。

バックアップ・ストレージ・データの複製の有効化に関する考慮事項

バックアップ・ストレージ・データの複製の有効化に関する考慮事項を検討してください。

- ご使用の環境で、暗号化された vSnap サーバーと暗号化されていない vSnap サーバーが混在している場合、「**暗号化ディスク・ストレージのみを使用します**」を選択して、暗号化された vSnap サーバーにデータを複製します。 このオプションが選択されているときに、暗号化された vSnap サーバーが使用可能でない場合、関連したジョブは失敗します。
- 単一のバックアップ・データの集合が複数の vSnap サーバーに複製される 1 対多の複製シナリオを作成するには、複製サイトごとに複数の SLA ポリシーを作成します。

2 次バックアップ・ストレージへのオフロード

vSnap サーバーは、スナップショットの 1 次バックアップ・ロケーションです。すべての IBM Spectrum Protect Plus 環境に少なくとも 1 つの vSnap サーバーがあります。オプションで、スナップショットを vSnap サーバーから 2 次バックアップ・ストレージにオフロードできます。

以下の 2 次バックアップ・ストレージ・ターゲットが、オフロード操作に使用できます。

- IBM Cloud™ オブジェクト・ストレージ(IBM Cloud オブジェクト・ストレージ・システムを含む)
- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure
- リポジトリー・サーバー (現行リリースの IBM Spectrum Protect Plus の場合、リポジトリー・サーバーは IBM Spectrum Protect サーバーでなければなりません)

これらのターゲットは、以下のストレージ・タイプをサポートします。使用するストレージ・タイプは、リカバリー時間やセキュリティー目標などの要因によって異なります。

オブジェクト・ストレージ

オブジェクト・ストレージは、ファイル階層を使用しないが、すべてのオブジェクトを同じレベルに保管するストレージ・プールまたはリポジトリーにデータが個別ユニットまたはオブジェクトとして保管される、データの保管方式です。

オブジェクト・ストレージは、データを IBM Spectrum Protect サーバー またはクラウド・ストレージ・システムにオフロードする 場合のオプションです。スナップショット・データがオブジェクト・ストレージにオフロードされると、最初のオフロード操作中にフルコピーが作成されます。 後続のコピーは増分コピーで、前回のオフロード以降の累積変更をキャプチャーします。

バックアップおよびリカバリーの時間を比較的高速にするが、磁気テープまたはクラウド・アーカイブ・ストレージによって可能になる長期的な保護、コスト、およびセキュリティー上のメリットは必要でない場合は、スナップショットをオブジェクト ・ストレージにオフロードすると便利です。

磁気テープまたはクラウド・アーカイブ・ストレージ

磁気テープ・ストレージとは、データが物理磁気テープ・メディアまたは仮想テープ・ライブラリーに保管されることを意味します。磁気テープ・ストレージは、データを IBM Spectrum Protect サーバー

にオフロードするときのオプションです。インターネットに接続されていない安全なオフサイト・ロケーションにテープ・ボリュームを保管することにより、マルウェアやハッカーなどのオンライン脅威からデータを保護する上で役立ちます。

クラウド・アーカイブ・ストレージは、Amazon Glacier、IBM Cloud Object Storage Archive Tier、または Microsoft Azure Archive のいずれかのストレージ・サービスにデータをコピーする長期保管方式です。

データを磁気テープまたはクラウド・ストレージ・システムにオフロードすると、データのフルコピーが作成されます。

スナップショットを磁気テープまたはクラウド・アーカイブ・ストレージにオフロードすると、追加のコストとセキュリティー上のメリットが得られます。 ただし、これらのストレージ・タイプへのオフロードには完全なデータ・コピーが必要であるため、データのコピーに必要な時間が長くなります。さらに、リカバリー時間が予測不能になり、データが使用可能になる前に処理に時間がかかる場合があります。

各クラウド・ストレージ・システムのオブジェクト ・ストレージおよびアーカイブ・ストレージにスナップショット・データをコピーする方法については、19 ページの『クラウド要件』を参照してください。

2 次バックアップ・ストレージの追加とバックアップ・ポリシーの作成

データを 2 次ストレージにオフロードするには、以下のアクションが必要です。

アクション	方法
リポジトリー・サーバーにデータをオフロードします • IBM Spectrum Protect サーバー環境のオブジェクト・クライアントとして IBM Spectrum Protect Plus をセットアップします。 • ストレージを IBM Spectrum Protect Plus に追加します。	258 ページの『オフロード・ターゲットとしての IBM Spectrum Protect サーバー の構成』および 263 ページの『バックアップ・ストレージ・プロバイダーとしてのリポジトリー・サーバーの追加』を参照してください。
クラウド・ストレージにデータをオフロードするために、ストレージを IBM Spectrum Protect Plus に追加します	選択したストレージ・タイプの指示に従います。 • 253 ページの『バックアップ・ストレージ・プロバイダーとしての Amazon S3 クラウド・ストレージの追加』 • 254 ページの『バックアップ・ストレージ・プロバイダーとしての IBM Cloud Object Storage の追加』 • 256 ページの『バックアップ・ストレージ・プロバイダーとしての Microsoft Azure クラウド・ストレージの追加』 • 263 ページの『バックアップ・ストレージ・プロバイダーとしてのリポジトリー・サーバーの追加』
ストレージを含むバックアップ・ポリシーを作成します。	73 ページの『バックアップ・ポリシーの作成』を参照してください。

デプロイメント例

以下の図は、2 つのアクティブなロケーションにデプロイされている IBM Spectrum Protect Plus を示しています。各ロケーションには、保護が必要なインベントリーがあります。ロケーション 1 には、1 つの vCenter サーバーと 2 つの vSphere データ・センター (および仮想マシンのインベントリー) があり、ロケーション 2 には単一のデータ・センター (および仮想マシンの小規模なインベントリー) があります。

IBM Spectrum Protect Plus サーバーは 1 つのサイトのみにデプロイされます。保護された vSphere リソースのコンテキストでデータ移動をローカライズするために、VADP プロキシーと vSnap サーバー (および対応するディスク) が各サイトにデプロイされます。

2 つのサイトの vSnap サーバー間で行われるように、双方向の複製が構成されます。

スナップショットは、長期のデータ保護のために、2 次サイトの vSnap サーバーからクラウド・ストレージにオフロードされます。

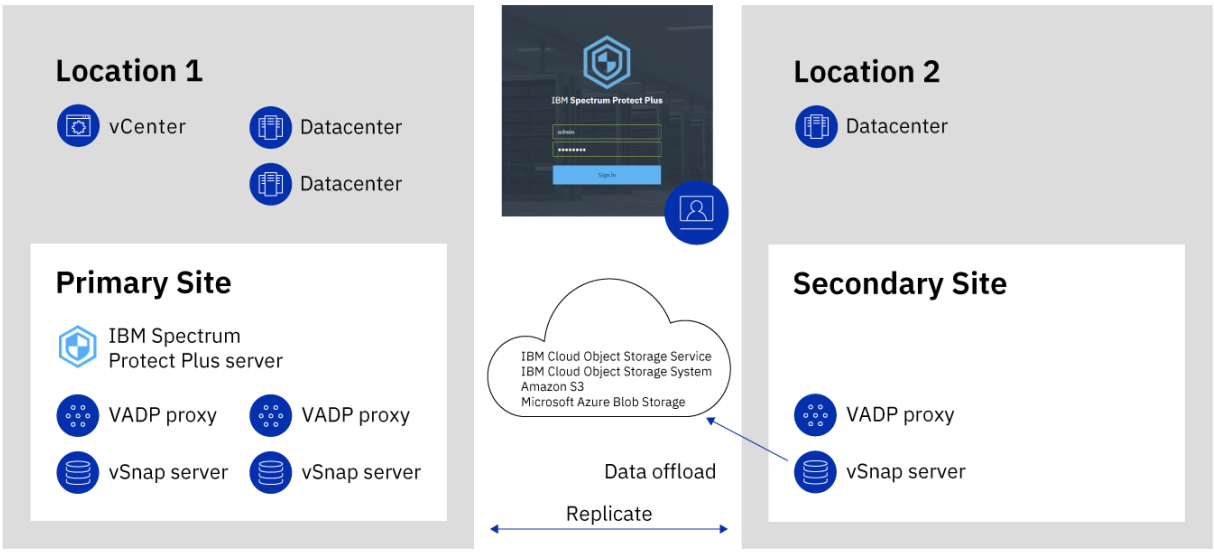


図 *2.* クラウド・ストレージにオフロードする、*2* つの地理的ロケーションにおける *IBM Spectrum Protect Plus* デプロイメント

以下の図は、上記の図と同じデプロイメントを示しています。

ただし、このデプロイメントでは、スナップショットは、長期のデータ保護のために、2 次サイトの vSnap サーバーから IBM Spectrum Protect にオフロードされます。

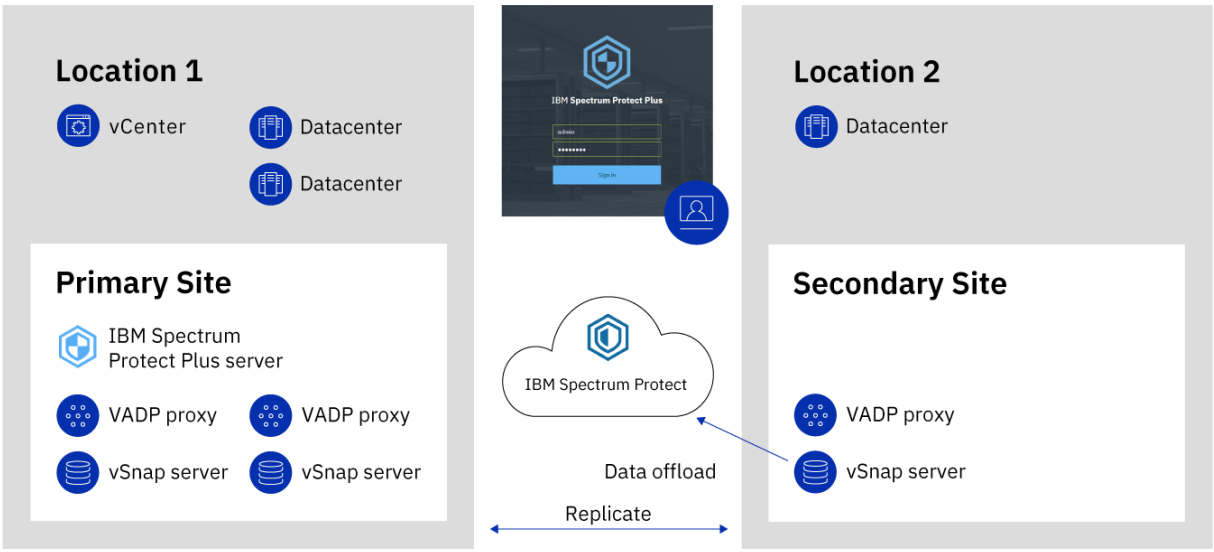


図 *3. IBM Spectrum Protect* にオフロードする、*2* つの地理的ロケーションにおける *IBM Spectrum Protect Plus* デプロイメント

IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus は、IBM Cloud for VMware Solutions サービスである IBM Spectrum Protect Plus on IBM Cloud として使用できます。

IBM Cloud for VMware Solutions を使用すると、スケーラブルな IBM Cloud インフラストラクチャーと VMware ハイブリッド仮想化テクノロジーを使用して、オンプレミスの VMware ワークロードを IBM Cloud に統合またはマイグレーションすることができます。

IBM Cloud for VMware Solutions には、以下のような大きなメリットがあります。

グローバルな展開
ハイブリッド・クラウドのフットプリントを、世界中に設置されているエンタープライズ・クラスの IBM Cloud データ・センターに最大 30 拠点まで展開できます。

合理化された統合
合理化されたプロセスを使用して、ハイブリッド・クラウドを IBM Cloud インフラストラクチャーに統合します。

自動デプロイメントと構成
VMware 環境の自動デプロイメントと構成を使用して、エンタープライズ・クラスの VMware 環境をオンデマンドの IBM Cloud ベアメタル・サーバーおよび仮想サーバーと一緒にデプロイします。

単純化
基礎の物理計算、ストレージ、ネットワーク・インフラストラクチャーやソフトウェア・ライセンスを特定、調達、デプロイ、および管理することなく、VMware クラウド・プラットフォームを使用します。

拡張と縮小の柔軟性
ビジネス要件に応じて、VMware ワークロードの拡張と縮小を行います。

単一の管理コンソール
IBM Cloud 上の VMware 環境を単一のコンソールを使用してデプロイ、アクセス、管理できます。

IBM Spectrum Protect Plus on IBM Cloud で使用可能な機能

IBM Spectrum Protect Plus は、VMware と Microsoft の両方の Hyper-V 環境をサポートします。

ただし、IBM Spectrum Protect Plus on IBM Cloud は VMware 環境のみをサポートします。

この資料には、Hyper-V に固有の機能に関するトピックを記載しています。IBM Spectrum Protect Plus on IBM Cloud を使用している場合、これらの機能は使用できません。

IBM Spectrum Protect Plus と IBM Spectrum Protect Plus on IBM Cloud の現行バージョンが同じでない場合があります。使用しているバージョンの IBM Spectrum Protect Plus on IBM Cloud 資料を見つけるには、オンライン製品資料 にアクセスして、該当の製品バージョンを選択してください。

詳細情報

IBM Spectrum Protect Plus on IBM Cloud の注文、インストール、および構成の方法については、以下の資料を参照してください。資料にアクセスするには、IBMid が必要です。

- Getting started with IBM Cloud for VMware Solutions
- Components and considerations for IBM Spectrum Protect Plus on IBM Cloud
- Managing IBM Spectrum Protect Plus on IBM Cloud

AWS クラウド・プラットフォーム上の IBM Spectrum Protect Plus

Amazon Web Services (AWS) クラウド・プラットフォーム上の IBM Spectrum Protect Plus は、オンプレミスで IBM Spectrum Protect Plus を実行するが、AWS クラウドで実行中のデータベースは保護したいユーザーのためのソリューションです。

IBM Spectrum Protect Plus on AWS は、IBM Spectrum Protect Plus サーバーがオンプレミスで、vSnap サーバーが AWS 上にあるハイブリッド・ソリューションです。

IBM Spectrum Protect Plus のポリシー、システム管理、アクセス制御、およびその他の機能は、オンプレミス IBM Spectrum Protect Plus サーバーによって管理および保守されます。AWS 上にあるデータベースからのデータは、これも AWS 上にある vSnap サーバーに保管されます。

AWS への IBM Spectrum Protect Plus のデプロイ

AWS Marketplace の IBM Spectrum Protect Plus ページは、vSnap サーバーを AWS にデプロイするために必要な AWS CloudFormation テンプレートのほか、価格設定、使用法、およびサポート情報を提供します。このページおよび IBM Spectrum Protect Plus on the AWS Cloud Deployment Guide に記載されている手順に従って、オンプレミス環境および AWS 環境をセットアップしてください。

IBM Spectrum Protect Plus on AWS デプロイメントには、IBM Spectrum Protect Plus バージョン 10.1.3 が含まれています。現行バージョンの IBM Spectrum Protect Plus を使用する場合は、83 ページの『第 5 章 IBM Spectrum Protect Plus コンポーネントの更新』の説明に従って、アップグレードを完了してください。

第 2 章 IBM Spectrum Protect Plus のインストール

IBM Spectrum Protect Plus をインストールする前に、システム要件とインストール手順を確認してください。

製品デプロイメントのロードマップ

ロードマップに従って、IBM Spectrum Protect Plus をインストールし、構成し、使用を開始します。

アクション	方法
ご使用のシステム環境がハードウェア要件およびソフトウェア要件を満たしていることを確認します。	11 ページの『システム要件』を参照してください。
IBM Spectrum Protect Plus 環境におけるコンポーネントのサイジング、ビルド、および配置の方法を決定します。	IBM Spectrum Protect Plus Blueprints を参照してください。
IBM Spectrum Protect Plus をインストールします。	11 ページの『第 2 章 IBM Spectrum Protect Plus のインストール』を参照してください。
ご使用の環境をサポートするために追加の vSnap サーバーが必要な場合は、それらのサーバーをインストールし、構成します。	53 ページの『第 3 章 vSnap サーバーのインストールおよび構成』を参照してください。
ご使用の環境をサポートするために追加の VMware vStorage API for Data Protection (VADP) プロキシーが必要な場合は、それらのプロキシーを作成し、構成します。	107 ページの『VADP バックアップ・プロキシーの管理』を参照してください。
IBM Spectrum Protect Plus をセットアップして使用を開始する基本的な手順を実行します。	69 ページの『第 4 章 まずはクイック・スタートから』を参照してください。

システム要件

IBM Spectrum Protect Plus をインストールする前に、ストレージ環境にインストールする予定の製品やその他のコンポーネントのハードウェア要件とソフトウェア要件を検討してください。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

IBM Spectrum Protect Plus 環境の仕様にリストされているコンポーネントのサイジング、ビルド、および配置の方法を確認するには、IBM Spectrum Protect Plus Blueprints を参照してください。

コンポーネントの要件

IBM Spectrum Protect Plus をデプロイし、実行するために必要なシステム構成とサポートされるブラウザーを用意していることを確認してください。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

IBM Spectrum Protect Plus におけるサード・パーティー製のプラットフォーム、アプリケーション、サービス、およびハードウェアに対するサポートは、サード・パーティー・ベンダーに匹敵します。サード・パーティー・ベンダーの製品またはバージョンが拡張サポート、セルフサービス・サポート、または生産終了を開始すると、IBM Spectrum Protect Plus は同じレベルで対応します。

© Copyright IBM Corp. 2017, 2019

仮想マシンのインストール

IBM Spectrum Protect Plus は仮想アプライアンスとしてインストールされます。 IBM Spectrum Protect Plus をホストにデプロイする前に、以下の要件が満たされていることを確認してください。

- vSphere 5.5、6.0、6.5、または 6.7
- Microsoft Hyper-V Server 2016、または Hyper-V 2019

初期のデプロイメントの場合、以下の最小要件を満たすように仮想アプライアンスを 構成します。

- 64 ビット 8 コア・マシン
- 48 GB のメモリー
- 仮想マシン用の 536 GB のディスク・ストレージ

IBM Spectrum Protect Plus 仮想アプライアンス、ストレージ・アレイ、ハイパーバイザー、アプリケーション・サーバーなどの、ご使用の環境にある IBM Spectrum Protect Plus リソース全体でタイム・ゾーンを同期するには、Network Time Protocol (NTP) サーバーを使用します。各種システムのクロックの同期が大幅にずれている場合、アプリケーション登録、メタデータのカタログ作成、インベントリー、バックアップ、リストア、またはファイル・リストアのジョブ時にエラーが検出される可能性があります。タイマーのドリフトの特定と解決について詳しくは、VMware Knowledge Base の記事 Time in virtual machine drifts due to hardware timer drift を参照してください。

ブラウザー・サポート

インストールされた仮想アプライアンスにアクセスできるコンピューターから、IBM Spectrum Protect Plus を実行します。IBM Spectrum Protect Plus は、以下の Web ブラウザーに対してテスト済みです。これ以降のバージョンのブラウザーもサポートされます。

- Firefox 55.0.3
- Google Chrome 60.0.3112 以降
- Microsoft Edge 40.15063/Microsoft EdgeHTML 15.15063 以降

画面解像度が 1024 x 768 ピクセル未満である場合、一部の項目がウィンドウに収まらない可能性があります。 ヘルプ・システムや一部の IBM Spectrum Protect Plus 操作にアクセスするには、ブラウザーでポップアップ・ウィンドウが使用可能でなければなりません。

IBM Spectrum Protect の要件

クラウド・オフロード操作用のリポジトリー・サーバーとして IBM Spectrum Protect を使用する予定の場合は、IBM Spectrum Protect V8.1.8 を使用する必要があります。

IBM Spectrum Protect Plus のポート

IBM Spectrum Protect Plus および関連サービスでは、以下のポートを使用します。「ファイアウォール規則」列の「受け入れ」で示されるポートは、セキュア接続 (HTTPS または SSL) を使用します。

表 *1.* 着信ファイアウォール接続 *(IBM Spectrum Protect Plus* アプライアンス*)*

ポート	プロトコル	ファイアウォール	サービス	説明
22	TCP	Accept	OpenSSH 5.3 (プロトコル 2.0)	IBM Spectrum Protect Plus のトラブルシューティングに使用されます。
443	TCP	Accept	リバース・プロキシーを実行するマイクロサービス	クライアント接続 (SSL) のメインエントリー・ポイント

表 1. 着信ファイアウォール接続 (IBM Spectrum Protect Plus アプライアンス) (続き)				
ポート	**プロトコル**	**ファイアウォール**	**サービス**	**説明**
5671	TCP、AMQP	Accept	RabbitMQ	VADP プロキシーおよび VMware ジョブ管理ワーカーによって作成およびコンシュームされるメッセージの管理に使用されるメッセージ・フレームワーク。また、ジョブ・ログの管理を容易にします。
8090	TCP	Accept	Administrative Console Framework (ACF)	システム管理機能の拡張可能なフレームワーク。システム更新やカタログのバックアップ操作またはリストア操作などの操作を実行するプラグインをサポートします。
8761	TCP	Accept	Discovery Server	自動的に VADP プロキシーを検出し、IBM Spectrum Protect Plus VM バックアップ操作で使用されます。

表 2. 着信ファイアウォール接続 (内蔵 vSnap サーバー)				
ポート	**プロトコル**	**ファイアウォール**	**サービス**	**説明**
111	TCP	Accept	RPC Port Bind	Open Network Computing (ONC) クライアントが ONC サーバー (内部) との通信に必要としたポートをクライアントが検出できるようにします。
2049	TCP	Accept	NFS	vSnap (内部) との間での NFS データ転送に使用されます。
3260	TCP	Accept	iSCSI	vSnap (内部) との間での iSCSI データ転送に使用されます。

表 2. 着信ファイアウォール接続 (内蔵 vSnap サーバー) (続き)				
ポート	**プロトコル**	**ファイアウォール**	**サービス**	**説明**
20048	TCP	Accept	NFS	vSnap (内部) との間での NFS データ転送に使用されます。

表 3. 発信ファイアウォール接続 (IBM Spectrum Protect Plus アプライアンス)			
ポート	**プロトコル**	**サービス**	**説明**
22	TCP	OpenSSH 5.3 (プロトコル 2.0)	ゲスト・アプリケーション・コンポーネントを実行するリモート・サーバーとの SSH 通信に使用されます。
25	TCP	SMTP	E メール・サービス。
389	TCP	LDAP	活動ディレクトリー・サービス。
443	TCP	VMware ESXi ホスト	操作を管理するための ESXi ホスト・ポート。
443	TCP	VMware vCenter	vCenter とのクライアント接続。
636	TCP	LDAP	活動ディレクトリー・サービス (SSL)。
902	TCP	VMware NFC サービス	Network File Copy (NFC) は、vSphere コンポーネントに対するファイル・タイプ認識 FTP サービスを提供します。デフォルトでは、ESXi はデータ・ストア間のデータのコピーや移動などの操作に NFC を使用します。
5985	TCP	Windows リモート管理 (WinRM)	Hyper-V およびゲスト・アプリケーション・クライアント接続。
8098	TCP	VADP プロキシー (VADP proxy)	仮想マシン・データ保護プロキシー。
8900	TCP	vSnap	データ保護操作のターゲットとして使用される、OVA/Installer バージョンのインテリジェント・ストレージ・フレームワーク。

vSnap サーバーの要件

vSnap サーバーは、IBM Spectrum Protect Plus の 1 次バックアップの宛先です。VMware 環境または Hyper-V 環境のどちらかで、IBM Spectrum Protect Plus 仮想アプライアンスが最初にデプロイされる時点

で、名前が `localhost` という 1 つの vSnap サーバーが自動的にインストールされます。大規模なバックアップ・エンタープライズ環境では、追加の vSnap サーバーが必要になる場合があります。

効率的な重複排除のためにバックアップ容量に基づいてメモリーを割り振ります。サイジングのガイダンスについて詳しくは、 IBM Spectrum Protect Plus Blueprints を参照してください。

初期のデプロイメントの場合、仮想マシンまたは物理的な Linux マシンが以下の最小要件を満たしていることを確認してください。

- 64 ビット 8 コア・プロセッサー
- 32 GB のメモリー
- ルート・ファイル・システム上の 16 GB のフリー・スペース
- `/opt/vsnap-data` にマウントされている別個のファイル・システム上の 128 GB のフリー・スペース

Linux ネットワーク管理サービスをインストールして実行する必要があります。

オプションとして、ソリッド・ステート・ドライブ (SSD) により、バックアップとリストアのパフォーマンスが向上します。

- バックアップのパフォーマンスを向上させるために、SSD によってサポートされる 1 つ以上のログ装置を使用するようにプールを構成します。冗長性を向上させるためのミラー・ログを作成するために、2 つ以上のログ装置を指定してください。
- リストアのパフォーマンスを向上させるために、SSD によってサポートされるキャッシュ装置を使用するようにプールを構成します。

vSnap サーバー仮想マシンのインストール要件

vSnap サーバーをホストにデプロイする前に、以下の要件が満たされていることを確認してください。

- vSphere 5.5、6.0、6.5、または 6.7
- Microsoft Hyper-V 2016 または Microsoft Hyper-V 2019

vSnap サーバーの物理インストール要件

V10.1.3 以降の IBM Spectrum Protect Plus が提供する機能には、RHEL 7.5 および CentOS 7.5 でサポートされるカーネル・レベルが必要です。 RHEL 7.5 および CentOS 7.5 より前のオペレーティング・システムを使用する必要がある場合は、物理 vSnap V10.1.2 のインストールに IBM Spectrum Protect Plus V10.1.2 を使用してください。

IBM Spectrum Protect Plus V10.1.4 以降の物理 vSnap サーバーのインストールでは、以下の Linux オペレーティング・システムがサポートされます。

- CentOS 7.1804 (7.5) (x86_64)
- CentOS 7.1810 (7.6) (x86_64)
- RedHat Enterprise Linux 7.5 (x86_64)
- Red Hat Enterprise Linux 7.6 (x86_64)

以下のオペレーティング・システムを使用する場合は、物理 vSnap サーバー V10.1.2 のインストールに IBM Spectrum Protect Plus V10.1.2 を使用してください。

- CentOS Linux7.3.1611 (x86_64)
- CentOS Linux7.4.1708 (x86_64)
- Red Hat Enterprise Linux 7.3 (x86_64)
- Red Hat Enterprise Linux 7.4 (x86_64)

vSnap サーバーのポート

vSnap サーバーは、以下のポートを使用します。「ファイアウォール規則」列の「受け入れ」で示されるポートは、セキュア接続 (HTTPS/SSL) を使用します。

表 *4.* 着信 *vSnap* ファイアウォール接続

ポート	プロトコル	ファイアウォール	サービス	説明
22	TCP	Accept	SSH	vSnap サーバーのトラブルシューティングに使用されます。
111	TCP	Accept	RPC Port Bind	Open Network Connectivity (ONC) クライアントが ONC サーバー (内部) との通信に必要とするポートをクライアントが検出できるようにします。
137	UDP	Accept	SMB/CIFS	vSnap サーバー (内部) との間での SMB または CIFS データ転送に使用されます。
138	UDP	Accept	SMB/CIFS	vSnap サーバー (内部) との間での SMB または CIFS データ転送に使用されます。
139	TCP	Accept	SMB/CIFS	vSnap サーバー (内部) との間での SMB または CIFS データ転送に使用されます。
445	TCP	Accept	SMB/CIFS	vSnap サーバー (内部) との間での SMB または CIFS データ転送に使用されます。
2049	TCP	Accept	NFS	vSnap (内部) サーバーとの間での NFS データ転送に使用されます。
3260	TCP	Accept	iSCSI	vSnap (内部) サーバーとの間での iSCSI データ転送に使用されます。
8900	TCP	Accept	HTTPS	vSnap サーバー REST API

表 4. 着信 *vSnap* ファイアウォール接続 (続き)				
ポート	**プロトコル**	**ファイアウォール**	**サービス**	**説明**
20048	TCP	Accept	NFS	vSnap (内部) サーバーとの間での NFS データ転送に使用されます。

VADP プロキシー要件

IBM Spectrum Protect Plus では、VADP を使用した仮想マシン・バックアップ・ジョブの実行は、システム・リソースに重い負担がかかります。VADP バックアップ・ジョブ・プロキシーの作成によって、IBM Spectrum Protect Plus バックアップ・ジョブに対してロード・シェアリングとロード・バランシングを有効にします。プロキシーが存在する場合、処理中の負荷全体が IBM Spectrum Protect Plus アプライアンスからプロキシーにシフトされます。

この機能は、SUSE Linux Enterprise Server 環境と Red Hat 環境についてのみテスト済みです。また、最小カーネル 2.6.32 の 64 ビット・クワッド・コア以上の構成でのみサポートされます。

VADP プロキシーは、VMware トランスポート・モード File、SAN、HotAdd、NBDSSL、および NBD をサポートします。VMware トランスポート・モードについて詳しくは、Virtual Disk Transport Methods を参照してください。

この機能は、以下の Linux 環境で 64 ビット・クワッド・コア以上の構成でのみサポートされます。

- CentOS Linux 6.5 以降の保守レベルおよびモディフィケーション・レベル (10.1.1 パッチ 1 以降)
- CentOS Linux 7.0 以降の保守レベルおよびモディフィケーション・レベル (10.1.1 パッチ 1 以降)
- Red Hat Enterprise Linux 6、フィックスパック 4 以降の保守レベルおよびモディフィケーション・レベル
- Red Hat Enterprise Linux 7 以降の保守レベルおよびモディフィケーション・レベル
- SUSE Linux Enterprise Server 12 以降の保守レベルおよびモディフィケーション・レベル

サイジングのガイダンスについて詳しくは、IBM Spectrum® Protect Plus Blueprints を参照してください。

VADP プロキシー・サーバーの初期のデプロイメントの場合、Linux マシンが以下の最小要件を満たしていることを確認してください。

- 64 ビット・クワッド・コア・プロセッサー
- 8 GB RAM が必須、推奨 16 GB
- 60 GB の空きディスク・スペース

VADP プロキシー・サーバー上の使用済み CPU の増加や並行性の向上には、プロキシー・サーバーに割り振られているメモリーを適宜に増やす必要があります。

プロキシーは NFS ファイル・システムをマウントできなければなりませんが、多くの場合、これには NFS クライアント・パッケージのインストールが必要です。正確なパッケージの詳細は、ディストリビューションによって異なります。

各プロキシーには完全修飾ドメイン名が必要であり、解決して vCenter に接続できなければなりません。vSnap サーバーがプロキシーから接続可能でなければなりません。VADP プロキシー・サーバー上のポート 8098 は、プロキシー・サーバーのファイアウォールが使用可能であるときに開いていなければなりません。

VADP プロキシー・ポート

VADP プロキシーは、以下のポートを使用します。「ファイアウォール規則」列の「受け入れ」で示されるポートは、セキュア接続 (HTTPS または SSL) を使用します。

表 5. 着信 *VADP* プロキシー・ファイアウォール接続

ポート	プロトコル	ファイアウォール	サービス	説明
22	TCP	Accept	SSH	VADP プロキシーをホスト・ノードにプッシュするのに、ポート 22 が使用されます。
8098	TCP	Accept	VADP	IBM Spectrum Protect Plus サーバーと VADP プロキシー間の TLS ベースの REST API 通信用のデフォルト・ポート。

表 6. 発信 *VADP* プロキシー・ファイアウォール接続

ポート	プロトコル	サービス	説明
111	TCP	vSnap RPC Port Bind	ONC クライアントが ONC サーバー (内部) との通信に必要とするポートをクライアントが検出できるようにします。
443	TCP	VMware ESXi ホスト/ vCenter	vCenter とのクライアント接続。
902	TCP	VMware ESXi ホスト	Network File Copy (NFC) は、vSphere コンポーネントに対するファイル・タイプ認識 FTP サービスを提供します。ESXi は、デフォルトでデータ・ストア間のデータのコピーや移動などの操作に NFC を使用します。
2049	TCP	vSnap NFS	vSnap サーバーを使用した NFS ファイル共有に使用されます。
5671	TCP	RabbitMQ	VADP プロキシーおよび VMware ジョブ管理ワーカーによって作成およびコンシュームされるメッセージの管理に使用されるメッセージ・フレームワーク。また、ジョブ・ログを容易にします。
8761	TCP	Discovery Server	自動的に VADP プロキシーを検出し、IBM Spectrum Protect Plus VM バックアップ操作で使用されます。

表 6. 発信 *VADP* プロキシー・ファイアウォール接続 (続き)			
ポート	**プロトコル**	**サービス**	**説明**
20048	TCP	vSnap マウント	VADP プロキシー、アプリケーション・サーバー、仮想化データ・ストアなどのクライアントに vSnap ファイル・システムをマウントします。

ヒント : VADP プロキシーは、SSH ポート 22 を介して Linux ベースのサーバーにプッシュし、インストールすることができます。

ファイアウォール・コマンド・スクリプトがご使用のシステムでは使用できない場合は、ファイアウォールを手動で編集して必要なポートを追加し、ファイアウォールを再始動してください。ファイアウォール規則の編集について詳しくは、49 ページの『ファイアウォール・ポートの編集』で確認できます。

vSnap サーバー上の VADP プロキシーの要件

VADP プロキシーは、IBM Spectrum Protect Plus 環境内の vSnap サーバーにインストールできます。VADP プロキシーと vSnap サーバーの組み合わせの場合は、両方の装置の最小要件を満たす必要があります。両方の装置のシステム要件を調べ、コアと RAM の要件を一緒に追加して、VADP プロキシーと vSnap サーバーの組み合わせの最小要件を特定してください。

VADP プロキシーと vSnap サーバーの組み合わせが、各装置の要件の合計である以下の推奨最小要件を満たしていることを確認します。

仮想 vSnap サーバーにインストールされている VADP プロキシー:

- 64 ビット 8 コア・プロセッサー
- 48 GB RAM

VADP プロキシーと vSnap サーバーの組み合わせで、必要な VADP プロキシーと vSnap サーバーのすべてのポートが開いていなければなりません。詳しくは、システム要件の VADP プロキシーおよび vSnap ポートのセクションを参照してください。

クラウド要件

クラウド・ストレージにデータをオフロードするには、IBM Spectrum Protect Plus およびクラウド環境が以下の要件を満たしている必要があります。

ディスク・キャッシュ領域

オフロードまたはクラウドからのリストアに関連したすべての機能について、vSnap サーバーには、vSnap サーバー上のディスク・キャッシュ領域が必要です。

- オフロード操作中に、このキャッシュは、クラウド・エンドポイントへのアップロード保留中であるオブジェクト用の一時ステージング領域として使用されます。
- ディスク・キャッシュ領域は、リストア操作中に、ダウンロードされたオブジェクトをキャッシュに入れるため、およびリストア・ボリュームに書き込まれる一時データを保管するために使用されます。

キャッシュのサイジングおよびインストールの 手順については、Cloud offload configuration または IBM Spectrum Protect Plus Blueprints を参照してください。

証明書の要件

- **自己署名証明書:** クラウド・エンドポイントまたはリポジトリー・サーバーで自己署名証明書が使用される場合、IBM Spectrum Protect Plus ユーザー・インターフェースでクラウドまたはリポジトリー ・サーバーを登録するときに、証明書を (Privacy Enhanced Mail (PEM) 形式で) 指定する必要があります。

- **プライベート認証局で署名される証明書:** クラウド・エンドポイントまたはリポジトリー・サーバーで、プライベート認証局 (CA) で署名された証明書が使用される場合、IBM Spectrum Protect Plus ユーザー・インターフェースでクラウドまたはリポジトリー・サーバーを登録するときに、そのエンドポイント証明書が (PEM 形式で) 指定されなければなりません。さらに、以下の手順を使用して、プライベート CA のルート/中間証明書を各 vSnap サーバー内のシステム証明書ストアに追加する必要があります。

  1. serveradmin ユーザーとして vSnap サーバー・コンソールにログインし、プライベート CA 証明書 (PEM 形式) はすべて一時的な場所にアップロードします。
  2. 次のコマンドを実行して、各証明書ファイルをシステム証明書ストア・ディレクトリー (/etc/pki/ca-trust/source/anchors/) にコピーします。

     ```
     $ sudo cp /tmp/private-ca-cert.pem /etc/pki/ca-trust/source/anchors/
     ```

  3. 新たに追加されたカスタム証明書を取り込み、システム証明書バンドルを更新するには、次のコマンドを実行します。

     ```
     $ sudo update-ca-trust
     ```

- **パブリック認証局で署名される証明書:** クラウド・エンドポイントでパブリック CA で署名された証明書を使用する場合、特別なアクションは不要です。vSnap サーバーは、デフォルトのシステム 証明書ストアを使用して証明書を検証します。

ネットワークの要件

vSnap サーバーとクラウドまたはリポジトリー・サーバーのエンドポイントとの間の通信には、以下のポートが使用されます。

表 7. 発信 *vSnap* サーバー・ファイアウォール接続

ポート	プロトコル	サービス	説明
443	TCP	HTTPS	vSnap が Amazon S3、Azure、または IBM Cloud Object Storage エンドポイントと通信できるようにします。
9000	TCP	HTTPS	vSnap が IBM Spectrum Protect (リポジトリー・サーバー) エンドポイントと通信できるようにします。

vSnap サーバーとクラウド・エンドポイントとの間のトラフィックに SSL インターセプトまたはディープ・パケット・インスペクションを実行するファイアウォールまたはネットワーク・プロキシーがあると、vSnap サーバー上の SSL 証明書の検証を妨害する可能性があります。この妨害により、クラウド・オフロード・ジョブが失敗する可能性があります。 この妨害を回避するには、ファイアウォールまたはプロキシー構成で SSL インターセプトおよびインスペクションから vSnap サーバーを除外する必要があります。

クラウド・プロバイダーの要件

ネイティブ・ライフサイクル 管理はサポートされません。IBM Spectrum Protect Plus は、自動的に永久増分バックアップ・アプローチを使用して、アップロードされたオブジェクトのライフサイクルを 管理します。このアプローチでは、古いオブジェクトが新しいスナップショットで引き続き使用できます。IBM Spectrum Protect Plus の外部でオブジェクトの 自動または手動の期限切れ操作を行うと、データが破損します。

自己署名されているか、またはプライベート認証局によって署名された SSL 証明書を使用するクラウド・プロバイダーの場合は、証明書の要件を参照してください。

Amazon S3 クラウドの要件

- **オフロード:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、サポートされる以下のいずれかの Storage Tier の既存のバケットを指定する必要があります。S3 Standard、S3 Intelligent-Tiering、S3 Standard-Infrequent Access、または S3 One Zone-Infrequent Access。
- **アーカイブ:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、サポートされる以下のいずれかの Storage Tier の既存のバケットを指定する必要があります。S3 Standard、S3 Intelligent-Tiering、S3 Standard-Infrequent Access、または S3 One Zone-Infrequent Access。IBM Spectrum Protect Plus は、データ・ファイルを Glacier Tier に直接アップロードします。 一部の小さいメタデータ・ファイルは、バケットのデフォルトの Tier に保管されます。 これらのメタデータ・ファイルのコピーは、災害復旧のために Glacier Tier にも置かれます。

IBM Cloud Object Storage の要件

- **オフロード:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、既存のバケットを指定する必要があります。 指定されたバケットに、一定の期間オブジェクトをロックする WORM ポリシーがある場合、IBM Spectrum Protect Plus は自動的に構成を検出し、WORM ポリシーによりロックが解除された後にスナップショットを削除します。
- **アーカイブ:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、既存のバケットを指定する必要があります。 指定されたバケットに、一定の期間オブジェクトをロックする WORM ポリシーがある場合、IBM Spectrum Protect Plus は自動的に構成を検出し、WORM ポリシーによりロックが解除された後にスナップショットを削除します。IBM Spectrum Protect Plus は、データ・ファイルを Archive Tier にマイグレーションするために、バケットに単一のライフサイクル管理規則を作成します。

Microsoft Azure の要件

- **オフロード:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、ホットまたはクール・ストレージ・アカウント内の既存のコンテナーを指定する必要があります。
- **アーカイブ:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、ホットまたはクール・ストレージ・アカウント内の既存のコンテナーを指定する必要があります。 IBM Spectrum Protect Plus は、オンデマンドでファイルを Tier 間で移動します。 データ・ファイルは、即時に Archive Tier に移動され、リストア操作時にのみ一時的に Hot Tier に戻ります。一部の小さいメタデータ・ファイルは、コンテナーのデフォルトの Tier に保管されます。 これらのメタデータ・ファイルのコピーは、災害復旧のために Archive Tier にも置かれます。

IBM Spectrum Protect (リポジトリー・サーバー) の要件

- **オフロード:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、既存のバケットを使用できません。 IBM Spectrum Protect Plus は、固有の名前を持つバケットを独自に作成します。
- **アーカイブ:** クラウド・プロバイダーが IBM Spectrum Protect Plus で登録されるときに、既存のバケットを使用できません。 IBM Spectrum Protect Plus は、固有の名前を持つバケットを独自に作成します。IBM Spectrum Protect Plus は、データ・ファイルを IBM Spectrum Protect 磁気テープ・ストレージに直接アップロードします。一部の小さいメタデータ・ファイルは、IBM Spectrum Protect オブジェクト・ストレージに保管されます。 これらのメタデータ・ファイルのコピーは、災害復旧のために IBM Spectrum Protect 磁気テープ・ストレージにも置かれます。

表 *8.* クラウド・プロバイダーのオフロードおよびアーカイブの要件

操作	プロバイダー	要件
オフロード	Amazon S3	サポートされるいずれかの Storage Tier から、既存のバケットを指定する必要があります。
オフロード	IBM Cloud Storage	既存のバケットを指定する必要があります。

表 8. クラウド・プロバイダーのオフロードおよびアーカイブの要件 (続き)		
操作	**プロバイダー**	**要件**
オフロード	Microsoft Azure	Hot Storage Tier または Cool Storage Tier から、既存のコンテナーを指定する必要があります。
オフロード	IBM Spectrum Protect	IBM Spectrum Protect Plus は、独自の固有バケットを作成します。
アーカイブ	Amazon S3	vSnap が IBM Spectrum Protect (リポジトリー・サーバー) エンドポイントと通信できるようにします。
アーカイブ	IBM Cloud Storage	Archive Tier から既存のバケットを指定する必要があります。
アーカイブ	Microsoft Azure	Hot Storage Tier または Archive Tier から、既存のコンテナーを指定する必要があります。
アーカイブ	IBM Spectrum Protect	IBM Spectrum Protect Plus は、IBM Spectrum Protect 磁気テープ・ストレージにコピーされる独自の固有バケットを作成します。

特定のクラウド・プロバイダーへのデータのセットアップおよびオフロードに役立つクイック・スタート情報については、Data offload to cloud object storage with IBM Spectrum Protect Plus を参照してください。

ハイパーバイザー要件

IBM Spectrum Protect Plus のハイパーバイザー要件を確認します。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

Hyper-V 要件

Microsoft Hyper-V サーバーは以下の最小要件を満たす必要があります。

- Hyper-V Server 2016 または Microsoft Hyper-V on Windows Server 2016
- Microsoft Hyper-V on Windows Server 2019

共用仮想ハード・ディスク (共用 VHDX) のバックアップとリストアはサポートされません。既知の問題と制約事項については、https://www.ibm.com/support/docview.wss?uid=ibm10884592 を参照してください。

IBM Spectrum Protect Plus は、Hyper-V レプリカが有効になっている環境を保護しません。

Microsoft iSCSI Initiator Service が、すべての Hyper-V サーバー (クラスター・ノードを含む) 上で実行されている必要があります。「**サービス**」ウィンドウで、Microsoft iSCSI Initiator Service の始動タイプを「**自動**」に設定し、Hyper-V サーバーまたはクラスター・ノードが始動したときにサービスを使用できるようにします。

Hyper-V サーバーで **DiskPart** 自動マウント・パラメーターが有効になっている必要があります。自動マウント・パラメーターの有効化について詳しくは、Microsoft Web サイトの自動マウントのトピックを参照してください。

Hyper-V サーバーは、ドメイン・ネーム・システム (DNS) 名または IP アドレスを使用して登録できます。DNS 名は IBM Spectrum Protect Plus によって解決可能でなければなりません。Hyper-V サーバーがクラ

スターの一部である場合、そのクラスター内のすべてのノードは DNS を使用して解決可能でなければなりません。DNS が使用できない場合、コマンド・ラインを使用して IBM Spectrum Protect Plus アプライアンス上の /etc/hosts ファイルにサーバーを追加する必要があります。複数の Hyper-V サーバーをクラスター環境でセットアップする場合、すべてのサーバーを /etc/hosts ファイルに追加する必要があります。IBM Spectrum Protect Plus でクラスターを登録する場合、Failover Cluster Manager を登録します。

VMware 要件

以下のバージョンの VMware vSphere がサポートされています。

- vSphere 5.5 (すべての更新およびパッチ・レベルを含む)
- vSphere 6.0 (すべての更新およびパッチ・レベルを含む)
- vSphere 6.5 (すべての更新およびパッチ・レベルを含む)
- vSphere 6.7 (すべての更新およびパッチ・レベルを含む)

最新バージョンの VMware Tools が環境にインストールされていることを確認してください。IBM Spectrum Protect Plus は、VMware Tools 9.10.0 をインストールした状態でテストされています。

物理 pRDM ボリュームはスナップショットをサポートしません。物理互換モード (pRDM) でプロビジョニングされた 1 つ以上のロー・デバイス・マッピング (RDM) ボリュームがある仮想マシンがバックアップされます。 ただし、これらの pRDM ボリュームは仮想マシンのバックアップ操作の一環としては処理されません。

ファイル索引付けおよびリストア要件

IBM Spectrum Protect Plus のファイル索引付けおよびリストア要件を検討します。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア 要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

ゲスト・オペレーティング・システムに直接マップされる iSCSI ディスクには、索引付けが行われません。サポートされるボリュームには、関連した仮想マシンの構成を使用してマウントされる VMDK ボリュームまたは VHD ボリュームがあります。

カタログ内のメタデータに必要なフリー・スペースの量は、環境内に存在するファイルの総数によって異なります。100 万個のファイルをカタログするには、IBM Spectrum Protect Plus アプライアンス内のカタログ・ボリュームに、保持するバージョンごとに約 350 MB のフリー・スペースが必要です。 ファイル索引付けメタデータで使用されるスペースは、対応するバックアップ・インスタンスの有効期限が切れると再利用されます。

VMware 要件

拡張構成における仮想マシンの設定では、disk.enableUUID 設定が存在し、true に設定されなければなりません。

Windows 要件

サポートされるオペレーティング・システム	• Windows Server 2008 R2 • Windows Server 2012 R2 および Windows Server 2012 R2 core • Windows Server 2016 および Windows Server 2016 Core • Windows Server 2019 および Windows Server 2019 core

サポートされるファイル・システム	• NTFS • ReFS • CsvFS
サポートされるディスク・ストレージ・タイプ	以下のものが備わった基本ディスク • MBR 区画 • GPT 区画 **制約事項 :** 動的ディスク上でのファイルのバックアップまたはリストアはサポートされません。

- IBM Spectrum Protect Plus は、ハイパーバイザーから利用できるオペレーティング・システムのみをサポートします。サポートされるオペレーティング・システムについては、ご使用のハイパーバイザーの資料を参照してください。
- ファイル索引付けとリストア操作は、Hyper-V 環境における SCSI ディスクをサポートします。Integrated Drive Electronics (IDE) ディスクはサポートされません。第 1 世代の仮想マシンには、IDE ブート・ディスクが必要であることに注意してください。ただし、追加の SCSI ディスクが使用可能である場合、ファイル索引付けとリストア操作はそれらのディスクでサポートされます。
- Windows Remote Shell (WinRM) が有効でなければなりません。

  重要 : IBM Spectrum Protect Plus は、他のファイル・システムを使用する仮想マシンの保護およびリストアはできますが、ファイル索引付けとリストアに適格であるのは、リストされているファイル・システムのみです。
- Windows 環境でファイルの索引付けが実行される場合、リソース上の以下のディレクトリーはスキップされます。

  ```
  ¥Drivers
  ¥Program Files
  ¥Program Files (x86)
  ¥Windows
  ¥winnt
  ```

  注 : これらのディレクトリー内のファイルは、IBM Spectrum Protect Plus インベントリーに追加されず、ファイル・リカバリーに使用できません。
- 最新バージョンの VMware Tools が VMware 仮想マシンにインストールされ、Hyper-V Integration Services がご使用の Hyper-V 仮想マシンにインストールされていることを確認してください。

スペース所要量

- ファイル索引付けの結果を保存できる十分な一時スペースが、`C:¥` ドライブに必要です。
- ファイル・システムに索引が付けられる場合、一時メタデータ・ファイルが `/tmp` ディレクトリーに生成され、索引付けが完了すると直ちに削除されます。メタデータに必要なフリー・スペースの量は、システム上に存在するファイルの総数によって異なります。100 万個のファイルごとに約 350 MB のフリー・スペースがあるようにしてください。

接続要件

- IBM Spectrum Protect Plus アプライアンスのホスト名は、Windows 仮想マシンから解決可能でなければなりません。
- 索引付け用に選択された仮想マシンの IP アドレスは、vSphere Client または Hyper-V Manager から可視でなければなりません。
- 索引付け用に選択された Windows 仮想マシンは、IBM Spectrum Protect Plus アプライアンスでポート 22 (SSH) との発信接続が可能でなければなりません。
- IBM Spectrum Protect Plus が WinRM を使用してサーバーに接続できるように、すべてのファイアウォールが構成されていなければなりません。

認証と特権の要件

仮想マシンに指定される資格情報には、以下の特権を持つユーザーが含まれていなければなりません。

- ユーザー ID には、「サービスとしてログオン」権限が必要です。この権限は、ローカル・マシンの管理ツール・コントロール・パネル (「**ローカル セキュリティ ポリシー**」 > 「**ローカル ポリシー**」 > 「**ユーザー権利の割り当て**」 > 「**サービスとしてログオン**」) から割り当てられます。

  「サービスとしてログオン」権限について詳しくは、Add the Log on as a service Right to an Account を参照してください。
- デフォルトのセキュリティー・ポリシーでは Windows NTLM プロトコルを使用します。Hyper-V 仮想マシンがドメインに接続されている場合、ユーザー ID はデフォルトの `domain¥Name` 形式に従います。ユーザーがローカル管理者である場合は、`<local administrator>` 形式が使用されます。関連付けられたバックアップ・ジョブ定義の中で「**ゲスト OS のユーザー名**」オプションと「**ゲスト OS のパスワード**」オプションを使用して、関連する仮想マシンの資格情報が設定されている必要があることに注意してください。
- システム・ログイン資格情報には、ローカル管理者の許可が必要です。

Kerberos 要件

- Kerberos ベースの認証は、IBM Spectrum Protect Plus アプライアンスの構成ファイルを使用して有効にすることができます。この設定により、デフォルトの Windows NTLM プロトコルが指定変更されます。Kerberos では、ローカル・ユーザー・アカウントを使用することができず、すべてのマシンが単一ドメインにある環境にのみ適しているので注意してください。
- Kerberos ベースの認証の場合に限り、ユーザー ID は `username@FQDN` 形式で指定する必要があります。完全修飾ドメイン名で指定されたドメイン上の鍵配布センター (KDC) から発券許可証 (TGT) を取得するには、指定されたユーザー名が、登録済みのパスワードを使用して認証できなければなりません。
- Kerberos 認証には、ドメイン・コントローラーと IBM Spectrum Protect Plus アプライアンスとの間のクロック・スキューが 5 分未満であることも必要です。デフォルトの Windows NTLM プロトコルは時間に依存しないので注意してください。

Linux 要件

サポートされるオペレーティング・システム	• Red Hat Enterprise Linux 6.4 以降の保守レベルおよびモディフィケーション ・レベル • CentOS 6.4 以降の保守レベルおよびモディフィケーション・レベル • Red Hat Enterprise Linux 7.0 以降の保守レベルおよびモディフィケーション ・レベル • CentOS 7.0 以降の保守レベルおよびモディフィケーション・レベル • SUSE Linux Enterprise Server 12.0 以降の保守レベルおよびモディフィケーション ・レベル
サポートされるファイル・システム	• ext2 • ext3 • ext4 • XFS

- 新しいカーネル・バージョンで作成されるファイル・システムが、旧カーネルを使用するシステムにマウントできない場合があります。この場合、新規システムから旧システムへのファイルのリストアはサポートされません。

IBM Spectrum Protect Plus は、ハイパーバイザーから利用できるオペレーティング・システムのみをサポートします。サポートされるオペレーティング・システムについては、ご使用のハイパーバイザーの資料を参照してください。

注 : IBM Spectrum Protect Plus は、他のファイル・システムを使用する仮想マシンの保護およびリストアはできますが、ファイル索引付けとリストアに適格であるのは、リストされているファイル・システムのみです。

- Linux 環境でファイルの索引付けが実行される場合、リソース上の以下のディレクトリーはスキップされます。

  ```
  /tmp
  /usr/bin
  /Drivers
  /bin
  /sbin
  ```

- /proc、/sys、/dev のような仮想ファイル・システム内のファイルもスキップされます。これらのディレクトリー内のファイルは、IBM Spectrum Protect Plus インベントリーに追加されず、ファイル・リカバリーに使用できません。

スペース所要量

- ファイル索引付けの結果を保存できる十分な一時スペースが、システム・ディスクに必要です。
- ファイル・システムに索引が付けられる場合、一時メタデータ・ファイルが /tmp ディレクトリーに生成され、索引付けが完了すると直ちに削除されます。メタデータに必要なフリー・スペースの量は、システム上に存在するファイルの総数によって異なります。100 万個のファイルごとに約 350 MB のフリー・スペースがあるようにしてください。

ソフトウェア要件

- Python バージョン 2.6 (任意のレベル) または 2.7 (任意のレベル) がインストールされなければなりません。
- Red Hat Enterprise Linux/CentOS 6.x のみ: **yum update util-linux-ng** を実行して util-linux-ng パッケージが最新のものであることを確認してください。ご使用のバージョンまたはディストリビューションに応じて、パッケージには util-linux という名前が付けられる場合があります。
- データが LVM ボリューム上にある場合、LVM バージョンが 2.0.2.118 以降であることを確認してください。バージョンを確認するには **lvm version** を実行します。必要に応じてパッケージを更新するには **yum update lvm2** を実行します。
- データが LVM ボリューム上にある場合、**lvm2-lvmetad** サービスが使用不可になっている必要があります。このサービスは、ボリューム・グループ・スナップショットまたはクローンのマウントおよび再署名を行う IBM Spectrum Protect Plus の機能を妨害する可能性があるためです。このサービスを使用不可にするには、以下のステップを実行します。

  1. 次のコマンドを実行します。

     ```
     systemctl stop lvm2-lvmetad
     systemctl disable lvm2-lvmetad
     ```

  2. /etc/lvm/lvm.conf を編集して、以下の設定を指定します。

     ```
     use_lvmetad = 0
     ```

  lvmetad サービスについて詳しくは、 The Metadata Daemon (lvmetad)を参照してください。

- データが XFS ファイル・システム上にあり、**xfsprogs** のバージョンが 3.2.0 からバージョン 4.1.9 までのものである場合、ファイル・リストアは、**xfsprogs** での既知の問題により失敗する可能性があります。この問題は、UUID が変更された場合にクローンまたはスナップショットのファイル・システムが破損する原因です。この問題を解決するには、**xfsprogs** をバージョン 4.2.0 以上に更新してください。

詳しくは、Debian Bug report logs を参照してください。

接続要件

SSH サービスがサーバー上のポート 22 で実行中でなければなりません。また IBM Spectrum Protect Plus が SSH を使用してサーバーに接続できるようにファイアウォールが構成されていなければなりません。SSH 用の SFTP サブシステムも使用可能でなければなりません。

認証と特権の要件

仮想マシンに指定される資格情報は、以下の **sudo** 特権を持つユーザーを指定する必要があります。

- sudoers 構成では、ユーザーがパスワードなしにコマンドを実行できなければなりません。
- !requiretty 設定値を指定する必要があります。

推奨される方法では、以下の特権を持つ専用の IBM Spectrum Protect Plus エージェント・ユーザーを作成します。構成例は次のとおりです。

- ユーザーを作成します。`useradd -m sppagent`

  ここで、**sppagent** は IBM Spectrum Protect Plus エージェント・ユーザーを指定します。
- パスワードを設定します。`passwd <sppagent>`

sudoers 構成ファイル (通常、`/etc/sudoers`) の終わりに以下の行を指定します。既存の sudoers ファイルが、別のディレクトリー (例えば、`/etc/sudoers.d`) から構成をインポートするように構成されている場合、そのディレクトリーの新しいファイルにもそれらの行を指定できます。

```
Defaults: sppagent !requiretty
sppagent ALL=(root) NOPASSWD:ALL
```

Microsoft Exchange Server の要件

IBM Spectrum Protect Plus をインストールする前に、製品やその他のコンポーネントのハードウェア要件とソフトウェア要件を検討してください。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

IBM Spectrum Protect Plus に対する Exchange データベースのバックアップ要件とリストア要件は次のとおりです。

構成

使用する Microsoft Exchange Server のバージョンが、ご使用のオペレーティング・システムでサポートされていることを確認してください。

アプリケーションのバージョン

- Microsoft Exchange Server 2013 CU16 以降の CU および保守レベル: Standard または Enterprise Edition。
- Microsoft Exchange Server 2016 CU 5 以降の CU および保守レベル: Standard および Enterprise Edition。
- Microsoft Exchange Server 2019 以降の保守レベル: Standard および Enterprise Edition。

注 : Microsoft Exchange データベース可用性グループ (DAG) がサポートされています。

オペレーティング・システム

- Windows Server 2012R2 以降の保守レベル (64 ビット・カーネル): Standard および Datacenter Edition
- Windows Server 2016 以降の保守レベル (64 ビット・カーネル): Standard および Datacenter Edition
- Windows Server 2019 以降の保守レベル (64 ビット・カーネル): Standard および Datacenter Edition

注 : Windows Server 2019 Core のインストールはサポートされます。ただし、コア・インストールでは高細分度リストア機能がサポートされません。

追加の注意事項

ご使用の環境に最新の Microsoft Exchange Server パッチおよび更新をインストールしてください。

Exchange Server の仮想化サポートについては、160 ページの『Microsoft Exchange Server の前提条件』を参照してください。

ソフトウェア

サポートされるバージョンの Windows 64 ビットのオペレーティング・システムがインストールされている必要があります。

Microsoft の以下の前提条件が必要であり、IBM Spectrum Protect Plus を使用する前にインストールされていなければなりません。

- Windows PowerShell 4 以降
- Windows Management Framework 4 以降

Microsoft Exchange Server 2013 と高細分度リストア機能を使用する場合は、 Microsoft Exchange Messaging API (MAPI) Client および Collaboration Data Objects (MAPI/CDO) に対してサポートされている最小レベルは、バージョン 6.5.8320.0 です。

注 : MAPI/CDO は Microsoft Exchange Server 2013 のみに必要です。Microsoft Exchange Server 2016 または Exchange Server 2019 を実行している場合は必要ありません。

Microsoft Exchange Server 2016 または Microsoft Exchange Server 2019 で高細分度リストア機能を使用する場合、Microsoft 32 ビット Outlook 2016 または Microsoft 32 ビット Outlook 2019 が必要です。

Microsoft の以下の前提条件が必要であり、仮想マシン上にまだ存在しない場合は、IBM Spectrum Protect Plus 高細分度リストア機能によって自動的にインストールされます。

- 32 ビット Microsoft Visual C++ 2012 Redistributable Package
- 64 ビット Microsoft Visual C++ 2012 Redistributable Package
- 32 ビット Microsoft Visual C++ 2017 Redistributable Package
- 64 ビット Microsoft Visual C++ 2017 Redistributable Package
- Microsoft .NET Framework 4.5
- Microsoft ReportViewer 2012 SP1 Redistributable
- Microsoft SQL Server 2012 System CLR Types
- Microsoft SQL Server 2014 System CLR Types
- Microsoft SQL Server 2016 System CLR Types

ヒント : これらの前提条件のインストールには、システム再始動が必要な場合があります。システム再始動を避けるには、IBM Spectrum Protect Plus 高細分度リストア機能を開始する前に、これらの前提条件がインストールされていることを確認してください。

特権

IBM Spectrum Protect Plus エージェント・ユーザーには以下の特権があります。

Microsoft Exchange Server は、役割ベースの認証によって保護されます。 Microsoft Exchange エージェントが IBM Spectrum Protect Plus 環境で機能するには、適切な特権をセットアップする必要があります。詳しくは、160 ページの『特権』を参照してください。

ポート

IBM Spectrum Protect Plus エージェント・ユーザーは、以下のポートを使用します。「ファイアウォール規則」列の「受け入れ」で示されるポートは、セキュア接続 (HTTPS または SSL) を使用します。

表 9. 着信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	ファイアウォール規則	サービス	説明
5985	TCP	Accept	WinRM	Windows Remote Management Service
5986	TCP	Accept	WinRM	Secure Windows Remote Management Service

表 10. 発信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	サービス	説明
3260*	TCP	vSnap iSCSI	バックアップとリカバリー用に LUNS をマウントするのに使用される iSCSI vSnap ターゲット・ポート
137	UDP	vSnap SMB/CIFS	トランザクション・ログのバックアップとリカバリー用にファイル・システム共有をマウントするのに使用される、vSnap SMB ターゲット・ポートまたは CIFS ターゲット・ポート
138	UDP	vSnap SMB/CIFS	トランザクション・ログのバックアップとリカバリー用にファイル・システム共有をマウントするのに使用される、vSnap SMB ターゲット・ポートまたは CIFS ターゲット・ポート
139	TCP	vSnap SMB/CIFS	トランザクション・ログのバックアップとリカバリー用にファイル・システム共有をマウントするのに使用される、vSnap SMB ターゲット・ポートまたは CIFS ターゲット・ポート
445	TCP	vSnap SMB/CIFS	トランザクション・ログのバックアップとリカバリー用にファイル・システム共有をマウントするのに使用される、vSnap SMB ターゲット・ポートまたは CIFS ターゲット・ポート

*このノードでは iSCSI イニシエーターが必要です。

ハードウェア

システム	ディスク・スペース	高細分度リストア操作用のディスク・スペース
x64: オペレーティング・システムおよび Microsoft Exchange Server によってサポートされる互換ハードウェア	製品のインストールに 200 MB 以上のディスク・スペース	まだインストールされていない場合に自動的にインストールされる、「追加の Microsoft 前提条件」用の 2.1 GB 以上のディスク・スペース

Db2 の要件

Db2 を IBM Spectrum Protect Plus に登録する前に、ご使用の環境が以下に示された要件を満たしていることを確認してください。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

IBM Spectrum Protect Plus に対する IBM Db2 データベースのバックアップ要件とリストア要件は次のとおりです。

構成要件

以下の IBM Db2 データベースがサポートされています。

- IBM Db2 バージョン 10.5 以降の保守レベルおよびモディフィケーション ・レベル: Enterprise Server Edition。
- IBM Db2 バージョン 11.1 以降の保守レベルおよびモディフィケーション ・レベル: Enterprise Server Edition。

オペレーティング・システム

次のオペレーティング・システムがサポートされています。

- PowerPC® の場合:
  - AIX® 7.1 以降のモディフィケーションおよびフィックスパック ・レベル (64 ビット・カーネル)。
  - AIX 7.2 以降のモディフィケーションおよびフィックスパック ・レベル (64 ビット・カーネル)。
- Linux x86_x64 の場合:
  - Red Hat Enterprise Linux 6.8 以降の保守レベルおよびモディフィケーション ・レベル。
  - Red Hat Enterprise Linux 7 以降の保守レベルおよびモディフィケーション ・レベル。
  - SUSE Linux Enterprise Server 11.0 SP4 以降の保守レベルおよびモディフィケーション ・レベル。
  - SUSE Linux Enterprise Server 12.0 SP1 以降の保守レベルおよびモディフィケーション ・レベル。
- Linux on Power® System (リトル・エンディアン) の場合:
  - Red Hat Enterprise Linux 7.1 以降の保守レベルおよびモディフィケーション ・レベル。
  - SUSE Linux Enterprise Server 12.0 SP1 以降の保守レベルおよびモディフィケーション ・レベル。

追加の注意事項

ご使用の環境に最新の IBM Db2 パッチおよび更新をインストールしてください。

IBM Db2 pureScale® はサポートされていません。

Db2 環境が以下の基準を満たすように構成されていることを確認してください。

- Db2 アーカイブ・ロギングがアクティブになり、Db2 がリカバリー可能モードです。
- Db2 表スペース (データおよび一時表スペース)、ローカル・データベース・ディレクトリー、および Db2 ログ・ファイルを保持する論理ボリュームは、Linux では論理ボリューム・マネージャー (LVM2) によって、また、AIX では JFS2 によってそれぞれ管理されます。Linux 上の LVM2 と AIX 上の JFS2 は、一時ボリューム・スナップショットの作成に使用されます。スナップショットが存在する間、データがソース・ボリューム上で変更されるにつれて、論理ボリュームのサイズがデータで大きくなります。詳しくは、140 ページの『LVM2 および JFS2』を参照してください。
- 複数の区画を保護する場合、Db2 は並列バックアップ・モードでなければなりません。並列バックアップ・モードは、Db2 レジストリー変数を使用して有効にすることができます。詳しくは、137 ページの『Db2 の前提条件』を参照してください。

ソフトウェア

以下のソフトウェア要件を確認します。

- bash パッケージと sudo パッケージがインストールされていなければなりません。Sudo のバージョンは 1.7.6p2 以上でなければなりません。バージョンを確認するには、sudo -V を実行してください。

  注 : 必要な bash パッケージおよび sudo パッケージは、サポートされる Linux86_64 および Linux Power Systems (リトル・エンディアン) の各オペレーティング・システムに含まれています。
- Linux では Python バージョン 2.6 (任意のレベル) または 2.7 (任意のレベル) がインストールされている必要があります。
- AIX では Python バージョン 2.7.x がインストールされている必要があります。
- サポートされるバージョンの Linux x86_64、Linux Power Systems (リトル・エンディアン)、または AIX がインストールされていることを確認します。

接続性

以下の接続基準を満たしていることを確認してください。

- SSH サービスがサーバー上のポート 22 で実行中であること。
- IBM Spectrum Protect Plus が SSH を使用してサーバーに接続できるようにファイアウォールが構成されていなければならないこと。
- SSH の SFTP サブシステムが 使用可能であること。
- サーバーは DNS 名または IP アドレスを使用して登録できること。DNS 名は IBM Spectrum Protect Plus によって解決可能でなければなりません。
- AIX で、コマンド **nfso -p -o nfs_use_reserved_port=1** を使用することで NFS 通信が予約済みポートを使用して構成されていることを確認してください。

認証と特権

Db2 サーバーは IBM Spectrum Protect Plus で登録されなければなりません。これには、Db2 サーバーに存在するオペレーティング・システム・ユーザー (IBM Spectrum Protect Plus エージェント・ユーザーと呼ばれます) を使用します。

パスワードが正しく構成されていること、および他のプロンプト (パスワードをリセットするプロンプトなど) が表示されることなくユーザーがログインできることを確認します。

IBM Spectrum Protect Plus エージェント・ユーザーには以下の特権が必要です。

- root ユーザーとしてコマンドを実行する特権、および sudo を使用して Db2 ソフトウェア所有者ユーザーとしてコマンドを実行する特権。IBM Spectrum Protect Plus では、ストレージ・レイアウトの検出、ディスクのマウントとアンマウント、データベースの管理などのさまざまなタスクにこの特権が必要です。
  - sudoers 構成では、IBM Spectrum Protect Plus エージェント・ユーザーがパスワードなしにコマンドを実行できなければなりません。
  - `!requiretty` 設定値を指定する必要があります。

- `/usr/local/bin/db2ls` を使用して Db2 インベントリーを読み取る特権。IBM Spectrum Protect Plus では、IBM Db2 インスタンスとデータベースに関する情報を検出し、収集するのにこの特権が必要です。

ポート

IBM Spectrum Protect Plus エージェントは、以下のポートを使用します。Accept のマークが付いているポートはセキュア接続 (HTTPS/SSL) を使用します。

表 *11.* 着信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	ファイアウォール	サービス	説明
22	TCP	Accept	SSH	内部 vSnap サーバーとの間での SSH データ転送に使用されます。

表 *12.* 発信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	サービス	説明
111	TCP	vSnap RPC Port Bind	Open Network Computing (ONC) クライアントが ONC サーバーとの通信に必要とするポートをクライアントが検出できるようにします。
2049	TCP	vSnap NFS	vSnap を介した NFS ファイル共有に使用されます。
20048	TCP	vSnap NFS Mount	VADP プロキシー、アプリケーション・サーバー、仮想化データ・ストアなどのクライアントに vSnap ファイル・システムをマウントします。

MongoDB の要件

MongoDB を IBM Spectrum Protect Plus に登録する前に、ご使用の環境が以下に示された要件を満たしていることを確認してください。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

IBM Spectrum Protect Plus に対する MongoDB データベースのバックアップ要件とリストア要件は次のとおりです。

構成要件

以下のバージョンの MongoDB データベースがサポートされています。

- MongoDB バージョン 3.6 以降の保守レベルおよびモディフィケーション ・レベル: Community Server および Enterprise Server Edition。

- MongoDB バージョン 4.0 以降の保守レベルおよびモディフィケーション・レベル: Community Server および Enterprise Server Edition。

オペレーティング・システム

次のオペレーティング・システムがサポートされています。

- Linux x86_x64 の場合:
  - Red Hat Enterprise Linux 6.8 以降の保守レベルおよびモディフィケーション・レベル
  - CentOS 6.8 以降の保守レベルおよびモディフィケーション・レベル
  - Red Hat Enterprise Linux 7 以降の保守レベルおよびモディフィケーション・レベル
  - CentOS 7 以降の保守レベルおよびモディフィケーション・レベル
  - SUSE Linux Enterprise Server 12.0 SP1 以降の保守レベルおよびモディフィケーション・レベル
- Linux Power Systems (リトル・エンディアン)
  - Red Hat Enterprise Linux 7.1 以降の保守レベルおよびモディフィケーション・レベル
  - CentOS 7 以降の保守レベルおよびモディフィケーション・レベル

注: Linux Power Systems (リトル・エンディアン) では、MongoDB エンタープライズ・サーバー・エディションのみがサポートされます。

追加の注意事項

パフォーマンスを最適化するには、ご使用の環境で使用可能な最新の MongoDB パッチおよび更新をインストールしてください。

MongoDB 環境が以下の基準を満たすように構成されていることを確認してください。

- MongoDB は、スタンドアロン・インスタンスまたはレプリカ・セットとして構成されています。MongoDB sharded クラスター・インスタンスのバックアップ操作はサポートされません。バックアップには常に、インスタンス内のすべてのデータベースが含まれます。
- MongoDB インスタンスは、WiredTiger Storage Engine を使用するように構成されています。
- IBM Spectrum Protect Plus における MongoDB アプリケーション・サーバー登録のユーザーは、MongoDB 管理データベースからサーバー情報と状況を取得できなければなりません。
- MongoDB データの論理ボリュームとログ・パスは、Linux 論理ボリューム・マネージャー (LVM2) によって管理されます。 LVM2 は、一時ボリューム・スナップショットの作成に使用されます。データベース・ファイルとジャーナル名は単一のボリュームに配置されなければなりません。スナップショットが存在する間、データがソース・ボリューム上で変更されるにつれて、論理ボリュームのサイズがデータで大きくなります。詳しくは、196 ページの『Linux LVM2 』を参照してください。

ソフトウェア

以下のソフトウェア要件を確認します。

- Python バージョン V2.6 (任意のレベル) または V2.7 (任意のレベル) がインストールされている必要があります。
- MongoDB アプリケーション・サーバーが RHEL 6 または CentOS 6 を実行する場合、`openssl` パッケージがバージョン 1.0.1e-57 以上であることを確認します。この要件に合うように更新するには、「`yum update openssl`」を実行してください。
- サポートされるバージョンの Linux x86_64 または Linux Power リトル・エンディアンがインストールされていることを確認します。

接続性

以下の接続基準を満たしていることを確認してください。

- SSH サービスがサーバー上のポート 22 で実行中であること。

- IBM Spectrum Protect Plus が SSH を使用してサーバーに接続できるようにファイアウォールが構成されていなければならないこと。
- SSH の SFTP サブシステムが使用可能であること。
- アプリケーション・サーバーが DNS 名または IP アドレスを使用して IBM Spectrum Protect Plus に登録できること。DNS 名は IBM Spectrum Protect Plus によって解決可能でなければなりません。

認証と特権

MongoDB サーバーは、IBM Spectrum Protect Plus に登録されている必要があります。これには、MongoDB サーバー上に存在するオペレーティング・システム・ユーザー (このトピックの残りの部分では *IBM Spectrum Protect Plus* エージェント・ユーザー と呼びます) を使用します。

パスワードが正しく構成されていること、および他のプロンプト (パスワードをリセットするプロンプトなど) が表示されることなくユーザーがログインできることを確認します。

MongoDB で、SSL ベースの暗号化と証明書ベースの認証はサポートされません。

MongoDB Enterprise Server Edition では、ストレージでの暗号化のみがサポートされます。

IBM Spectrum Protect Plus エージェント・ユーザーには以下の特権が必要です。

- root ユーザーとしてコマンドを実行する特権、および sudo を使用して MongoDB ソフトウェア所有者ユーザーとしてコマンドを実行する特権。IBM Spectrum Protect Plus では、ストレージ・レイアウトの検出、ディスクのマウントとアンマウント、データベースの管理などのタスクにこの特権が必要です。
  - sudoers 構成では、IBM Spectrum Protect Plus エージェント・ユーザーがパスワードなしにコマンドを実行できなければなりません。
  - `!requiretty` 設定値を指定する必要があります。
- 標準の MongoDB サーバー・モジュール `/usr/local/bin/mongodb` を実行する特権。IBM Spectrum Protect Plus では、インスタンスの割り当て済みの DNS/IP 名とポートを使用して MongoDB サーバーに接続できるように pymongo API を使用するのにこの特権が必要です。このメカニズムは、MongoDB インスタンスとデータベースに関する情報の収集に使用されます。
- MongoDB サーバーが役割ベースの認証によって保護されている場合、MongoDB エージェントが IBM Spectrum Protect Plus 環境で機能するには、適切な特権をセットアップする必要があります。詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。

ポート

IBM Spectrum Protect Plus エージェント・ユーザーは、以下のポートを使用します。「ファイアウォール規則」列の「受け入れ」で示されるポートは、セキュア接続 (HTTPS/SSL) を使用します。

表 *13.* 着信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	ファイアウォール規則	サービス	説明
22	TCP	Accept	SSH	内部 vSnap サーバーとの間での SSH データ転送に使用されます

表 14. 発信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続			
ポート	**プロトコル**	**サービス**	**説明**
111	TCP	vSnap RPC Port Bind	Open Network Computing (ONC) クライアントが ONC サーバーとの通信に必要とするポートをクライアントが検出できるようにします
2049	TCP	vSnap NFS	vSnap を介した NFS ファイル共有に使用されます
20048	TCP	vSnap NFS Mount	VADP プロキシー、アプリケーション・サーバー、仮想化データ・ストアなどのクライアントに vSnap ファイル・システムをマウントします

Oracle 要件

IBM Spectrum Protect Plus の Oracle データベースのバックアップ要件とリストア要件を検討します。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

構成要件

データベース・バージョン

- Oracle 11g R2
- Oracle 12c R1
- Oracle 12c R2
- Oracle 18c

注 : Oracle 12c 以降のマルチテナント・データベースの場合、IBM Spectrum Protect Plus は、すべてのプラグ可能なデータベース (PDB) を含めて、コンテナー・データベースの保護とリカバリーをサポートします。特定の PDB の細分性の高いリカバリーは、RMAN と組み合わせた Instant Disk Restore リカバリーにより実行できます。

オペレーティング・システム

- AIX 6.1 TL9 以降の保守レベルおよびモディフィケーション ・レベル
- AIX 7.1 以降の保守レベルおよびモディフィケーション ・レベル
- Red Hat Enterprise Linux CentOS 6.5 以降の保守レベルおよびモディフィケーション ・レベル
- Red Hat Enterprise Linux CentOS 7.0 以降の保守レベルおよびモディフィケーション ・レベル
- SUSE Linux Enterprise Server 11.0 SP4 以降の保守レベルおよびモディフィケーション ・レベル
- SUSE Linux Enterprise Server 12.0 SP1 以降の保守レベルおよびモディフィケーション ・レベル
- SUSE Linux Enterprise Server 15.0 以降の保守レベルおよびモディフィケーション ・レベル

追加の注意事項

- Oracle DataGuard はサポートされません。

- データベースは ARCHIVELOG モードでなければなりません。IBM Spectrum Protect Plus は、NOARCHIVELOG モードで実行中のデータベースを保護できません。
- Real Application Cluster (RAC) データベース・リカバリーは、サーバー・プール対応ではありません。IBM Spectrum Protect Plus は、データベースを RAC にリカバリーできますが、特定のサーバー・プールにはリカバリーできません。
- RMAN のスナップショット制御ファイルの位置が、すべてのクラスター・インスタンスからアクセス可能な共用ストレージを指すように、RAC データベースが構成されなければなりません。
- バックアップ時にマルチスレッド対応で構成された Oracle データベースをリストアしても、リストアされたデータベースはマルチスレッドになりません。リストアされたデータベースでマルチスレッドを使用するには、手動で再構成する必要があります。

ソフトウェア

- **bash** パッケージと **sudo** パッケージがインストールされていなければなりません。**sudo** のバージョンは 1.7.6p2 以上でなければなりません。バージョンを確認するには、**sudo -V** を実行してください。
- Python バージョン 2.6.x または 2.7.x がインストールされていなければなりません。
- **RHEL/CentOS 6.x のみ:**

  yum update util-linux-ng を実行して、`util-linux-ng` パッケージが最新であることを確認します。

  ご使用のバージョンまたはディストリビューションに応じて、パッケージには `util-linux` という名前が付けられる場合があります。

接続性

- SSH サービスがサーバー上のポート 22 で実行し、IBM Spectrum Protect Plus が SSH を使用してサーバーに接続できるように、何らかのファイアウォールが構成されている必要があります。SSH 用の SFTP サブシステムも 使用可能でなければなりません。
- サーバーは DNS 名または IP アドレスを使用して登録できます。DNS 名は IBM Spectrum Protect Plus によって解決可能でなければなりません。
- DNS が使用できない場合、コマンド・ラインを使用して IBM Spectrum Protect Plus アプライアンス上の `/etc/hosts` ファイルにサーバーを追加する必要があります。
- Oracle RAC ノードを登録する際に、物理 IP または名前を使用して各ノードを登録します。仮想名または Single Client Access Name (SCAN) を使用しないでください。

認証と特権

- Oracle サーバーは、Oracle サーバーに存在するオペレーティング・システム・ユーザーを使用して IBM Spectrum Protect Plus で登録されなければなりません。その後、ユーザーは IBM Spectrum Protect Plus エージェント・ユーザーと呼ばれます。
- パスワードが正しく構成されていること、および他のプロンプト (パスワードをリセットするプロンプトなど) が表示されることなくユーザーがログインできることを確認します。

IBM Spectrum Protect Plus エージェント・ユーザーには以下の特権が必要です。

- root としてコマンドを実行する特権、および **sudo** を使用して Oracle ソフトウェア所有者ユーザー (例えば、`oracle`、`grid`) としてコマンドを実行する特権。これらの特権は、ストレージ・レイアウトの検出、ディスクのマウントとアンマウント、データベースと ASM の管理などのさまざまなタスクに必要です。
  - `sudoers` 構成では、IBM Spectrum Protect Plus エージェント・ユーザーがパスワードなしにコマンドを実行できなければなりません。
  - !requiretty 設定値を指定する必要があります。
  - ENV_KEEP 設定では、ORACLE_HOME および ORACLE_SID 環境変数が保持できなければなりません。

- Oracle インベントリーを読み取る特権。これらの特権は、Oracle ホームおよびデータベースに関する情報の検出および収集などのタスクに必要です。

  これを実現するには、IBM Spectrum Protect Plus エージェント・ユーザーが、Oracle インベントリー・グループ (通常、`oinstall` という名前) に属している必要があります。

必要な特権を持つユーザーの作成については、38 ページの『IBM Spectrum Protect Plus エージェント・ユーザーの構成例』を参照してください。

NFS

Oracle サーバーには、ネイティブの Linux または AIX NFS クライアントがインストールされている必要があります。IBM Spectrum Protect Plus は、NFS を使用して、バックアップ操作とリストア操作用のストレージ・ボリュームをマウントします。

データベースのリストア時に、Oracle Direct NFS 機能が必要です。IBM Spectrum Protect Plus は、(まだ有効になっていない場合) Direct NFS を自動的に有効にします。

Direct NFS が正しく機能するには、各 Oracle ホームの実行可能な `<ORACLE_HOME>/bin/oradism` が root によって所有され、setuid 特権を持っている必要があります。これは通常、Oracle インストーラーによって事前構成されますが、特定のシステムでは、バイナリーに必要な特権がない場合があります。詳しくは、Oracle サポートの Web サイトにある資料 Database Startup Failed with Direct NFS を参照してください。

正しい特権を設定するには、以下のコマンドを実行します。

- `chown root:oinstall <ORACLE_HOME>/bin/oradism`
- `chmod 750 <ORACLE_HOME>/bin/oradism`

ここで、`oinstall` は、インストール済み環境を所有するグループを指定します。

データベースのディスカバリー

IBM Spectrum Protect Plus は、`/etc/oraInst.loc` ファイルと `/etc/oratab` ファイルだけでなく、実行中の Oracle プロセスのリストを調べて、Oracle インストール済み環境とデータベースを検出します。これらのファイルがデフォルトのロケーションに存在しない場合、IBM Spectrum Protect Plus がファイルを検索できるように、「locate」ユーティリティーがシステムにインストールされていなければなりません 。

IBM Spectrum Protect Plus は、実行中のインスタンスに接続し、データ・ファイル、ログ・ファイルなどのロケーションを照会して、データベースとそれらのストレージのレイアウトを 検出します。カタログ操作やコピー操作中に IBM Spectrum Protect Plus が正しくデータベースを検出できるようにするには、データベースが、「MOUNTED」、「READ ONLY」、または「READ WRITE」のいずれかのモードでなければなりません。IBM Spectrum Protect Plus は、シャットダウンされたデータベース・インスタンスを検出することも保護することもできません。

ブロック・チェンジ・トラッキング

IBM Spectrum Protect Plus では、増分バックアップを効率よく実行するために、保護されたデータベースで Oracle ブロック・チェンジ・トラッキングが有効でなければなりません。 ブロック・チェンジ・トラッキングがまだ有効になっていない場合、IBM Spectrum Protect Plus は、バックアップ・ジョブ中に自動的に有効にします。

ブロック・チェンジ・トラッキング・ファイルの配置をカスタマイズするには、関連したバックアップ・ジョブを実行する前にブロック・チェンジ・トラッキング機能を手動で有効にする必要があります。この機能が IBM Spectrum Protect Plus によって自動的に有効になる場合、ブロック・チェンジ・トラッキング・ファイルの配置を判別するのに以下の規則が使用されます。

- **db_create_file_dest** パラメーターが設定されている場合、ブロック・チェンジ・トラッキング・ファイルはこのパラメーターによって指定されたロケーションで作成されます。
- **db_create_file_dest** パラメーターが設定されていない場合、ブロック・チェンジ・トラッキング・ファイルは、SYSTEM 表スペースと同じディレクトリーで作成されます。

ログ・バックアップ

- **cron** デーモンがアプリケーション・サーバーで使用可能でなければなりません。
- IBM Spectrum Protect Plus エージェント・ユーザーには、**crontab** コマンドを使用して、cron ジョブを作成するのに必要な特権が必要です。特権は、cron.allow 構成ファイルを使用して付与できます。

IBM Spectrum Protect Plus エージェント・ユーザーの構成例

以下のコマンドは、IBM Spectrum Protect Plus が Oracle サーバーへのログインに使用するオペレーティング・システム・ユーザーを作成し、構成する場合の例です。コマンド構文は、ご使用のオペレーティング・システムのタイプとバージョンによって 異なる場合があります。

- IBM Spectrum Protect Plus エージェント・ユーザーとして指定されるユーザーを作成します。useradd -m sppagent
- パスワードを設定します。passwd sppagent
- 鍵ベースの認証を使用する場合、/home/sppagent/.ssh/authorized_keys ディレクトリーまたはご使用の SSHD 構成に応じた適切なファイルに公開鍵を置きます。次のように、正しい所有権と許可が設定されていることを確認します。

```
chown -R sppagent:sppagent /home/sppagent/.ssh
chmod 700 /home/sppagent/.ssh
chmod 600 /home/sppagent/.ssh/authorized_keys
```

- Oracle インストール済み環境と OSDBA グループにユーザーを追加します。usermod -a -G oinstall,dba sppagent
- ASM が使用中の場合、ユーザーを OSASM グループにも追加します。usermod -a -G asmadmin sppagent
- sudoers 構成ファイル (通常、/etc/sudoers) の終わりに以下の行を指定します。既存の sudoers ファイルが、別のディレクトリー (例えば、/etc/sudoers.d) から構成をインポートするように構成されている場合、そのディレクトリーの新しいファイルにもそれらの行を指定できます。

```
Defaults:sppagent !requiretty
Defaults:sppagent env_keep+="ORACLE_HOME"
Defaults:sppagent env_keep+="ORACLE_SID"
sppagent ALL=(ALL) NOPASSWD:ALL
```

ポート

IBM Spectrum Protect Plus エージェント・ユーザーは、以下のポートを使用します。「ファイアウォール・ルール」列の「受け入れ」で示されるポートは、セキュア接続 (HTTPS または SSL) を使用します。

表 *15.* 着信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	ファイアウォール規則	サービス	説明
22	TCP	Accept	SSH	内部 vSnap サーバーとの間での SSH データ転送に使用されます。

表 16. 発信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続			
ポート	**プロトコル**	**サービス**	**説明**
111	TCP	vSnap RPC Port Bind	Open Network Computing (ONC) クライアントが ONC サーバーとの通信に必要とするポートをクライアントが検出できるようにします。
443	TCP	HTTPS	ログ・バックアップの障害が発生した場合にアラートを送信するために、Oracle Server が IBM Spectrum Protect Plus と通信できるようにします。
2049	TCP	vSnap NFS	vSnap を介した NFS ファイル共有に使用されます。
20048	TCP	vSnap NFS Mount	VADP プロキシー、アプリケーション・サーバー、仮想化データ・ストアなどのクライアントに vSnap ファイル・システムをマウントします。

Microsoft SQL Server の要件

IBM Spectrum Protect Plus の Microsoft SQL Server データベースのバックアップ要件とリストア要件を検討します。

バックアップ操作やリストア操作が正常に実行できるように、ご使用のシステムでハードウェア要件とソフトウェア要件が満たされている必要があります。以下の要件を開始点として使用してください。 更新が含まれている可能性がある最新の要件については、技術情報 2013790 を参照してください。

構成

データベース・バージョン

- SQL Server 2008 R2 SP3
- SQL Server 2012
- SQL Server 2012 SP2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

最良のパフォーマンスを確保するには、ご使用の環境に最新の SQL Server パッチおよび更新をインストールしてください。

オペレーティング・システム

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Windows Remote Shell (WinRM) が有効でなければなりません。

SQL Server システムと vSnap サーバーとの間の iSCSI 経路が有効になっている必要があります。詳しくは、を参照してください。Microsoft iSCSI Initiator Step-by-Step Guide.

IBM Spectrum Protect Plus インベントリー・ジョブは、システム・データベースを検出し、保護の対象になるデータベースにマークを付けます。すべてのシステム・データベースと単純復旧モデルで実行するデータベースの場合、ログ・バックアップには不適格のマークが付けられます。

インメモリー OLTP

インメモリー・オンライン・トランザクション処理 (OLTP) は、データベース・アプリケーションのパフォーマンス向上に使用される、メモリーが最適化されたデータベース・エンジンです。このエンジンは、SQL Server 2014 以降でサポートされます。 インメモリー OLTP の使用には、以下の要件と制約事項が適用されます。

- 最大のリストア・ファイル・パスは 256 文字未満でなければなりません。元のパスがこの長さを超える場合は、長さを短くするためにカスタマイズされたリストア・ファイル・パスの使用を検討してください。
- リストアできるメタデータは、ボリューム・シャドー・コピー・サービス (VSS) および SQL Server のリストア機能を条件とします。

増分バックアップ

IBM Spectrum Protect Plus では、SQL Server 環境における増分バックアップを実行するために、更新シーケンス番号 (USN) 変更ジャーナル・テクノロジーを使用します。USN 変更ジャーナルは、ファイル・サイズが最小ファイル・サイズしきい値要件を満たすときにボリュームの書き込み範囲を追跡します。変更されたバイト・オフセットと長さ範囲情報を、特定のファイルに照らして照会できます。

書き込み範囲追跡を有効にする要件は次のとおりです。

- Windows Server 2012 R2 以降
- NTFS バージョン 3.0 以降

変更されたバイトの追跡には、以下のテクノロジーはサポートされません。

- Resilient File System (ReFS)
- Server Message Block (SMB) 3.0 プロトコル
- SMB TFO (Transparent Failover)
- スケールアウト・ファイル共有 (SO) を使用する SMB 3.0

デフォルトで、512 MB のスペースが USN 変更ジャーナリングに割り振られます。さらに、ジャーナル・オーバーフローが検出されると、ビジー・ファイル・システムを管理するために 2 GB のジャーナル・サイズが割り振られます。

シャドー・コピー・ストレージに必要な最小スペースは 100 MB ですが、アクティビティーが 増えたシステムではさらに多くのスペースが必要になる場合があります。SQL Server エージェントはソース・ボリューム・スペースを確認します。その結果、ソース・ボリューム上のフリー・スペースが 100 MB 未満である場合には、バックアップが失敗します。フリー・スペースが 10% 未満になるとジョブ・ログに警告メッセージが表示されてから、バックアップが続行します。

以下の条件が検出されると、基本バックアップが強制されます。

- ログが最大サイズに達したか、ジャーナリングを無効にしたか、またはカタログされた USN ID を変更したために、ジャーナルの不連続が報告される。
- ファイル・サイズが、追跡されるしきい値サイズ (デフォルトで 1MB) 以下である。
- 前のバックアップ・ジョブ後にファイルが追加される。

ログ・バックアップ

ログ・ファイルを vSnap リポジトリーにコピーする前に、IBM Spectrum Protect Plus は SQL Server インスタンス用に構成されたバックアップ・フォルダーを使用してログのコレクションをステージングします。バックアップ・ジョブ間のトランザクション・ログを保管するために十分なフリー・スペースが必要です。ステージング域は、SQL Server Management Studio (SSMS) を使用してバックアップ・フォルダー構成を変更することによって変更できます。

SQL Server ログ・バックアップが確実に正しく機能するためには、Windows グループ・ポリシーの変更が必要な場合があります。

「**コンピュータの構成**」 > 「**Windows の設定**」 > 「**セキュリティの設定**」 > 「**ローカルポリシー**」 > 「**セキュリティオプション**」にある「**ネットワークセキュリティ: LAN マネージャ認証レベル**」ポリシーのグループポリシーオブジェクト (GPO) 設定を、以下のいずれかのオプションに設定する必要があります。

- **未定義**
- **NTLMv2 応答のみ送信する**
- **NTLMv2 応答のみ送信する (LM を拒否する)**
- **NTLMv2 応答のみ送信する (LM と NTLM を拒否する)**

「**NTLM 応答のみ送信**」オプションは、vSnap CIFS または SMB のバージョンと互換性がなく、CIFS 認証の問題を引き起こす可能性があります。

SQL Server AlwaysOn 可用性グループの構成

SQL Server Management Studio を使用して、バックアップ操作の優先インスタンスを構成します。 以下のステップを実行してください。

1. **可用性グループ**・ノードを選択します。
2. 構成したい可用性グループを選択してから、「**プロパティ**」を選択します。
3. 「**可用性グループのプロパティ**」ダイアログ・ボックスで、「**バックアップの設定**」を選択します。

「**バックアップを実行する場所**」ペインで任意のオプションを選択します。2 次レプリカが優先され、複数の 2 次レプリカが使用可能である場合、IBM Spectrum Protect Plus ジョブ実行プログラムは、IBM Spectrum Protect Plus SQL Server エージェントによって報告される優先リスト内の最初の 2 次レプリカを選択します。

SQL Server エージェントは、VSS バックアップ・タイプを COPY_ONLY に設定します。

登録および認証

IBM Spectrum Protect Plus に各 SQL Server を名前または IP アドレスで登録します。SQL Server Cluster (AlwaysOn) ノードを登録する場合、各ノードを名前または IP アドレスで登録します。IP アドレスは公開であり、ポート 5985 で listen する必要があります。完全修飾ドメイン名は解決可能であり、IBM Spectrum Protect Plus アプライアンスからルーティング 可能でなければなりません。

ユーザー ID には、「**サービスとしてログオン**」権限を含めて、ノード上で IBM Spectrum Protect Plus Tools Service をインストールして開始できる十分な権限が必要です。 詳しくは、Microsoft Web サイトで記事 Add the Log on as a service Right to an Account を参照してください。

仮想マシンがドメインに接続されている場合、ユーザー ID はデフォルトの *domain¥Name* 形式に従います。ユーザーがローカル管理者である場合は、*local administrator* 形式が使用されます。

Kerberos

Kerberos ベースの認証は、IBM Spectrum Protect Plus アプライアンスの構成ファイルを指定することで、有効にすることができます。この設定により、デフォルトの Windows NTLM プロトコルが指定変更されます。

Kerberos ベースの認証の場合に限り、ユーザー ID は `username@FQDN` 形式で指定する必要があります。完全修飾ドメイン名で指定されたドメイン上の鍵配布センター (KDC) から発券許可証 (TGT) を取得するには、ユーザー名は、登録済みのパスワードを使用して認証できなければなりません。

特権

SQL Server の IBM Spectrum Protect Plus エージェント・ユーザーには、以下の許可が必要です。

- SQL Server の `public` 許可と `sysadmin` 許可
- Windows ローカル管理許可 (VSS フレームワークで必要) と、ボリュームおよびディスクのアクセス権
- SQL Server AlwaysOn および SQL Server FCI 環境でクラスター・リソースにアクセスする許可

各 SQL Server インスタンスは、特定のユーザー・アカウントを使用して、その SQL Server インスタンスのリソースにアクセスすることができます。

SQL Server データベースと対話し、バックアップおよびリストア操作をログに記録するには、SQL Server VDI ベースのフレームワークが使用されます。VDI 接続には SQL Server の `sysadmin` 許可が必要です。リストアされたデータベースの所有者は元の所有者に変更されません。リストアされたデータベースの所有者を変更するには、手動のステップが必要です。VDI フレームワークについて詳しくは、Microsoft の記事 SQL Server VDI backup and restore operations require Sysadmin privileges を参照してください。

ターゲット SQL Server サービス・アカウントには、SQL Server リストア・ファイルにアクセスする許可が必要です。Microsoft の記事 Securing Data and Log Files で『Administrative Considerations』セクションを参照してください。

Windows タスク・スケジューラーはログ・バックアップをスケジュールするために使用されます。環境によっては、ユーザーに次のエラーが表示されることがあります: 指定されたログオン・セッションは存在しません。すでに終了している可能性があります。このエラーは、ネットワーク・アクセス・グループ・ポリシー設定を無効にする必要があることが原因で発生します。この GPO を無効にする方法について詳しくは、Microsoft サポートの記事 (指定されたログオン・セッションは存在しません。すでに終了している可能性があります。DFS 共有のネットワーク・ドライブにマップしようとしたときのエラー) を参照してください。

ポート

IBM Spectrum Protect Plus エージェントは、以下のポートを使用します。「Accept」で示されるポートは、セキュア接続 (HTTPS または SSL) を使用します。

表 *17.* 着信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	ファイアウォール	サービス	説明
5985	TCP	Accept	WinRM	Windows Remote Management Service
5986	TCP	Accept	WinRM	Secure Windows Remote Management Service

表 18. 発信 *IBM Spectrum Protect Plus* エージェント・ファイアウォール接続

ポート	プロトコル	サービス	説明
3260 このノードには iSCSI イニシエーターが必要です。	TCP	vSnap iSCSI	バックアップ操作とリカバリー操作用に LUNS をマウントするのに使用される iSCSI vSnap ターゲット・ポート。
137	UDP	vSnap SMB/CIFS	トランザクション・ログのバックアップ操作とリカバリー操作用にファイル・システム共有をマウントするのに使用される、vSnap SMB/CIFS ターゲット・ポート。
138	UDP	vSnap SMB/CIFS	トランザクション・ログのバックアップ操作とリカバリー操作用にファイル・システム共有をマウントするのに使用される、vSnap SMB/CIFS ターゲット・ポート。
139	TCP	vSnap SMB/CIFS	トランザクション・ログのバックアップ操作とリカバリー操作用にファイル・システム共有をマウントするのに使用される、vSnap SMB/CIFS ターゲット・ポート。
443	TCP	HTTPS	ログ・バックアップの障害が発生した場合にアラートを送信するために、SQL Server が IBM Spectrum Protect Plus と通信できるようにします。
445	TCP	vSnap SMB/CIFS	トランザクション・ログのバックアップ操作とリカバリー操作用にファイル・システム共有をマウントするのに使用される、vSnap SMB/CIFS ターゲット・ポート。

IBM Spectrum Protect Plus インストール・パッケージの入手

IBM Spectrum Protect Plus インストール・パッケージは、IBM ダウンロード・サイト (パスポート・アドバンテージや Fix Central など) から入手できます。これらのパッケージには、IBM Spectrum Protect Plus コンポーネントのインストールまたは更新に必要なファイルが含まれています。

始める前に
コンポーネント別のインストール・パッケージのリスト、およびファイルのダウンロード・サイトへのリンクについては、技術情報 879861 を参照してください。

手順

適切なインストール・ファイルをダウンロードします。

VMware システムおよび Microsoft Hyper-V システムへのインストール用に、別のインストール・ファイルが提供されています。ご使用の環境に合わせて、必ず正しいファイルをダウンロードしてください。

重要 : インストール・ファイルまたは更新ファイルの名前を変更しないでください。インストール・プロセスまたは更新プロセスがエラーなしで完了するには、オリジナルのファイル名が必要です。

関連概念

83 ページの『IBM Spectrum Protect Plus コンポーネントの更新』
IBM Spectrum Protect Plus 仮想アプライアンス、vSnap サーバー、および VADP プロキシー・サーバーを更新して、最新の機能や機能拡張を取得することができます。 ソフトウェア・パッチや更新のインストールには、IBM Spectrum Protect Plus 管理コンソール、またはこれらのコンポーネントのコマンド・ライン・インターフェースを 使用します。

関連タスク

44 ページの『VMware 仮想アプライアンスとしての IBM Spectrum Protect Plus のインストール』
IBM Spectrum Protect Plus を VMware 環境にインストールするには、Open Virtualization Format (OVF) テンプレートをデプロイします。OVF テンプレートをデプロイすると、アプリケーションが含まれている仮想アプライアンスが ESXi サーバーなどの VMware ホスト上に作成されます。

46 ページの『Hyper-V 仮想アプライアンスとしての IBM Spectrum Protect Plus のインストール』
IBM Spectrum Protect Plus を Microsoft Hyper-V 環境にインストールするには、Hyper-V テンプレート用に IBM Spectrum Protect Plus をインポートします。テンプレートをインポートすると、IBM Spectrum Protect Plus アプリケーションを含む仮想アプライアンスが Hyper-V 仮想マシン上に作成されます。すでに名前が付けられて登録されているローカルの vSnap サーバーも、その仮想アプライアンス上にインストールされます。

53 ページの『vSnap サーバーのインストール』
IBM Spectrum Protect Plus アプライアンスをデプロイすると、vSnap サーバーが自動的にインストールされます。このサーバーは 1 次バックアップの宛先になります。大規模なエンタープライズ環境では、追加の vSnap サーバーが必要になる場合があります。

VMware 仮想アプライアンスとしての IBM Spectrum Protect Plus のインストール

IBM Spectrum Protect Plus を VMware 環境にインストールするには、Open Virtualization Format (OVF) テンプレートをデプロイします。OVF テンプレートをデプロイすると、アプリケーションが含まれている仮想アプライアンスが ESXi サーバーなどの VMware ホスト上に作成されます。

始める前に

以下のタスクを実行してください。

- 11 ページの『コンポーネントの要件』および 22 ページの『ハイパーバイザー要件』に記載されている IBM Spectrum Protect Plus システム要件を確認します。
- パスポート・アドバンテージ・オンラインから仮想アプライアンス・テンプレート・インストール・ファイル `CC1QCML.ova` をダウンロードします。ファイルのダウンロードについては、技術情報 879861 を参照してください。
- ダウンロードしたテンプレート・インストール・ファイルの MD5 チェックサムを検証します。生成されたチェックサムが、ソフトウェア・ダウンロードの一部である MD5 チェックサム・ファイルに提供されているものと一致していることを確認してください。
- デプロイメント時に、VMware ユーザー・インターフェースからネットワーク・プロパティーを入力するようプロンプトが表示されます。静的 IP アドレス構成を入力するか、またはすべてのフィールドをブランクにすると DHCP 構成を使用できます。
- デプロイメント後に静的 IP アドレスを再割り当てするには、NetworkManager テキスト・ユーザー・インターフェース (nmtui) ツールを使用できます。詳しくは、48 ページの『静的 IP アドレスの割り当て』を参照してください。

以下の考慮事項に注意してください。

- IBM Spectrum Protect Plus をデプロイする予定の VM ネットワークに関連付けられている IP アドレス・プールの構成が必要な場合があります。IP アドレス・プールの正しい構成は、IP アドレス範囲 (使用されている場合)、ネットマスク、ゲートウェイ、DNS 検索ストリング、および DNS サーバー IP アドレスのセットアップから成ります。
- ユーザー介入によって、あるいは DNS を使用して新しい IP アドレスが取得されて、デプロイメント後に IBM Spectrum Protect Plus アプライアンスのホスト 名が変更された場合、IBM Spectrum Protect Plus アプライアンスは 再始動する必要があります。
- デプロイメント前に、デフォルトのゲートウェイを適切に構成する必要があります。複数の DNS ストリングがサポートされており、スペースを使用せずにコンマで区切る必要があります。
- vSphere の新しいバージョンでは、IBM Spectrum Protect Plus アプライアンスをデプロイするのに、vSphere Web クライアントが必要な場合があります。
- IBM Spectrum Protect Plus は、IPv6 環境についてはテストされていません。

手順

IBM Spectrum Protect Plus を仮想アプライアンスとしてインストールするには、以下のステップを実行してください。

1. 以下のいずれかのアクションを実行して、IBM Spectrum Protect Plus をデプロイします。
   a) vSphere Client を使用している場合は、「**アクション**」メニューから、「**OVF テンプレートのデプロイ**」をクリックします。
   b) vSphere Web クライアントを使用している場合は、「**VM の作成/登録**」をクリックしてから、「**OVF ファイルまたは OVA ファイルから仮想マシンをデプロイ**」を選択します。
2. 仮想アプライアンスを実行するための ESXi リソースを選択します。「**次へ**」をクリックします。
3. 詳細を確認します。「**次へ**」をクリックします。

   重要 :

   vSphere Web クライアントを使用する場合は、`disk.enableUUID = true` が「**追加構成**」に含まれていることを確認してください。含まれていない場合、または vSphere Client を使用する場合は、インストール手順に進んで、後で vSphere Web クライアントからこのオプションを 有効にしてください。
4. `CC1QCML.ova` ファイルの場所を指定して、そのファイルを選択します。「**次へ**」をクリックします。
5. テンプレートにわかりやすい名前を付けます。この名前が仮想マシンの名前になります。 仮想マシンをデプロイするのに適した場所を指定します。「**次へ**」をクリックします。
6. 仮想アプライアンスをインストールするストレージを 選択します。このストレージのデータ・ストアが、宛先ホストで構成されている必要があります。仮想アプライアンス 構成ファイルおよび仮想ディスク・ファイルがその中に格納されます。ストレージが、仮想アプライアンスとそれに関連付けられた仮想ディスク・ファイルを入れるための十分な大きさであることを確認してください。仮想ディスクのディスク・フォーマットを選択します。シック・プロビジョニングを使用すると、仮想アプライアンスのパフォーマンスが向上します。シン・プロビジョニングでは、パフォーマンスは犠牲になりますが、使用ディスク・スペースは少なくて済みます。「**次へ**」をクリックします。
7. テンプレートの詳細を読み、エンド・ユーザーご使用条件を受け入れます。vSphere Client の「**I accept all license agreements**」にチェック・マークを付けるか、vSphere Web Client の「**Accept**」をクリックします。 「**次へ**」をクリックします。
8. デプロイされたテンプレートが使用するネットワークを選択します。「**宛先ネットワーク**」をクリックすると、ESXi サーバー上の使用可能な複数のネットワークが選択可能になる場合があります。仮想マシン・デプロイメントのための適切な IP アドレスの割り振りを定義できるようにする宛先ネットワークを選択してください。「**次へ**」をクリックします。
9. vSphere Web クライアントの場合は、仮想アプライアンスのプロパティー 値 (DNS、デフォルト・ゲートウェイ、ドメイン、ネットワーク IP アドレス、およびネットワーク接頭部) を入力します。静的 IP アドレスは指定することができます。ブランクのままにすると、DHCP サーバーで割り当てられた動的 IP アドレスが使用されます。ネットワーク接頭部の入力は、クラスレス・ドメイン間ルーティング (CIDR) 表記を使用して行う必要があります。有効値は 1 から 24 です。「**次へ**」をクリックします。

注 : vSphere Client の場合、これらのプロパティーは NetworkManager テキスト・ユーザー・インターフェース (nmtui) ツールを使用して構成することができます。また、このコマンドを使用して「検索ドメイン」フィールドの情報を追加できます。詳しくは、静的 IP アドレスの割り当を参照してください。

10. テンプレート設定を確認します。「**完了**」をクリックしてウィザードを終了し、OVF テンプレートのデプロイメントを開始します。
11. OVF テンプレートがデプロイされた後で、新たに作成された VM の電源を入れます。VM の電源オンは、vSphere Client から行えます。

    重要 : IBM Spectrum Protect Plus が完全に初期化するまで数分待ちます。

次のタスク

仮想アプライアンスがデプロイされると、IBM Spectrum Protect Plus アプリケーションとそれに組み込まれたローカル vSnap サーバーが自動的に登録されてインストールされます。IBM Spectrum Protect Plus を始動するには、以下の手順を実行します。

アクション	方法
VMware Remote Console または SSH を使用して、IBM Spectrum Protect Plus 仮想アプライアンスのコンソールに接続します。NetworkManager テキスト・ユーザー・インターフェース (nmtui) を使用して、ネットワーク構成をセットアップします。	静的 IP アドレスの割り当てを参照してください。
製品キーをアップロードします。	49 ページの『製品キーのアップロード』を参照してください。
サポートされている Web ブラウザーから IBM Spectrum Protect Plus を始動します。	71 ページの『IBM Spectrum Protect Plus の始動』を参照してください。

Hyper-V 仮想アプライアンスとしての IBM Spectrum Protect Plus のインストール

IBM Spectrum Protect Plus を Microsoft Hyper-V 環境にインストールするには、Hyper-V テンプレート用に IBM Spectrum Protect Plus をインポートします。テンプレートをインポートすると、IBM Spectrum Protect Plus アプリケーションを含む仮想アプライアンスが Hyper-V 仮想マシン上に作成されます。すでに名前が付けられて登録されているローカルの vSnap サーバーも、その仮想アプライアンス上にインストールされます。

始める前に

以下のタスクを実行してください。

- 11 ページの『コンポーネントの要件』および 22 ページの『ハイパーバイザー要件』に記載されている IBM Spectrum Protect Plus システム要件を確認します。
- パスポート・アドバンテージ・オンラインから インストール・ファイル CC1QDML.exe をダウンロードします。ファイルのダウンロードについては、技術情報 879861 を参照してください。
- 追加の Hyper-V システム要件を確認します。Windows サーバー上の HYPER-V のシステム要件を参照してください。
- ダウンロードしたテンプレート・インストール・ファイルの MD5 チェックサムを検証します。生成されたチェックサムが、ソフトウェア・ダウンロードの一部である、MD5 チェックサム・ファイルに提供されているものと一致していることを確認してください。
- ユーザー介入によって、あるいは DNS を使用して新しい IP アドレスが取得されて、デプロイメント後に IBM Spectrum Protect Plus 仮想アプライアンスのホスト名が変更された場合、IBM Spectrum Protect Plus 仮想アプライアンスを再始動する必要があります。

- クラスター・ノードなど、すべての Hyper-V サーバーでは、そのサービス・リストで Microsoft iSCSI Initiator Service が実行されている必要があります。サーバーの始動時にこのサービスが実行を開始するように、このサービスの開始タイプを「自動」に設定します。
- インストール・プロセスの実行時に特定のステップを完了するには、管理特権が必要な場合があります。

手順

IBM Spectrum Protect Plus を仮想アプライアンスとしてインストールするには、以下のステップを実行してください。

1. CC1QDML.exe ファイルをご使用の Hyper-V サーバーにコピーします。
2. インストーラーを開き、セットアップ・ウィザードを実行します。
3. Hyper-V マネージャーを開いて、必要なサーバーを選択します。
4. Hyper-V マネージャーの「**アクション**」ペインで、「**仮想マシンのインポート**」をクリックします。「仮想マシンのインポート」ウィザードが開きます。「**次へ**」をクリックします。
5. 「**フォルダーを検索 (Locate Folder)**」ステップで、「**参照...**」をクリックし、インストール時に指定したフォルダーに移動します。「**SPP-{release}**」が含まれているフォルダーを選択します。「**次へ**」をクリックします。
6. 「**仮想マシンの選択**」ステップで、仮想マシンの「**SPP-{release}**」が選択されていることを確認してから、「**次へ**」をクリックします。「**インポート・タイプの選択**」ダイアログが開きます。
7. 「**インポート・タイプの選択**」ステップで、「**仮想マシンを同所に登録 (既存の固有 ID を使用) (Register the virtual machine in-place (use the existing unique ID))**」を選択します。「**次へ**」をクリックします。

   重要 : 1 つの Hyper-V サーバーに複数の IBM Spectrum Protect Plus 仮想アプライアンスをインポートしないでください。
8. 「**ネットワークの接続**」ステップで、使用する仮想スイッチへの接続を設定します。「**次へ**」をクリックします。
9. 「**要約**」ステップで、「説明」を表示します。「**完了**」をクリックして「仮想マシンのインポート」ウィザードを閉じます。
10. Hyper-V マネージャーで、**SPP-{release}** という名前の新規仮想マシンを探します。この仮想マシンを右クリックし、「**設定**」をクリックします。
11. この仮想マシンの「設定」ダイアログが開きます。左側のペインで、「**ハードウェア**」 **>** 「**IDE コントローラー 0**」 **>** 「**ハードウェア・ドライブ**」をクリックします。
12. 「メディア」セクションで、正しい仮想ハード・ディスクが選択されていることを確認します。オリジナルの仮想ディスクのファイル名に注意してください。「**編集**」をクリックします。
13. 「仮想ハード・ディスクの編集」ウィザードが開きます。「**アクションの選択**」ステップに進みます。
14. 「**アクションの選択**」ステップで、「**変換**」をクリックしてから「**次へ**」をクリックします。
15. 「**ディスク・フォーマットの選択 (Choose Disk Format)**」ステップで、「**VHDX**」が選択されていることを確認します。「**次へ**」をクリックします。
16. 「**ディスク・タイプの選択**」ステップでは、「**固定サイズ**」をクリックします。 「**次へ**」をクリックします。
17. 「**ディスクの構成**」ステップでは、IBM Spectrum Protect Plus 仮想アプライアンスの仮想ディスク・ファイルを格納するフォルダーを検索します。ステップ 12 でメモしたものと同じファイル名を再使用してください。ステップ 2 と同じインストール・ディレクトリーを再使用する場合は、別の名前を使用してください。「**次へ**」をクリックします。

    重要 : フォルダーが常駐するディスク・ドライブに、固定サイズの仮想ディスク・ファイルを入れるための十分なディスク・スペースがあることを確認してください。
18. 「**要約**」ステップで、「説明」を表示します。「**完了**」をクリックすると、「仮想ハード・ディスクの編集 (Edit Virtual Hard Disk)」ウィザードが閉じ、仮想ディスクの変換が開始されます。処理が完了すると、オリジナルの仮想ハード・ディスク・ファイルは削除されます。
19. 仮想マシンの「設定」ダイアログで、「**参照**」をクリックします。前のステップで新規作成された仮想ハード・ディスク (VHDX) ファイルを開きます。

20. 「**ハードウェア**」 > 「**SCSI コントローラー**」の下で、各ハード・ディスクについてステップ 12 から 19 までを繰り返します。「**OK**」をクリックして、「設定」ダイアログを閉じます。
21. Hyper-V マネージャーで、仮想マシンを右クリックし、「**開始**」をクリックします。
22. 新規仮想マシンのアドレスが自動的に割り当てられる場合は、Hyper-V マネージャーを使用して IP アドレスを識別します。仮想マシンに静的 IP を割り当てるには、NetworkManager テキスト・ユーザー・インターフェース (nmtui) ツールを使用します。

    詳しくは、48 ページの『静的 IP アドレスの割り当て』を参照してください。

次のタスク

仮想アプライアンスをインストールした後で、以下のアクションを実行します。

アクション	方法
仮想アプライアンスを再始動します。	仮想アプライアンスの資料を参照してください。
製品キーをアップロードします。	49 ページの『製品キーのアップロード』を参照してください。
サポートされている Web ブラウザーから IBM Spectrum Protect Plus を始動します。	71 ページの『IBM Spectrum Protect Plus の始動』を参照してください。

静的 IP アドレスの割り当て

最初のデプロイメント後に新しい静的 IP アドレスを再割り当てするには、ネットワーク管理者が NetworkManager テキスト・ユーザー・インターフェース (nmtui) ツールを使用して静的 IP アドレスを割り当てることができます。nmtui を実行するには、sudo 特権が必要です。

手順

新しい静的 IP アドレスを再割り当てするには、IBM Spectrum Protect Plus 仮想マシンの電源がオンになっていることを確認して、以下のステップを実行します。

1. ユーザー ID **serveradmin** で仮想マシン・コンソールにログオンします。

   初期パスワードは sppDP758 です。
2. CentOS コマンド・ラインで、nmtui と入力してインターフェースを開きます。
3. メインメニューで、「**接続の編集**」を選択してから、「**OK**」をクリックします。
4. ネットワーク接続を選択してから、「**編集**」をクリックします。
5. 「**接続の編集**」画面で、まだ使用されていない使用可能な静的 IP アドレスを入力します。
6. 「**OK**」をクリックして静的 IP 構成を保存してから、IBM Spectrum Protect Plus アプライアンスを再始動します。

関連タスク

44 ページの『VMware 仮想アプライアンスとしての IBM Spectrum Protect Plus のインストール』
IBM Spectrum Protect Plus を VMware 環境にインストールするには、Open Virtualization Format (OVF) テンプレートをデプロイします。OVF テンプレートをデプロイすると、アプリケーションが含まれている仮想アプライアンスが ESXi サーバーなどの VMware ホスト上に作成されます。

46 ページの『Hyper-V 仮想アプライアンスとしての IBM Spectrum Protect Plus のインストール』
IBM Spectrum Protect Plus を Microsoft Hyper-V 環境にインストールするには、Hyper-V テンプレート用に IBM Spectrum Protect Plus をインポートします。テンプレートをインポートすると、IBM Spectrum Protect Plus アプリケーションを含む仮想アプライアンスが Hyper-V 仮想マシン上に作成されます。すでに名前が付けられて登録されているローカルの vSnap サーバーも、その仮想アプライアンス上にインストールされます。

製品キーのアップロード

IBM Spectrum Protect Plus は、一定の期間、評価モードで実行します。IBM Spectrum Protect Plus 機能を無制限に使用可能にするためには、有効な製品キーが必要です。

始める前に
インターネットにアクセスできるコンピューターに対する製品キーを保管し、そのキーの場所を記録してください。

手順

製品キーをアップロードするには、以下のステップを実行します。

1. サポートされているブラウザーで、次の URL を入力します。

   ```
   https://HOSTNAME:8090/
   ```

   ここで、*HOSTNAME* は、アプリケーションがデプロイされている 仮想マシンの IP アドレスです。
2. ログイン・ウィンドウで、「**認証タイプ**」 > 「**システム**」を選択します。パスワード `serveradmin` を入力して、管理コンソールにアクセスします。デフォルトのパスワードは `sppDP758` です。

   最初のログイン時に、管理コンソールにアクセスするために新規パスワードを入力するようプロンプトが表示されます。
3. 「**ライセンスの管理**」をクリックします。
4. 「**ファイルの選択**」をクリックしてから、ご使用のコンピューター上の製品キーを参照します。
5. 「**新規ライセンスのアップロード**」をクリックします。
6. 「**ログアウト**」をクリックします。

次のタスク
製品キーをアップロード後、以下のアクションを実行します。

アクション	方法
サポートされている Web ブラウザーから IBM Spectrum Protect Plus を始動します。	71 ページの『IBM Spectrum Protect Plus の始動』を参照してください。

ファイアウォール・ポートの編集

提供されている例を、リモート VADP プロキシー・サーバーまたはアプリケーション・サーバーでファイアウォール・ポートを開く場合の参照として使用してください。ポート・トラフィックは必要なネットワークまたはアダプターのみに制限する必要があります。

Red Hat Enterprise Linux 7 以降、および CentOS 7 以降

リモート VADP プロキシー・サーバーまたはアプリケーション ・サーバーでポートを開く

開くポートをリストするには、以下のコマンドを使用します。

```
firewall-cmd --list-ports
```

ゾーンをリストするには、以下のコマンドを使用します。

```
firewall-cmd --get-zones
```

イーサネット・ポート `eth0` を含むゾーンをリストするには、以下のコマンドを使用します。

```
firewall-cmd --get-zone-of-interface=eth0
```

TCP トラフィック用のポート *8098* を開くには、以下のコマンドを使用します。このコマンドは永続的なものではありません。

```
firewall-cmd --add-port 8098/tcp
```

ファイアウォール規則を再始動した後で、TCP トラフィック用のポート *8098* を開くには、以下のコマンドを使用します。変更内容を保持するには、このコマンドを使用します。

```
firewall-cmd --permanent --add-port 8098/tcp
```

ポートへの変更を元に戻すには、このコマンドを使用します。

```
firewall-cmd --remove-port 8098/tcp
```

一連のポートを開くには、以下のコマンドを使用します。

```
firewall-cmd --permanent --add-port 60000-61000/tcp
```

ファイアウォールの更新内容をファイアウォール規則に再ロードするには、以下のコマンドを使用します。

```
firewall-cmd --reload
```

SUSE Linux Enterprise Server 12

「**セキュリティーおよびユーザー**」メニューから SUSE Linux Enterprise Server 12 拡張セキュリティー・ファイアウォール・オプションを編集します。必要な新しいポート範囲を指定して、変更を適用します。

IP テーブルを使用するファイアウォール構成

iptables ユーティリティーは、ほとんどの Linux ディストリビューションで、ファイアウォール規則およびポリシー設定を有効にするために使用できます。これらの Linux ディストリビューションには、Red Hat Enterprise Linux 6.8、Red Hat Enterprise Linux 7 以降、CentOS 7 以降、および SUSE Linux Enterprise Server 12 が含まれます。これらのコマンドを使用する前に、デフォルトで有効になっているファイアウォール・ゾーンを確認してください。ゾーン設定に応じて、必要な規則のゾーンと一致するように INPUT および OUTPUT の項の名前変更が必要になる場合があります。

Red Hat Enterprise Linux 7 以降の場合は、以下のコマンド例を参照してください。

現行のファイアウォール・ポリシーをリストするには、以下のコマンドを使用します。

```
sudo iptables -S sudo iptables -L
```

内部サブネット *<172.31.1.0/24>* からインバウンド TCP トラフィックのポート *8098* を開くには、以下のコマンドを使用します。

```
sudo iptables -A INPUT -p tcp -s 172.31.1.0/24 --dport 8098 -j ACCEPT
```

内部サブネット *<172.31.1.0/24>* へのアウトバウンド TCP トラフィックのポート *8098* を開くには、以下のコマンドを使用します。

```
sudo iptables -A OUTPUT -p tcp -d 172.31.1.0/24 --sport 8098 -j ACCEPT
```

外部サブネット *<10.11.1.0/24>* へのアウトバウンド TCP トラフィック用で、イーサネット・ポート・アダプター eth1 専用のポート *8098* を開くには、以下のコマンドを使用します。

```
sudo iptables -A OUTPUT -o eth1 -p tcp -d 10.11.1.0/24 --sport 8098 -j ACCEPT
```

一連の CES IP アドレス (10.11.1.5 から 10.11.1.11) へのインバウンド TCP トラフィック用で、イーサネット・ポート・アダプター eth1 専用のポート *8098* を開くには、以下のコマンドを使用します。

```
sudo iptables -A INPUT -i eth1 -p tcp -m iprange --dst-range
10.11.1.5-10.11.1.11 --dport 8098 -j ACCEPT
```

内部ネットワークのイーサネット・ポート・アダプター eth1 が外部ネットワークのイーサネット・ポート・アダプター eth0 と通信できるようにするには、以下のコマンドを使用します。

sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT。このサンプルは、Red Hat Enterprise Linux 7 以降に固有のものです。

パブリック・ゾーン内のイーサネット・ポート eth1 で、サブネット *10.18.0.0/24* からインバウンド・トラフィックのポート *8098* を開くには、以下のコマンドを使用します。

```
iptables -A IN_public_allow -i eth1 -p tcp -s 10.18.0.0/24 --dport 8098 -j
ACCEPT
```

ファイアウォール規則の変更を保存して、ファイアウォールの再起動プロセス後も保持されるようにするには、以下のコマンドを使用します。

```
sudo iptables-save
```

Uncomplicated Firewall (UFW) の開始と停止を行うには、以下のコマンドを使用します。

```
service iptables stop service iptables start
```

第 3 章 vSnap サーバーのインストールおよび構成

IBM Spectrum Protect Plus の各インストールには、1 次バックアップの宛先である vSnap サーバーが 1 つ以上必要です。

VMware 環境と Hyper-V 環境の両方で、IBM Spectrum Protect Plus アプライアンスが最初にデプロイされるときに、 名前が localhost という 1 つの vSnap サーバーが自動的にインストールされます。内蔵の vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスの区画に常駐し、IBM Spectrum Protect Plus で登録され、初期化されます。小規模なバックアップ環境では、内蔵の vSnap サーバーで十分です。

大規模なエンタープライズ環境では、追加の vSnap サーバーが必要になる場合があります。IBM Spectrum Protect Plus 環境における vSnap サーバーとその他のコンポーネントのサイジング、ビルド、および配置のガイダンスについては、IBM Spectrum Protect Plus Blueprints を参照してください。

IBM Spectrum Protect Plus アプライアンスがインストールされ、デプロイされた後、追加の vSnap サーバーを仮想アプライアンスまたは物理アプライアンスにいつでもインストールできます。インストール後、これらのスタンドアロン vSnap サーバーにはいくつかの登録と構成のステップが必要です。

スタンドアロン vSnap サーバーをセットアップするプロセスは次のとおりです。

1. vSnap サーバーをインストールします。
2. vSnap サーバーをディスク・ストレージとして IBM Spectrum Protect Plus に追加します。
3. システムを初期化し、ストレージ・プールを作成します。

vSnap サーバーのインストール

IBM Spectrum Protect Plus アプライアンスをデプロイすると 、vSnap サーバーが自動的にインストールされます。このサーバーは 1 次バックアップの宛先になります。大規模なエンタープライズ環境では、追加の vSnap サーバーが必要になる場合があります。

始める前に

以下のステップを実行してください。

1. 11 ページの『コンポーネントの要件』で vSnap のシステム要件を確認します。
2. インストール・パッケージをダウンロードします。物理マシンにインストールするか仮想マシンにインストールするかに応じて、異なるインストール・ファイルが用意されています。ご使用の環境に合わせて、必ず正しいファイルをダウンロードしてください。ファイルのダウンロードについて詳しくは、技術情報 879861 を参照してください。

物理 vSnap サーバーのインストール

物理マシンに vSnap サーバーをインストールするには、物理 vSnap インストールをサポートする Linux オペレーティング・システムが必要です。

手順

1. 物理的 vSnap インストールをサポートする Linux オペレーティング・システムをインストールします。サポートされるオペレーティング・システムについては、15 ページの『vSnap サーバーの物理インストール要件』を参照してください。

   最小インストール構成でも十分ですが、グラフィカル・ユーザー・インターフェース (GUI) を含む追加パッケージをインストールすることもできます。インストール後に、ルート区画に少なくとも 8 GB のフリー・スペースが必要です。
2. `/etc/selinux/config` ファイルを編集して、SELinux モードを Permissive に変更します。
3. 再起動せずに設定をすぐに適用するには、`setenforce 0` を実行します。

© Copyright IBM Corp. 2017, 2019

4. vSnap インストール・ファイル CC1QGML.run をパスポート・アドバンテージ・オンラインからダウンロードします。ファイルのダウンロードについては、技術情報 879861 を参照してください。
5. コマンド chmod +x *file_name*.run を使用してファイルを実行可能にしてから、実行可能ファイルを実行します。vSnap パッケージと、必要なすべてのコンポーネントがインストールされます。

次のタスク

vSnap サーバーをインストールした後、以下のアクションを実行してください。

アクション	ハウツー
IBM Spectrum Protect Plus に vSnap サーバーを追加し、vSnap 環境を構成する。	56 ページの『vSnap サーバーの管理』を参照してください。

VMware 環境での仮想 vSnap サーバーおよび VADP プロキシーのインストール

VMware 環境で仮想 vSnap サーバーおよび vStorage API for Data Protection (VADP) プロキシーをインストールするには、Open Virtualization Format (OVF) テンプレートをデプロイします。このテンプレートにより、vSnap サーバーおよび VADP プロキシーを含むマシンが作成されます。

始める前に

ネットワーク管理を容易にするために、仮想マシンの静的 IP アドレスを使用します。NetworkManager テキスト・ユーザー・インターフェース (nmtui) ツールを使用して、アドレスを割り当てます。説明については 48 ページの『静的 IP アドレスの割り当て』を参照し、ネットワーク・プロパティーを構成する場合はネットワーク管理者と連携して作業してください。

手順

1. サーバー・テンプレートおよびプロキシー・テンプレートのインストール・ファイル CC1QEML.ova をパスポート・アドバンテージ・オンラインからダウンロードします。ファイルのダウンロードについては、技術情報 879861 を参照してください。
2. vSnap サーバーをデプロイするには、次のいずれかをアクションを実行します。
   - vSphere Client を使用して vSnap サーバーをデプロイする場合は、「**ファイル**」メニューから「**OVF テンプレートのデプロイ**」をクリックします。
   vSphere Web Client を使用する場合は、「**VM の作成/登録**」をクリックしてから、「**OVF ファイルまたは OVA ファイルから仮想マシンをデプロイ**」をクリックします。「**次へ**」をクリックします。
3. CC1QEML.ova ファイルの場所を指定して、そのファイルを選択します。「**次へ**」をクリックします。
4. テンプレートの詳細を確認して、エンド・ユーザーのご使用条件を受け入れます。「**次へ**」をクリックします。
5. テンプレートにわかりやすい名前を付けます。この名前が仮想マシンの名前になります。仮想マシンをデプロイするのに適した場所を指定します。「**次へ**」をクリックします。
6. デプロイメント先のデータ・センター、サーバー、およびリソース・プールを識別します。ストレージの選択を求めるプロンプトが出されたら、宛先ホストにすでに構成済みのデータ・ストアからストレージを選択します。仮想マシン構成ファイルおよび仮想ディスク・ファイルがデータ・ストアに保管されます。仮想マシンとそのすべての仮想ディスク・ファイルが入る十分な容量のデータ・ストアを選択します。「**次へ**」をクリックします。
7. 仮想ディスクを保管するディスク・フォーマットを選択します。パフォーマンスを最適化するには、シック・プロビジョニング (事前選択されている) を選択します。シン・プロビジョニングは必要なディスク・スペースが少なく済みますが、パフォーマンスに影響を与える場合があります。「**次へ**」をクリックします。
8. デプロイするテンプレートで使用されるネットワークを選択します。宛先ネットワークをクリックすると、ESX サーバーで使用可能な複数のネットワークから選択可能になります。宛先ネットワークを選択すると、仮想マシン・デプロイメント用に適切な IP アドレス割り振りを定義できます。「**次へ**」をクリックします。
9. 仮想マシンのデフォルト・ゲートウェイ、DNS、検索ドメイン、IP アドレス、ネットワーク接頭部、およびマシン・ホスト名のネットワーク・プロパティーを入力します。動的ホスト構成プロトコル (DHCP) 構成を使用する場合は、すべてのフィールドを空白のままにしておいてください。

制約事項 : OVF テンプレートのデプロイメントの前に、デフォルト・ゲートウェイを正しく構成する必要があります。複数の DNS ストリングがサポートされています。各ストリングはスペースを使用せずにコンマで区切る必要があります。

ネットワーク接頭部はネットワーク管理者が指定する必要があります。また、ネットワーク接頭部は CIDR 表記を使用して入力する必要があります。有効値は 1 から 24 です。

10. VADP 構成の詳細 (IBM Spectrum Protect Plus アプライアンスの IP アドレスなど) を指定します。

    ESXi サーバー 5.5 の場合、OVF デプロイメント・テンプレートが「**プロパティー**」ステップに達すると、このプロンプトが表示されます。

    ESXi サーバー 6.0 の場合、OVF デプロイメント・テンプレートが「**テンプレートのカスタマイズ**」ステップに達すると、このプロンプトが表示されます。
11. 「**次へ**」をクリックします。
12. テンプレートの選択内容を確認します。「**完了**」をクリックしてウィザードを終了し、OVF テンプレートのデプロイメントを開始します。デプロイメントには、かなりの時間がかかることがあります。
13. OVF テンプレートをデプロイしたら、新しく作成した仮想マシンの電源をオン入れます。vSphere Client から VM の電源を入れることができます。

    重要 : IBM Spectrum Protect Plus アプリケーションをアクセス可能にするには、VM の電源を入れたままにしておく必要があります。
14. 新規作成した VM の IP アドレスを記録します。

    vSnap サーバーにアクセスして登録するには、この IP アドレスが必要です。IP アドレスを検索するには、vSphere Client で VM をクリックして「**要約**」タブで確認します。

次のタスク

vSnap サーバーをインストールした後、以下のアクションを実行してください。

アクション	ハウツー
IBM Spectrum Protect Plus に vSnap サーバーを追加し、vSnap 環境を構成する。	56 ページの『vSnap サーバーの管理』を参照してください。
VADP 環境を構成する。	110 ページの『VADP プロキシーのオプションの設定』を参照してください。

Hyper-V 環境での仮想 vSnap サーバーのインストール

Hyper-V 環境で vSnap サーバーをインストールするには、Hyper-V テンプレートをインポートします。このテンプレートは、Hyper-V 仮想マシン上に vSnap サーバーを含む仮想アプライアンスを作成します。

始める前に

クラスター・ノードを含むすべての Hyper-V サーバーで、それらサーバーの「サービス」リストにある Microsoft iSCSI イニシエーター・サービスが実行されている必要があります。サービスを「自動」に設定し、マシンを再始動したときにサービスが有効になるようにします。

手順

1. vSnap インストール・ファイル `CC1QFML.exe` をパスポート・アドバンテージ・オンラインからダウンロードします。ファイルのダウンロードについては、技術情報 879861 を参照してください。
2. インストール・ファイルを Hyper-V サーバーにコピーします。
3. インストーラーを起動してインストール手順を実行します。
4. Hyper-V マネージャーを開き、必要なサーバーを選択します。Hyper-V のシステム要件については、Windows サーバー上の HYPER-V のシステム要件を参照してください。
5. Hyper-V マネージャーの「**アクション**」メニューで、「**仮想マシンのインポート**」をクリックしてから、「**次へ**」をクリックします。「**フォルダーを検索**」ダイアログが開きます。

6. 解凍した vSnap フォルダー内にある「Virtual Machines」フォルダーの場所を参照します。「**次へ**」をクリックします。「**仮想マシンの選択**」ダイアログが開きます。
7. vSnap を選択してから「**次へ**」をクリックします。「**インポート・タイプの選択**」ダイアログが開きます。
8. インポート・タイプから「**仮想マシンを所定の場所に登録**」を選択します。 「**次へ**」をクリックします。
9. 「ネットワークの接続」ダイアログが開いたら、使用する仮想スイッチを指定して「**次へ**」をクリックします。「インポートの完了」ダイアログが開きます。
10. 説明を確認してから、「**完了**」をクリックしてインポート・プロセスを完了し、「**仮想マシンのインポート**」ウィザードを閉じます。仮想マシンがインポートされます。
11. 新しくデプロイした VM を右クリックして、「**設定**」をクリックします。
12. 「IDE コントローラー 0」というセクションで、「**ハード・ディスク**」を選択します。
13. 「**編集**」をクリックしてから、「**次へ**」をクリックします。
14. 「**アクションの選択**」画面で、「**変換**」を選択してから「**次へ**」をクリックします。
15. 「ディスク・フォーマット」については、「**VHDX**」を選択します。
16. 「ディスク・タイプ」については、「**固定サイズ**」を選択します。
17. 「ディスクの構成」オプションでは、ディスクに新しい名前を付け、オプションで新規の場所を指定します。
18. 説明を確認してから、「**完了**」をクリックして変換を完了します。
19. 「**参照**」をクリックし、新規作成した VHDX を探して選択します。
20. 「SCSI コントローラー」セクションの各ディスクについて、ステップ 12 から 18 を繰り返します。
21. 「**Hyper-V マネージャー**」から VM の電源をオンにします。プロンプトが表示されたら、カーネルをレスキュー・モードで起動するためのオプションを選択します。
22. 新規仮想マシンの IP アドレスが自動で割り当てられた場合は、Hyper-V マネージャーを使用して IP アドレスを識別します。NetworkManager テキスト・ユーザー・インターフェースを 使用して静的 IP を仮想マシンに割り当てるには、以下のセクションを参照してください。
23. 新規 VM のアドレスが自動的に割り当てられる場合は、Hyper-V マネージャーを使用して IP アドレスを識別します。VM に静的 IP を割り当てるには、NetworkManager テキスト・ユーザー・インターフェース (nmtui) ツールを使用します。手順については、48 ページの『静的 IP アドレスの割り当て』を参照してください。

次のタスク
vSnap サーバーをインストールした後、以下のアクションを実行してください。

アクション	ハウツー
IBM Spectrum Protect Plus に vSnap サーバーを追加し、vSnap 環境を構成する。	56 ページの『vSnap サーバーの管理』を参照してください。

vSnap サーバーの管理

バックアップとリストアのジョブを 有効にするには、少なくとも 1 つの IBM Spectrum Protect Plus 仮想アプライアンスと 少なくとも 1 つの vSnap サーバーが必要です。vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスまたは独自のアプライアンスに配置するか、物理的な vSnap インストール済み環境を使用することもできます。vSnap サーバーのロケーションは、IBM Spectrum Protect Plus が認識できるように、それぞれ追加する必要があります。

バックアップ・ストレージ・プロバイダーとしての vSnap サーバーの追加

オンボード vSnap サーバーは、アプライアンスがデプロイされるときに IBM Spectrum Protect Plus に登録されます。仮想アプライアンスまたは物理アプライアンスのいずれかにインストールされている 他のサーバーを追加して、IBM Spectrum Protect Plus によって認識されるようにする必要があります。

始める前に

vSnap サーバーをバックアップ・ストレージ・プロバイダーとして追加した後、ネットワーク構成やストレージ・プール管理など、vSnap の特定の側面の構成と管理が必要になることがあります。詳しくは、62 ページの『vSnap サーバー管理の解説』を参照してください。

手順

vSnap サーバーをバックアップ・ストレージ・デバイスとして追加するには、以下のステップを実行します。

1. ユーザー ID `serveradmin` を使用して vSnap サーバー・コンソールにログオンします。初期パスワードは `sppDP758` です。

   初回ログオン中にこのパスワードの変更を求めるプロンプトが表示されます。
2. **`vsnap user create`** コマンドを実行して、vSnap サーバーのユーザー名とパスワードを作成します。
3. サポートされているブラウザーで、IBM Spectrum Protect Plus がデプロイされている仮想マシンのホスト名または IP アドレスを入力して IBM Spectrum Protect Plus ユーザー・インターフェースを 開始します。
4. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。
5. 「**ディスク・ストレージの追加**」をクリックします。
6. 「**ストレージ・プロパティー**」ペインのフィールドに入力します。

   ホスト名/IP
   バックアップ・ストレージの解決可能な IP アドレスまたはホスト名を入力します。

   サイト
   バックアップ・ストレージのサイトを選択します。選択可能なオプションは、「**1 次**」、「**2 次**」、または「**新規サイトを追加します**」です。IBM Spectrum Protect Plus で 1 次、2 次、またはユーザー定義のサイトを複数使用できる場合は、使用可能なストレージ容量が最も大きいサイトが最初に使用されます。

   ユーザー名
   ステップ 57 ページの『2』 で作成した vSnap サーバーのユーザー名を入力します。

   パスワード
   ユーザーのパスワードを入力してください。
7. 「**保存**」をクリックします。

   IBM Spectrum Protect Plus により、ネットワーク接続が確認され、バックアップ・ストレージ・デバイスがデータベースに追加されます。

次のタスク

バックアップ・ストレージ・プロバイダーを追加した後、以下のアクションを実行します。

アクション	方法
vSnap サーバーを初期化します。	58 ページの『vSnap サーバーの初期化』を参照してください。
vSnap ストレージ・プールを拡張します。	60 ページの『vSnap ストレージ・プールの拡張』を参照してください。
必要に応じて、ネットワーク構成やストレージ・プール管理など、vSnap の特定の側面の構成と管理を行います。	62 ページの『vSnap サーバー管理の解説』

関連タスク

71 ページの『IBM Spectrum Protect Plus の始動』

IBM Spectrum Protect Plus を始動して、アプリケーションとその機能の使用を開始します。

vSnap サーバーの設定の編集

ご使用の IBM Spectrum Protect Plus 環境で変更を反映するよう、vSnap サーバーの構成設定を編集できます。

手順

vSnap サーバーの設定を編集するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。
2. vSnap サーバーに関連付けられている編集アイコン をクリックします。
   「**ストレージの編集**」ペインが表示されます。
3. vSnap サーバー設定を修正してから、「**保存**」をクリックします。

vSnap サーバーの削除

ご使用の IBM Spectrum Protect Plus 環境で使用されなくなった vSnap サーバーを削除できます。
environment.

手順

vSnap サーバーを削除するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。
2. vSnap サーバーに関連付けられている削除アイコン をクリックします。
3. 「**はい**」をクリックして、IBM Spectrum Protect Plus からそのサーバーを削除します。

vSnap サーバーの初期化

初期化プロセスでは、ソフトウェア・コンポーネントをロードして構成し、内部構成を初期化することで、新規 vSnap サーバーを使用できるように準備します。これは、新規インストール時に実行する必要がある 1 回限りのプロセスです。

このタスクについて

初期化プロセスの一部として、vSnap は、システム上の使用可能な未使用のディスクを使用してストレージ・プールを作成します。vSnap の OVA ベースのデプロイメントでは、それぞれデフォルトで 100 GB の未使用仮想ディスクがあり、プールの作成に使用できます。

未使用ディスクが見つからない場合は、初期化プロセスはプールを作成せずに完了します。

ストレージ・プールの拡張、作成、および管理の方法については、63 ページの『ストレージ管理』を参照してください。

vSnap サーバーを初期化するために、IBM Spectrum Protect Plus ユーザー・インターフェースまたは vSnap サーバー・コンソールを使用できます。

仮想環境にデプロイされているサーバーでは、ユーザー・インターフェースを 使用すると、初期化操作を簡単に実行できます。

物理環境にデプロイされているサーバーでは、vSnap サーバー・コンソールを使用した方がサーバーを初期化するために多くのオプションを利用できます。例えば、高度な冗長性のオプションと特定のディスク・リストを使用してストレージ・プールを作成できます。

簡単な初期化の実行

vSnap サーバーを使用するために準備するには、vSnap サーバーを初期化する必要があります。 仮想環境にデプロイされた vSnap サーバーを初期化するには、IBM Spectrum Protect Plus を使用します。

このタスクについて

IBM Spectrum Protect Plus のインストールの一部として登録されたオンボード vSnap インストール済み環境では、ユーザー・インターフェースに 初めてログインするときに初期化プロセスの開始を求めるプロンプトが表示されます。それ以上の手順は不要です。

手順

IBM Spectrum Protect Plus ユーザー・インターフェースを 使用して vSnap サーバーを初期化するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。
2. サーバーに関連付けられている「**アクション**」メニューから初期化方式を選択します。

   暗号化を有効にして初期化します
   vSnap サーバー上のバックアップ・データの暗号化を有効にします。

   初期化
   暗号化を有効にせずに vSnap サーバーを初期化します。

   初期化プロセスはバックグラウンドで実行され、それ以上のユーザー対話は不要です。このプロセスは、完了するまでに 5 分から 10 分かかることがあります。

高度な初期化の実行

物理環境にデプロイされた vSnap サーバーを初期化するには、vSnap サーバー・コンソールを使用します。vSnap サーバー・コンソールを使用して初期化する方がサーバーを初期化するために多くのオプションを利用できます。例えば、高度な冗長性のオプションと特定のディスク・リストを使用してストレージ・プールを作成できます。

手順

vSnap サーバー・コンソールを使用して vSnap サーバーを初期化するには、以下のステップを実行します。

1. ユーザー ID `serveradmin` を使用して vSnap サーバー・コンソールにログオンします。初期パスワードは `sppDP758` です。

   vSnap 管理特権を持つユーザー ID を **`vsnap user create`** コマンドで作成して使用することもできます。コンソール・コマンドの使用法について詳しくは、62 ページの『vSnap サーバー管理の解説』を参照してください。
2. **`vsnap system init --skip_pool`** コマンドを実行します。このコマンドでは、それ以上の対話は不要です。ストレージ・プールの作成を除くすべての初期化タスクが実行されます。このプロセスは、完了するまでに 5 分から 10 分かかることがあります。

次のタスク

初期化を完了した後、以下のアクションを実行します。

アクション	方法
ストレージ・プールを作成します	63 ページの『ストレージ管理』を参照してください。

vSnap ストレージ・オプションの設定

vSnap サーバー用に追加のストレージ関連オプションを設定できます。

手順

vSnap サーバー用のオプションを設定するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。
2. vSnap サーバーに関連付けられている管理アイコン をクリックしてから、「**ストレージ・オプション**」セクションを展開します。ストレージ・オプションを設定してください。

   圧縮を有効にする

   有効になっている場合、データの各着信ブロックは圧縮アルゴリズムを使用して圧縮されたうえで、ストレージ・プールに書き込まれます。 圧縮では、さほど多くない追加 CPU リソースが使用されます。

   重複排除を有効にする

   有効になっている場合、データの各着信ブロックは値に変換され、ストレージ・プール内の既存のブロックと比較されます。圧縮が有効であると、データは圧縮された後で比較されます。重複ブロックは、プールに書き込まれずに、スキップされます。重複排除は、デフォルトでは使用不可になっています。なぜなら、ブロック・ハッシュの重複排除テーブルを維持するために大量のメモリー・リソース (プール内のデータ量に比例) を消費するからです。

   同期書き込みモード

   同期書き込みを無効にすると、バックアップ・ジョブの実行中にストレージ・サーバーの予期しないシャットダウンまたはリブートが起きた場合に、データ損失とバックアップ・データの潜在的な破損が生じる可能性があります。ハードウェア/電源障害に対する十分な保護機能がある安定した環境にストレージ・サーバーが配置されていない限り、このオプションを無効にしないでください。

   暗号化が有効

   このオプションは、vSnap サーバーの暗号化状況を表示します。暗号化を有効にできるのは、vSnap の初期設定時のみです。 このオプションは、情報提供のみを目的としています。
3. 「**保存**」をクリックします。

vSnap ストレージ・プールの拡張

IBM Spectrum Protect Plus から、vSnap サーバーがストレージ容量に達していると報告された場合は、vSnap ストレージ・プールを拡張する必要があります。vSnap ストレージ・プールを拡張するには、まず vSnap サーバーに仮想ディスクまたは物理ディスクを追加する必要があります。そのためには、vSnap 仮想マシンに仮想ディスクを追加するか、vSnap 物理サーバーに物理ディスクを追加します。追加の仮想ディスクの作成については、vSphere の資料を参照してください。

手順

vSnap ストレージ・プールを展開するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。
2. 再スキャン対象の vSnap サーバーについて、「**アクション**」 > 「**再スキャン**」を選択します。
3. vSnap サーバーに関連付けられている管理アイコン をクリックして、「**バックアップ・ストレージに新規ディスクを追加**」セクションを展開します。
4. 選択したディスクを追加して保存します。追加されたディスクのサイズだけ、vSnap プールが拡張されます。

vSnap サーバー用の複製パートナーシップの構築

バックアップ・ストレージの複製を使用することにより、1 つの vSnap サーバーから別の vSnap サーバーへデータを非同期でバックアップすることができます。

始める前に

複製が機能するためには、すべての vSnap サーバーが同じバージョン・レベルでなければなりません。異なるバージョン間の複製はサポートされていません。

手順

複製パートナーシップを構築するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。
2. 複製パートナーシップの追加先にしたい vSnap サーバーに関連付けられている管理アイコン をクリックしてから、「**ストレージ・パートナーシップの構成**」セクションを展開します。
3. 追加アイコン をクリックします。
4. 「**パートナーの選択**」リストから、複製パートナーシップの構築先とする vSnap サーバーを選択します。
5. 「**パートナーの追加**」をクリックします。

次のタスク

複製パートナーシップを作成後、以下のアクションを実行して、複製を有効にします。

アクション	方法
バックアップ・ジョブに関連付けられている SLA ポリシーで「**バックアップ・ストレージの複製**」オプションを選択します。	89 ページの『SLA ポリシーの作成』を参照してください。

オフロード・スループット率の変更

サイト複製およびオフロードの操作のスループットを変更して、定義済みのスケジュールでネットワーク・アクティビティーを管理できるようにします。

手順

1. ナビゲーション・ペインで、「**システム構成**」 > 「**サイト**」をクリックして、「**サイト・プロパティー**」ペインを開きます。
2. スループットを変更するサイトに関連付けられている編集アイコン をクリックします。
3. 「**スロットルの有効化**」をクリックします。

   スループット率は MB/秒単位で表示されます。
4. スループットを調整します。
   - 上矢印および下矢印を使用してスループット率を変更します。
   - データ値を変更します。選択項目には、「バイト/秒」、「KB/s」、「MB/s」、または「GB/s」があります。

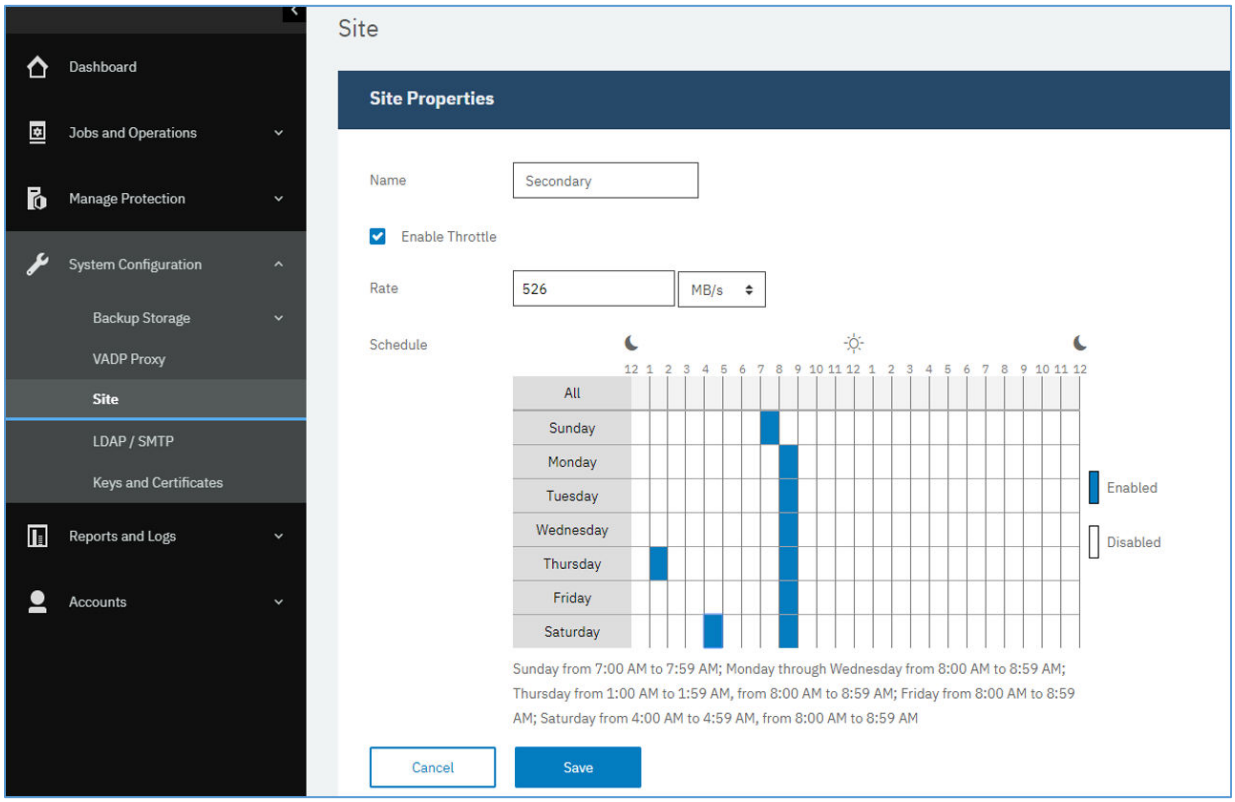


図 4. スループットを向上させるためのさまざまな時間に対するさまざまなスロットルの有効化

5. 変更したスループットの時間を週次スケジュール・テーブルで選択するか、変更した率の日時を指定します。

   注 : タイム・ゾーンをクリアするには、タイム・ゾーンをクリックします。スケジュール済みの選択項目がスケジュール・テーブルの下にリストされます。

6. 「**保存**」をクリックすると、変更がコミットされ、パネルが閉じます。

vSnap サーバー管理の解説

vSnap サーバーがインストールされ、登録され、初期化されたら、IBM Spectrum Protect Plus は自動的にその用途をバックアップ・ターゲットとして管理します。IBM Spectrum Protect Plus で定義された SLA ポリシーに基づいて、自動的にボリュームとスナップショットが作成され、管理されます。

ただし、ネットワーク構成やストレージ・プール管理などの特定の vSnap の側面の構成と管理が引き続き必要になる場合があります。

コマンド・ライン・インターフェースを使用した vSnap の管理

vSnap コマンド・ライン・インターフェースは、vSnap を管理するための 1 次手段です。このコマンド・ライン・インターフェースにアクセスするには、**vsnap** コマンドを実行します。このコマンドは、ユーザー ID `serveradmin`、または vSnap 管理特権を持つその他のオペレーティング・システム・ユーザーによって呼び出すことができます。これらの特権を持つオペレーティング・システム・ユーザーを追加で作成するには、**`vsnap user create`** コマンドを使用します。初期の `serveradmin` パスワードは sppDP758 です。

デフォルトで、`serveradmin` ユーザーには sudo 特権が割り当てられません。`serveradmin` ユーザーに sudo 特権を割り当てるには、vSnap サーバーのコマンド・ライン・インターフェースにログインし、次のコマンドを入力します。

```
echo "serveradmin ALL=(ALL) NOPASSWD: ALL" >/etc/sudoers.d/serveradmin
```

コマンド・ライン・インターフェースは、システムの各種側面を管理する複数のコマンドとサブコマンドで構成されます。これらのコマンドの使用について詳しくは、63 ページの『ストレージ管理』 および 66 ページの『ネットワーク管理』 を参照してください。 また、任意のコマンドまたはサブコマンドに **--help** フラグを渡して、使用法のヘルプを表示することもできます。例えば、**vsnap --help** または **vsnap pool create--help** です。

IBM Spectrum Protect Plus ユーザー・インターフェースを使用した vSnap の管理

最も一般的な操作の中には、IBM Spectrum Protect Plus ユーザー・インターフェースからも 実行できるものがあります。ユーザー・インターフェースにログインし、ナビゲーション・ペインで「**システム構成**」 >「**バックアップ・ストレージ**」 >「**ディスク**」**Disk** をクリックします。vSnap サーバーの管理アイコン をクリックして管理します。

関連タスク

53 ページの『vSnap サーバーのインストール』
IBM Spectrum Protect Plus アプライアンスをデプロイすると 、vSnap サーバーが自動的にインストールされます。このサーバーは 1 次バックアップの宛先になります。大規模なエンタープライズ環境では、追加の vSnap サーバーが必要になる場合があります。

56 ページの『vSnap サーバーの管理』
バックアップとリストアのジョブを 有効にするには、少なくとも 1 つの IBM Spectrum Protect Plus 仮想アプライアンスと 少なくとも 1 つの vSnap サーバーが必要です。vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスまたは独自のアプライアンスに配置するか、物理的な vSnap インストール済み環境を使用することもできます。vSnap サーバーのロケーションは、IBM Spectrum Protect Plus が認識できるように、それぞれ追加する必要があります。

ストレージ管理

vSnap サーバーのストレージ・プールを構成して管理することができます。

ディスクの管理

vSnap は、vSnap サーバーにプロビジョンされているディスクを 使用してストレージ・プールを作成します。仮想デプロイメントの場合、ディスクとして、バッキング・ストレージ上のデータ・ストアからプロビジョンされた RDM または仮想ディスクを使用できます。物理デプロイメントの場合は、ディスクとして、物理サーバーに接続されているローカル・ストレージまたは SAN ストレージを使用できます。ローカル・ディスクでは、既にハードウェア RAID コントローラーによって外部冗長性が得られていることがありますが、そうでない場合には、vSnap は内部冗長性のために RAID ベースのストレージ・プールを作成することもできます。

vSnap サーバーに接続されるディスクは、シック・プロビジョンする必要があります。ディスクがシン・プロビジョンされている場合、vSnap サーバーでストレージ・プール内のフリー・スペースの正確なビューが表示されず、そのために基礎となるデータ・ストアがスペース不足になった場合にデータ破損が生じる可能性があります。

vSnap が仮想アプライアンスの 一部としてデプロイされている場合は、プールを作成するために使用できる 100 GB のスターター仮想ディスクが既に用意されています。プールの作成前または作成後にディスクを追加して、さらに大容量のプールを作成したり、既存のプールを拡張したりするために使用できます。ジョブ・ログで vSnap サーバーがストレージ容量の限界に近づいていることが報告される場合は、さらに多くのディスクを vSnap プールに追加できます。あるいは、新規の SLA ポリシーを作成すると、バックアップで代替 vSnap が強制的に使用されます。

容量の限界に近づいている vSnap サーバー上の VMware データ・ストアに起因する破損から保護することが重要です。シック・プロビジョンされた VMDK を使用することで、RAID 構成が使用されない仮想 vSnap サーバーの安定した環境を作成してください。外部 vSnap サーバーに複製することでも、保護を強化できます。

vSnap プールが削除される場合、または vSnap ディスクが非冗長 RAID 構成で削除される場合、vSnap サーバーは無効になります。vSnap サーバー上のすべてのデータが失われます。vSnap サーバーが無効になった場合は、IBM Spectrum Protect Plus インターフェースを 使用して vSnap サーバーの登録を抹消してか

ら、メンテナンス・ジョブを実行する必要があります。この手順が完了した後、vSnap サーバーを再登録できます。

暗号化の管理

vSnap サーバー上のバックアップ・データの暗号化を有効にするには、サーバーの初期化時に「**暗号化を有効にして初期化します**」を選択します。サーバーが初期化され、プールが作成された後は、暗号化設定を変更できません。vSnap プールのすべてのディスクで、プール作成時に生成される同じ暗号鍵ファイルが使用されます。データは、vSnap サーバー上で保存されているときは暗号化されます。

vSnap の暗号化では、以下のアルゴリズムを使用しています。

暗号名
Advanced Encryption Standard (AES)

暗号モード
xts-plain64

キー(K)
256 ビット

Linux Unified Key Setup (LUKS) ヘッダー・ハッシュ
sha256

暗号鍵の管理

プール作成時に生成されるディスク暗号鍵ファイルは、各 vSnap サーバー上のディレクトリー /etc/vsnap/keys/ に保管されます。災害復旧を目的として、鍵ファイルを vSnap サーバーの外部に手動でバックアップしてください。プールが作成された後、以下のコマンドを serveradmin ユーザーとして使用し、それらを一時的なロケーションにコピーした後で、vSnap ホストの外部にある安全で望ましいバックアップ・ロケーションにコピーします。

```
mkdir /tmp/keybackup-$(hostname)
sudo cp -r /etc/vsnap/keys /tmp/keybackup-$(hostname)
```

ディスクの検出

vSnap サーバーにディスクを追加する場合、コマンド・ラインまたは IBM Spectrum Protect Plus ユーザー・インターフェースを 使用して、新たに接続されたディスクを検出します。

コマンド・ライン: `vsnap disk rescan` コマンドを実行します。

ユーザー・インターフェース: ナビゲーション・ペインの「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックして、関連する vSnap サーバーの横にある「**アクション**」メニュー・テキストをクリックし、「**再スキャン**」を選択します。

ディスクの表示

`vsnap disk show` コマンドを実行して、vSnap システム上のディスクをすべてリストします。

出力の「USED AS」列には、各ディスクが使用中であるかどうかが示されます。フォーマットも区画化もされていないディスクには未使用のマークが付けられ、そうでないディスクには、区画テーブルまたは区画テーブルで検出されたファイル・システムによって使用済みというマークが付けられます。

未使用のマークが付けられたディスクのみが、ストレージ・プールの作成または追加に適格となります。ストレージ・プールに追加しようとしているディスクが vSnap によって未使用として認識されない場合は、原因として、以前に使用されたことがあり、そのために古い区画テーブルやファイル・システムが残っていることが考えられます。この状態は、**`parted`** または **dd** などのシステム・コマンドを使用してディスク区画テーブルを消去することで修正できます。

ストレージ・プール情報の表示

vsnap pool show コマンドを使用して、各ストレージ・プールに関する情報を表示します。

ストレージ・プールの作成

59 ページの『簡単な初期化の実行』で説明されている簡単な初期化手順を完了している場合、ストレージ・プールは自動的に作成されているため、このセクションの情報は適用されません。

高度な初期化を実行するには、**vsnap pool create** コマンドを使用して、ストレージ・プールを手動で作成します。このコマンドを実行する前に、64 ページの『ディスクの表示』で説明しているように、1 つ以上の未使用ディスクを使用できることを確認してください。選択可能なオプションに関する情報を確認するには、コマンドまたはサブコマンドに **--help** フラグを渡します。

プールと 1 つ以上のディスクのリストに分かりやすい表示名を指定します。ディスクが指定されない場合、すべての使用可能な未使用ディスクが使用されます。作成時にプールに対して圧縮と重複排除を有効にすることを選択できます。後の時点で、**vsnap pool update** コマンドを使用して圧縮/重複排除設定を更新することもできます。

ストレージ・プールの作成時に指定するプール・タイプにより、プールの冗長度が決まります。

raid0
: プール・タイプが指定されない場合のデフォルト・オプションです。この場合、vSnap は、ディスクに外部冗長性があることを想定します。例えば、冗長ストレージでバッキングされているデータ・ストアで仮想ディスクを使用する場合です。この場合は、ストレージ・プールに内部冗長性はありません。

  ディスクは、raid0 プールに追加された後は削除できません。ディスクを切断すると、プールは使用できなくなり、プールを破棄して再作成することでしか解決できなくなります。

raid5
: このオプションを選択する場合、プールは、それぞれが 3 つ以上のディスクから成る 1 つ以上の RAID5 グループで構成されます。RAID5 グループの数と各グループ内のディスクの数は、プール作成時に指定するディスクの総数によって異なります。使用可能なディスクの数に基づき、vSnap は、合計容量を最大限に高めながら仮想メタデータの最適な冗長性を確保できる値を選択します。

raid6
: このオプションを選択する場合、プールは、それぞれが 4 つ以上のディスクから成る 1 つ以上の RAID6 グループで構成されます。RAID6 グループの数と各グループ内のディスクの数は、プール作成時に指定するディスクの総数によって異なります。使用可能なディスクの数に基づき、vSnap は、合計容量を最大限に高めながら仮想メタデータの最適な冗長性を確保できる値を選択します。

ストレージ・プールの拡張

プールを拡張する前に、64 ページの『ディスクの表示』で説明しているように、1 つ以上の未使用ディスクを使用できることを確認してください。

ストレージ・プールを拡張するには、コマンド・ラインまたは IBM Spectrum Protect Plus ユーザー・インターフェースを使用します。

コマンド・ライン: vsnap pool expand コマンドを実行します。選択可能なオプションに関する情報を確認するには、コマンドまたはサブコマンドに **--help** フラグを渡します。

ユーザー・インターフェース: ナビゲーション・ペインの「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」をクリックします。管理する vSnap サーバーの管理アイコン  をクリックして、「**新規ディスクの追加**」タブを展開します。このタブには、システムで検出されたすべての未使用ディスクが表示されます。1 つ以上のディスクを選択して、「**保存**」をクリックし、それらのディスクをストレージ・プールに追加します。

ネットワーク管理

vSnap サーバーのネットワーク・サービスを構成して管理します。

ネットワーク・インターフェース情報の表示

vsnap network show コマンドを実行して、ネットワーク・インターフェースと、各インターフェースに関連付けられているサービスをリストします。

デフォルトでは、以下の vSnap サービスをすべてのネットワーク・インターフェースで 使用できます。

mgmt
このサービスは、IBM Spectrum Protect Plus と vSnap の間の管理トラフィックに使用されます。

nfs
このサービスは、NFS を使用してデータをバックアップするときにデータ・トラフィックで使用されます。

iscsi
このサービスは、iSCSI を使用してデータをバックアップするときにデータ・トラフィックで使用されます。

smb
このサービスは、SMB/CIFS を使用してデータをバックアップするときにデータ・トラフィックで使用されます。

repl
このサービスは、複製時に vSnap サーバー間のデータ・トラフィックで使用されます。

ネットワーク・インターフェースに関連付けられているサービスの変更

vsnap network update コマンドを実行して、インターフェースに 関連付けられているサービスを変更します。例えば、パフォーマンスを向上させるためにデータ・トラフィックで専用のインターフェースを使用している場合です。

以下のオプションは必須です。

--id <id>
更新するインターフェースの ID を入力します。

--services <services>
`all` またはインターフェースで 有効にするサービスのコンマ区切りリストを指定します。有効な値は、`mgmt`、`nfs`、`smb`、および `iscsi` です。

サービスを複数のインターフェースで 使用できる場合、IBM Spectrum Protect Plus では任意のインターフェースを 1 つ使用できます。

vSnap サーバーを IBM Spectrum Protect Plus に登録するときに使用されたインターフェースで mgmt サービスが有効になったままであることを確認してください。

vSnap サーバーのアンインストール

ご使用の IBM Spectrum Protect Plus 環境から vSnap サーバーを除去することができます。

始める前に

vSnap サーバーをバックアップ・ロケーションとして定義する SLA ポリシーを使用しているジョブがないことを確認します。ジョブと関連付けられている SLA ポリシーを表示するには、バックアップ用にスケジュールされているハイパーバイザーまたはアプリケーションの「**バックアップ**」ページを参照してください。例えば、VMware バックアップ・ジョブの場合は、「**保護の管理**」>「**ハイパーバイザー**」>「**VMware**」をクリックします。

手順

1. ユーザー ID `serveradmin` で vSnap サーバー・コンソールにログオンします。初期パスワードは `sppDP758` です。

   `vsnap user create` コマンドを使用して作成した vSnap 管理者特権を持つユーザー ID を使用することもできます。コンソール・コマンドの使用法について詳しくは、62 ページの『vSnap サーバー管理の解説』を参照してください。
2. 次のコマンドを実行します。

   ```
   systemctl stop vsnap
   yum remove vsnap
   ```
3. オプション: vSnap サーバーをアンインストールした後に再インストールする予定がない場合は、次のコマンドを実行してデータと構成を削除します。

   ```
   rm -rf /etc/vsnap
   rm -rf /etc/nginx
   rm -rf /etc/uwsgi.d
   rm -f /etc/uwsgi.ini
   ```
4. システムをリブートします。これによって、確実にカーネル・モジュールがアンロードされ、vSnap プール・データが含まれているデータ・ディスクが切り離されます。

   注 : Hyper-V 環境で IBM Spectrum Protect Plus をアンインストールするには、SPP アプライアンスを Hyper-V から削除してから、インストール・ディレクトリーを削除します。

タスクの結果

vSnap サーバーがアンインストールされた後、構成は `/etc/vsnap` ディレクトリー内に保持されます。この構成は、vSnap サーバーが再インストールされる場合に、再使用されます。構成データを削除するオプション・コマンドを実行した場合は、構成が削除されます。

第 4 章 まずはクイック・スタートから

IBM Spectrum Protect Plus の使用を開始するには、保護するリソースの定義や、それらのリソースに対するサービス・レベル契約 (SLA) ポリシー (バックアップ・ポリシーとも呼ばれる) の作成を始めとする手順を実行する必要があります。この入門セクションでは、データをバックアップするために IBM Spectrum Protect Plus をセットアップして使用を開始する基本的な手順について説明します。データのオフロードおよびリストアなど、その他のタスクについては、資料の他の箇所で詳しく説明しています。

開始する前に、IBM Spectrum Protect Plus Blueprints の手順に従い、IBM Spectrum Protect Plus 環境におけるコンポーネントのサイジング、ビルド、および配置の方法を決定したこと、および 11 ページの『製品デプロイメントのロードマップ』にリストされているタスクが完了していることを確認してください。

次の表に示されているように、初期のインストールと構成のタスクは、IBM Spectrum Protect Plus のインフラストラクチャー管理者 が行います。デフォルトでは、初めてアプリケーションを起動する際にインフラストラクチャー管理者が使用できるように admin ユーザー・アカウントが作成されます。

次に、ハイパーバイザーとデータベース・アプリケーションのバックアップ・タスクとリストア・タスクが、アプリケーション管理者 によって実行されます。ただし、環境内のすべてのタスクに責任を持つのは単一の管理者です。

アクション	所有者	
IBM Spectrum Protect Plus の開始	インフラストラクチャー管理者およびアプリケーション管理者	インフラストラクチャー管理者は、パスワード password と一緒にデフォルトの admin ユーザー・アカウントを使用することで初めてアプリケーションを開始します。 管理者には、ログイン後に、このアカウントのユーザー名をリセットするようプロンプトが出されます。管理者は、ユーザー名を admin、root、または test にリセットすることはできません。 初期始動後、アプリケーション管理者は、このユーザー・アカウントか、またはインフラストラクチャー管理者によって作成された別のアカウントを使用して、アプリケーションを開始できます。

© Copyright IBM Corp. 2017, 2019

アクション	所有者	
	インフラストラクチャー管理者	サイトは、物理ロケーションまたは論理ロケーションに基づいて vSnap サーバーをグループ化するために使用されます。これは、バックアップ・データを迅速に識別して対話するのに役立ちます。vSnap サーバーが IBM Spectrum Protect Plus に追加されると、サイトが 1 つそのサーバーに割り当てられます。 デフォルトのサイトの名前は 1 次および 2 次となりますが、vSnap サーバーの追加時にカスタム・サイトを作成して割り当てることもできます。 以下のアクションを続行する前に、使用可能なサイトを確認し、新規サイトを追加するのか既存のサイトを変更するのかを決定してください。
バックアップ・ポリシーの作成	インフラストラクチャー管理者	バックアップ・ポリシーにより、バックアップ・ジョブに適用されるパラメーターが定義されます。これらのパラメーターには、バックアップの頻度や保存、および vSnap サーバー間でデータを複製するオプションや、長期保護のために 2 次バックアップ・ストレージにバックアップ・データをオフロードするオプションがあります。 バックアップ・ポリシーは、データをバックアップするためのターゲット・サイトも定義します。サイトには、vSnap サーバーを 1 つ以上含めることができます。 バックアップ・ポリシーは、IBM Spectrum Protect Plus においては SLA ポリシーと呼ばれます。
アプリケーション管理者用のユーザー・アカウントの作成	インフラストラクチャー管理者	ユーザー・アカウントにより、ユーザーが使用できるリソースと機能が決まります。
保護するリソースの追加	アプリケーション管理者	リソースは、保護するデータをホストするハイパーバイザーまたはデータベース・アプリケーション用のサーバーです。

アクション	所有者	
ジョブ定義へのリソースの追加	アプリケーション管理者	ジョブ定義では、保護するリソースと、1 つ以上の SLA ポリシーが関連付けられます。 SLA ポリシーで定義されるオプションとスケジュールは、リソースのバックアップ・ジョブに使用されます。
バックアップ・ジョブの開始	アプリケーション管理者	バックアップ・ジョブは、ジョブ定義に関連付けられた SLA ポリシーで定義されたとおりに開始されます。ジョブを手動で開始することもできます。
レポートの実行	アプリケーション管理者	IBM Spectrum Protect Plus は事前定義された複数のレポートを用意しています。これらのレポートは、デフォルトのパラメーターで実行するか、カスタム・レポートを作成するために変更することができます。

IBM Spectrum Protect Plus の始動

IBM Spectrum Protect Plus を始動して、アプリケーションとその機能の使用を開始します。

手順

IBM Spectrum Protect Plus を始動するには、以下のステップを実行します。

1. サポートされている Web ブラウザーで、次の URL を入力します。

   ```
   https://host_name
   ```

   ここで、*host_name* は、アプリケーションがデプロイされている仮想マシンの IP アドレスです。これにより、IBM Spectrum Protect Plus に接続されます。
2. ご使用のユーザー名とパスワードを入力して、ログオンします。

   今回が初めてのログオンの場合、デフォルトのユーザー名は admin、パスワードは password です。デフォルトのユーザー名とパスワードのリセットを求めるプロンプトが出されます。ユーザー名を、admin、root、または test にリセットすることはできません。
3. 「**サインイン**」をクリックします。
4. 初めて IBM Spectrum Protect Plus にログオンしている場合は、以下のアクションを実行するようプロンプトが出されます。
   - serveradmin パスワードを変更します。初期パスワードは sppDP758 です。serveradmin ユーザーは、管理コンソールと IBM Spectrum Protect Plus 仮想アプライアンスへのアクセスに使用されます。管理コンソールおよび IBM Spectrum Protect Plus 仮想アプライアンスにアクセスする前に、serveradmin のパスワードを変更する必要があります。
   - オンボード vSnap サーバーの初期化プロセスを開始します。「**初期化**」か、サーバー上でデータを暗号化するために「**暗号化を有効にして初期化する**」を選択します。

管理サイト

サイトは、物理ロケーションまたは論理ロケーションに基づいて vSnap サーバーをグループ化するために使用されます。これは、バックアップ・データを迅速に識別して対話するのに役立ちます。vSnap サーバーが IBM Spectrum Protect Plus に追加されると、サイトが 1 つそのサーバーに割り当てられます。

このタスクについて

vSnap サーバーが IBM Spectrum Protect Plus に追加されると、サイトが 1 つそのサーバーに割り当てられます。ナビゲーション・ペインで「**システム構成**」 > 「**サイト**」をクリックして使用可能なサイトを確認し、vSnap サーバー用に新規サイトを追加するのか既存のサイトを編集するのかを決定してください。

注 : デフォルトの 1 次サイトおよび 2 次サイトについて、サイト名およびその他のオプションを変更することができます。

デモ・サイトは、オンボード vSnap サーバーでのみ使用可能です。このサイトをその他の vSnap サーバーで使用することはできません。

手順

サイトを追加または編集するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**サイト**」をクリックします。
2. 新規サイトの追加または既存のサイトの編集をするには、以下の該当のアクションを実行してください。

アクション	方法
新規サイトを追加。	a.「**サイトの追加**」をクリックします。 b. サイト名を入力します。 c. オプション:「**スロットルの有効化**」を選択すると、267 ページの『サイトの追加』 に説明されているように、サイト複製操作およびオフロード操作のためのスループットを管理することができます。 d.「**保存**」をクリックします。
サイトを編集。	a.「**サイトの編集**」をクリックします。 b. サイトに関連付けられている編集アイコン をクリックします。 c. オプション:「**スロットルの有効化**」を選択すると、268 ページの『サイトの編集』 に説明されているように、サイト複製操作およびオフロード操作のためのスループットを管理することができます。 d.「**保存**」をクリックします。

関連概念

1 ページの『製品のコンポーネント』
IBM Spectrum Protect Plus ソリューションは、ストレージ・コンポーネントとデータ移動コンポーネントを組み込んだ、自己完結型仮想アプライアンスとして提供されています。

267 ページの『サイトの管理』

サイトは、環境内のデータ配置の管理に使用される IBM Spectrum Protect Plus ポリシー構造です。

バックアップ・ポリシーの作成

SLA ポリシーと呼ばれることもあるバックアップ・ポリシーは、バックアップ・ジョブに適用されるパラメーターを定義します。これらのパラメーターには、バックアップの頻度と保存が含まれます。

このタスクについて

3 つのデフォルトの SLA ポリシーは、「ゴールド」、「シルバー」、および「ブロンズ」です。これらのポリシーをそのまま使用することも、ポリシーを変更することもできます。カスタム SLA ポリシーを作成することもできます。

仮想マシンが複数の SLA ポリシーに関連付けられている場合は、それらのポリシーを並行実行のスケジュールに入れないでください。SLA ポリシーの相互の実行間隔を相当離してスケジュールに入れるか、全体を結合して単一の SLA ポリシーにしてください。

例示を目的とするこのタスクでは、vSnap サーバーの複製の有効化、または 2 次バックアップ・ストレージへのオフロードやアーカイブについては説明していません。これらはオプション機能です。SLA ポリシーでこれらの機能をセットアップする方法については、89 ページの『SLA ポリシーの作成』を参照してください。

データのバックアップ・コピーはスナップショットと呼ばれます。

手順

SLA ポリシーを作成する場合、以下の手順を実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ポリシーの概要**」をクリックします。
2. 「**SLA ポリシーの追加**」をクリックします。
   「**新規 SLA ポリシー**」ペインが表示されます。
3. 「**名前**」フィールドに、SLA ポリシーを分かりやすく説明する名前を入力します。
4. 「**メイン・ポリシー**」の下の「**操作の保護**」セクションで、バックアップ操作の以下のオプションを設定します。これらの操作は、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」ウィンドウで定義されている vSnap サーバーで実行されます。

   保存
   バックアップ・スナップショットの保存期間を指定します。

   スケジュールの無効化
   頻度も開始時刻も定義せずにメイン・ポリシーを作成する場合、このチェック・ボックスを選択します。 スケジュールを指定せずに作成されたポリシーはオンデマンドで実行できます。

   頻度
   バックアップ操作の頻度を入力します。

   開始時刻
   バックアップ操作を開始する日時を入力します。

   ターゲット・サイト
   データのバックアップに使用するターゲット・バックアップ・サイトを選択します。

   サイトには、vSnap サーバーを 1 つ以上含めることができます。サイト内に複数の vSnap サーバーがある場合は、IBM Spectrum Protect Plus サーバーが vSnap サーバーへのデータの配置を管理します。

   このリストには、vSnap サーバーに関連付けられたサイトのみが表示されます。IBM Spectrum Protect Plus に追加されていても、vSnap サーバーに関連付けられていないサイトは表示されません。

   暗号化ディスク・ストレージのみを使用します
   暗号化されたサーバーと暗号化されていないサーバーが混在している環境で、暗号化された vSnap サーバーにデータをバックアップする場合、このチェック・ボックスを選択します。

制約事項 : このオプションが選択される場合、使用できる暗号化された vSnap サーバーがないと、関連ジョブは失敗します。

以下に、`Copper` という新規 SLA ポリシーの例を示します。このポリシーは、3 日ごとに午前 0 時に実行され、保存期間は 1 カ月です。

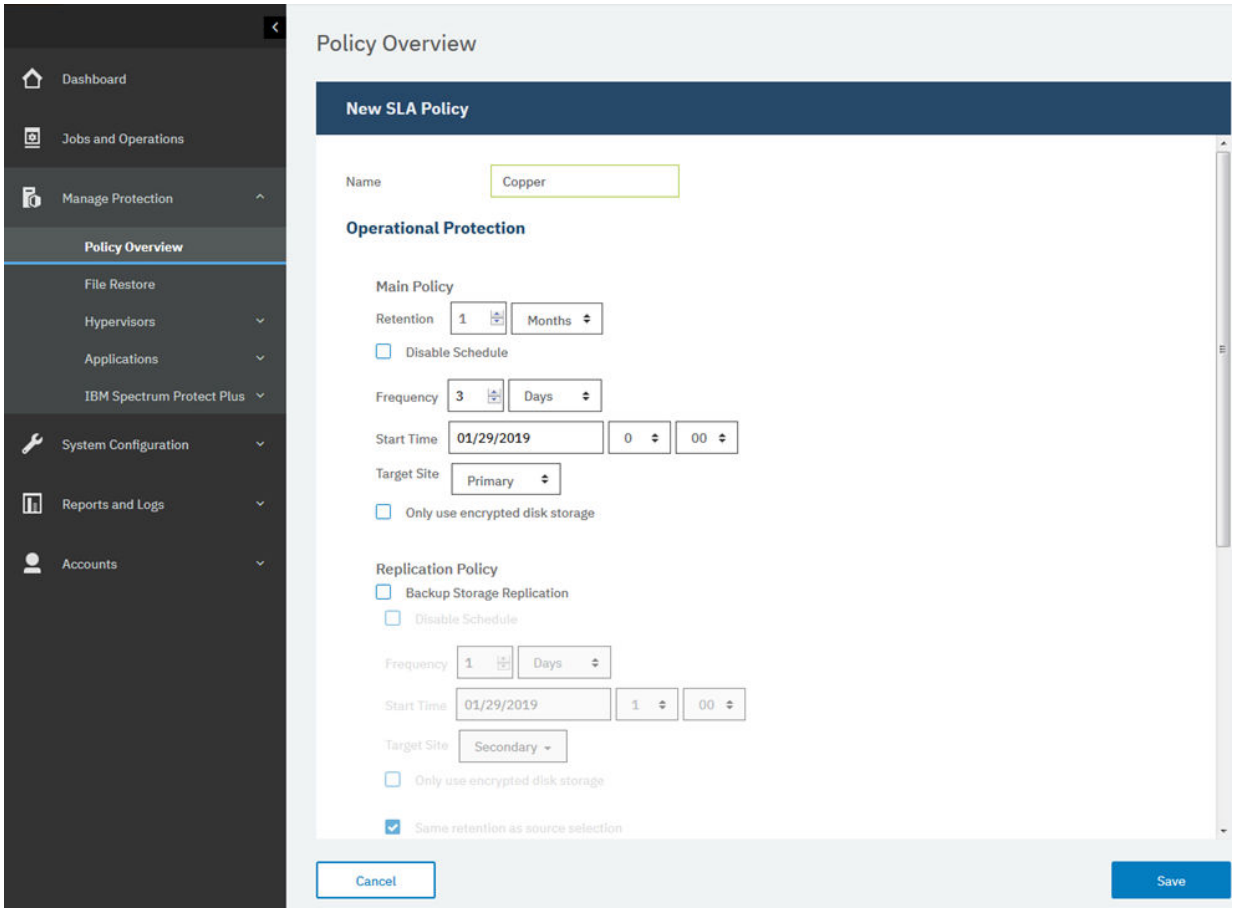


図 *5. SLA* ポリシーの作成

5. 「**保存**」をクリックします。これで、SLA ポリシーをバックアップ・ジョブ定義に適用できます (78 ページの『ジョブ定義へのリソースの追加』を参照)。

関連概念

5 ページの『バックアップ・ストレージ・データの複製』
バックアップ・データの複製を有効にすると、vSnap サーバーからのデータが、別の vSnap サーバーに非同期で複製されます。例えば、1 次サイト上の vSnap サーバーから、2 次サイト上の vSnap サーバーにバックアップ・データを複製できます。

6 ページの『2 次バックアップ・ストレージへのオフロード』
vSnap サーバーは、スナップショットの 1 次バックアップ・ロケーションです。すべての IBM Spectrum Protect Plus 環境に少なくとも 1 つの vSnap サーバーがあります。オプションで、スナップショットを vSnap サーバーから 2 次バックアップ・ストレージにオフロードできます。

89 ページの『バックアップ操作用の SLA ポリシーの管理』
サービス・レベル契約 (SLA) は、バックアップ・ポリシーとも呼ばれ、バックアップ・ジョブのパラメーターを定義します。これらのパラメーターには、バックアップの頻度や保存期間、およびバックアップ・データを複製またはオフロードするオプションがあります。事前定義された SLA ポリシーを使用することもできるし、それらを必要に応じてカスタマイズすることもできます。

アプリケーション管理者用のユーザー・アカウントを作成する

ご使用の環境内にあるハイパーバイザーまたはアプリケーションについてバックアップ 操作およびリストア操作を実行できる管理者用のユーザー・アカウントを作成します。

始める前に

例として、次の手順は、VMware データ保護の責任を負う個別のユーザーのアカウントを作成する方法を示します。このアカウントでは、既存のユーザー役割およびリソース・グループを使用します。

LDAP グループのアカウントを作成するには、302 ページの『LDAP グループのユーザー・アカウントの作成』を参照してください。

カスタム・ユーザー役割およびリソース・グループを作成するには、293 ページの『リソース・グループの作成』および 298 ページの『役割の作成』を参照してください。

手順

アプリケーション管理者のアカウントを作成するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ユーザー**」をクリックします。
2. 「**ユーザーの追加**」をクリックします。「**ユーザーの追加**」ペインが表示されます。
3. 「**追加するユーザーまたはグループのタイプを 選択**」 > 「**個別の新規ユーザー**」をクリックします。
4. アプリケーション管理者の名前とパスワードを入力します。
5. 「**役割の割り当て**」セクションで、「**VM Admin**」を選択します。
   許可は、「**許可グループ**」セクションに示されます。

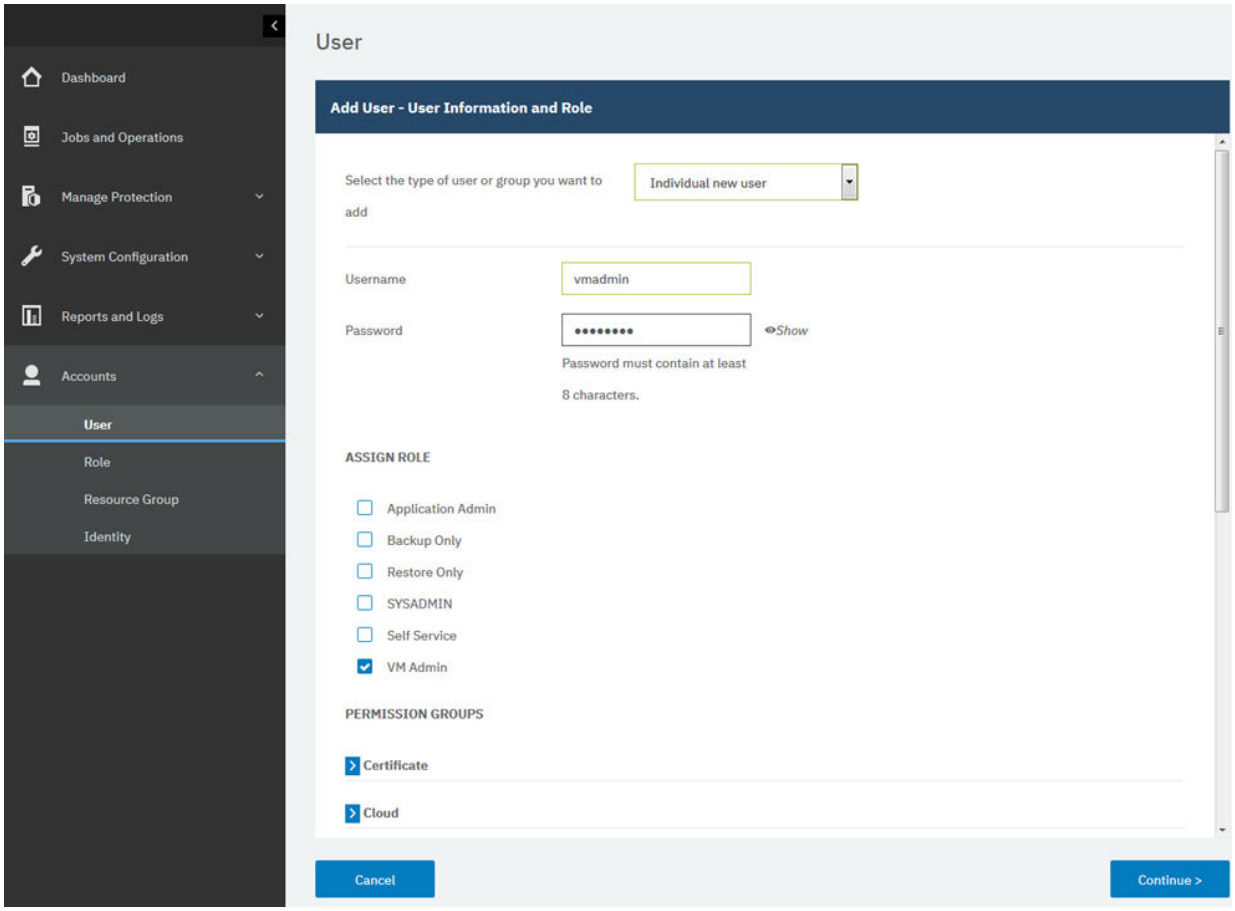


図 6. ユーザー・アカウントの作成と役割の割り当て

6. 「**続行**」をクリックします。
7. 「**ユーザーの追加 - リソースの割り当て**」セクションで、「**すべてのリソース**」リソース・グループを選択してから、「**リソースの追加**」をクリックします。
   リソース・グループは、「**選択されたリソース**」セクションに追加されます。

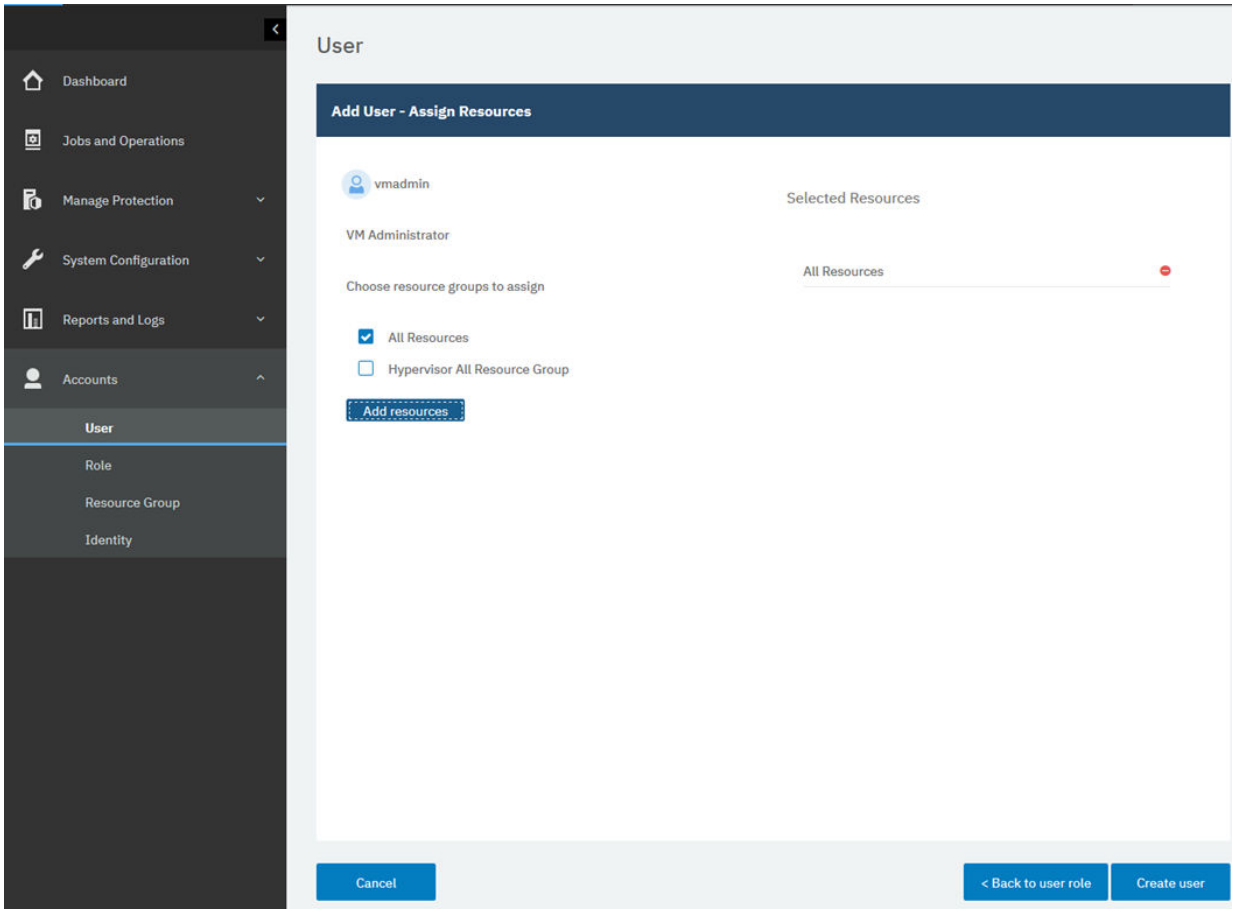


図 7. ユーザー・アカウントのためのリソース・グループの選択

8. 「**ユーザーの作成**」をクリックします。

関連概念

293 ページの『ユーザー・アクセスの管理』
役割ベースのアクセス制御を使用すると、IBM Spectrum Protect Plus ユーザー・アカウントから使用可能なリソースや許可を設定できます。

保護するリソースの追加

リソースとは、保護するデータをホストするハイパーバイザーまたはアプリケーションのサーバーです。リソースが登録された後、リソースのインベントリーがキャプチャーされ、IBM Spectrum Protect Plus インベントリーに追加されるため、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

このタスクについて

例を挙げる目的で、このタスクでは VMware リソースを追加する方法を説明しています。その他のリソースを追加するには、95 ページの『第 7 章 ハイパーバイザーの保護』および137 ページの『第 8 章 アプリケーションの保護』のリソース・タイプ別の説明を参照してください。

手順

vCenter Server インスタンスを追加するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. 「**vCenter の管理**」をクリックして、「**vCenter の追加**」をクリックします。
3. 「**vCenter プロパティー**」セクションのフィールドにデータを設定します。

   ホスト名/IP
   解決可能な IP アドレスまたは解決可能なパスとマシン名を入力します。

   既存のユーザーの使用
   vCenter Server インスタンスについて以前に入力済みのユーザー名とパスワードを選択できます。

   ユーザー名
   vCenter Server インスタンスのユーザー名を入力します。

   パスワード
   vCenter Server インスタンスのパスワードを入力します。

   ポート
   vCenter Server インスタンスの通信ポートを入力します。暗号化された Secure Sockets Layer (SSL) 接続を有効にするには、「**SSL の使用**」チェック・ボックスを選択します。通常、デフォルト・ポートは、非 SSL 接続の場合は 80 で、SSL 接続の場合は 443 です。
4. 「**オプション**」セクションで、以下のオプションを構成します。

   ESX サーバーごと、および SLA ごとに同時に処理する VM の最大数
   ESX サーバーを処理するための同時 VM スナップショットの最大数を設定します。

   以下の例は、データが設定されたフィールドを示しています。

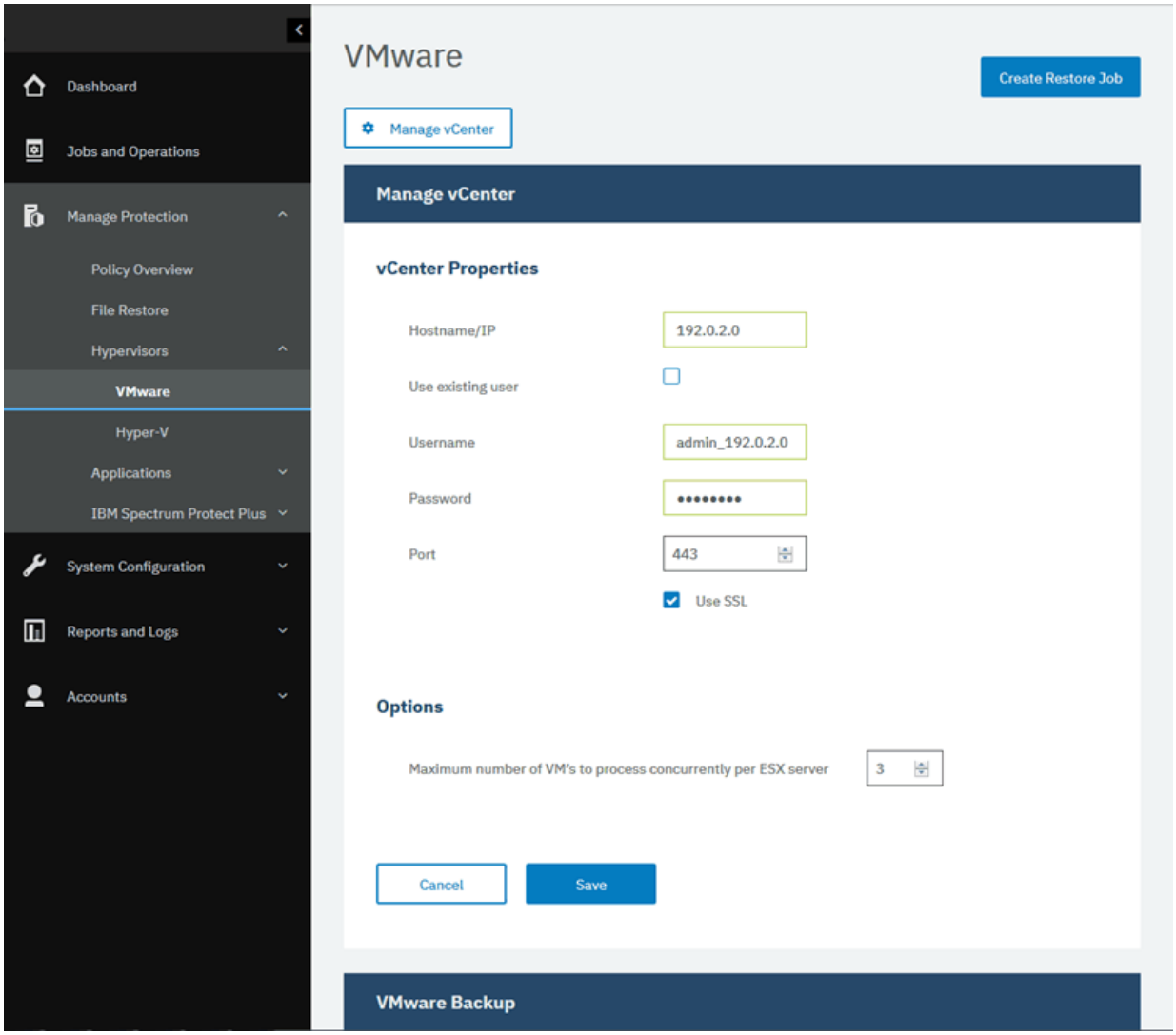


図 *8. vCenter Server* インスタンスの追加

5. 「**保存**」をクリックします。

   IBM Spectrum Protect Plus により、ネットワーク接続が確認され、リソースがデータベースに追加され、リソースがカタログされます。接続が失敗したことを示すメッセージが表示される場合は、項目を確認してください。項目が正確であっても接続が失敗する場合は、ネットワーク管理者に連絡して接続を確認し、可能な場合には修正してください。

ジョブ定義へのリソースの追加

リソースのバックアップを実行するには、その前に、そのリソースを 1 つ以上のバックアップ・ポリシー (SLA ポリシーともいいます) に関連付けるジョブ定義を作成する必要があります。

このタスクについて

例として、次の作業では VMware vCenter にあるリソースの SLA ポリシーの選択方法を説明します。その他のリソースのポリシーを選択するには、95 ページの『第 7 章 ハイパーバイザーの保護』および 137 ページの『第 8 章 アプリケーションの保護』 に示されているリソース・タイプ別の説明を参照してください。

手順

SLA ポリシーを選択する場合、以下の手順を実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. バックアップするリソースを選択します。vCenter 内のすべてのリソースを選択することも、ドリルダウンして特定のリソースを選択することもできます。

   検索機能を使用して使用可能なリソースを検索し、表示されたリソースを「**表示**」フィルターで切り替えます。使用可能なオプションは、「**VM とテンプレート**」、「**VM**」、「**データ・ストア**」、「**タグとカテゴリー**」、および「**ホストおよびクラスター**」です。vSphere に適用されるタグは、メタデータを仮想マシンに割り当てるために使用できます。

   次の例は、バックアップ用に選択された特定のハード・ディスクを示しています。

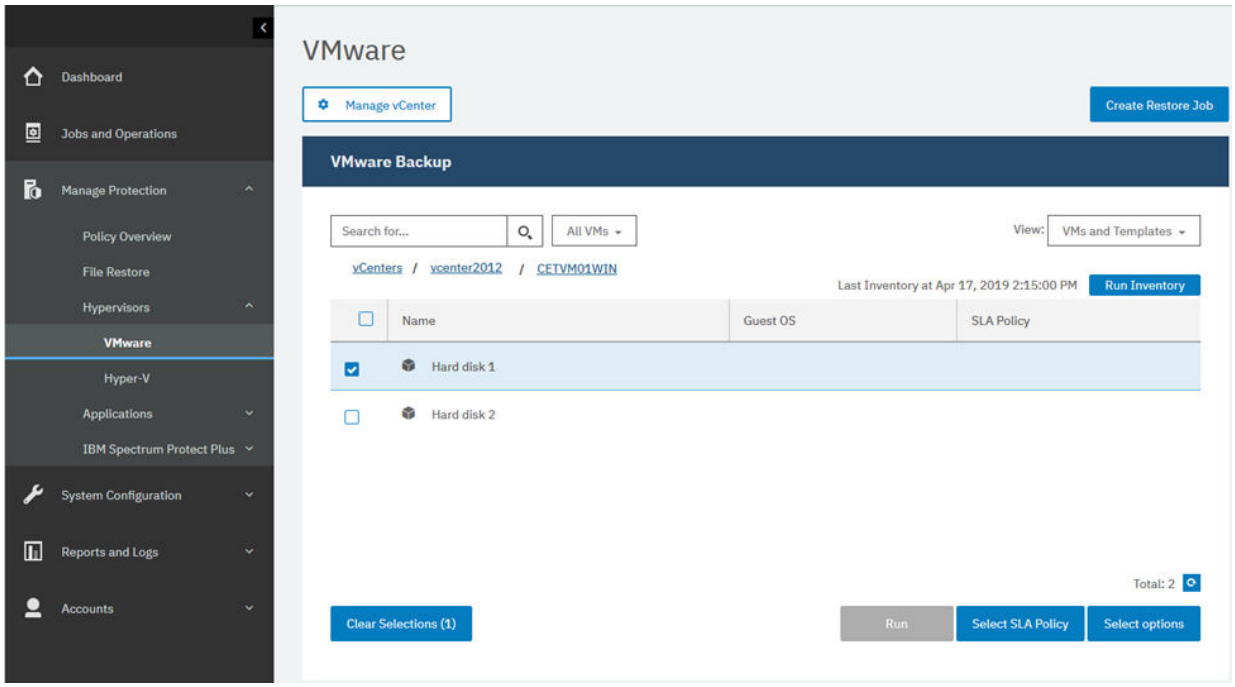


図 *9. バックアップ用のリソースの選択*

3. 「**SLA ポリシーの選択**」をクリックし、お客様のバックアップ・データ基準に合う 1 つ以上の SLA ポリシーをジョブ定義に追加します。

   以下の例では、SLA ポリシー「**Copper**」が選択されています。

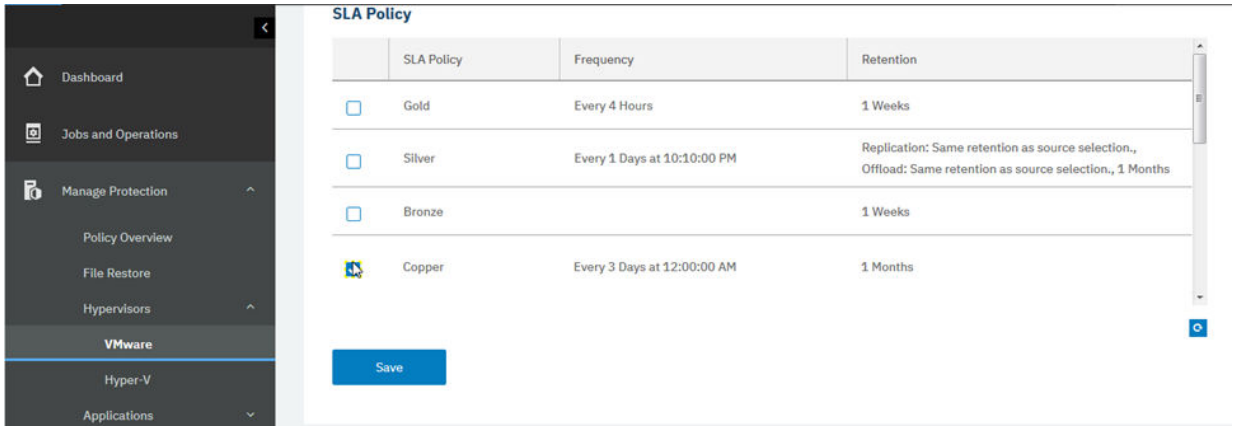


図 *10. SLA ポリシーの選択*

4. デフォルト・オプションを使用してジョブ定義を作成するには、「**保存**」をクリックします。
5. オプション: 追加のオプションを構成するには、「**オプションの選択**」をクリックし、103 ページの『VMware データのバックアップ』の手順に従ってください。
6. 「**保存**」をクリックします。

ジョブ定義を保存した後、「**表示**」フィルターで「**VM とテンプレート**」を選択すると、仮想マシン内で使用可能な仮想マシン・ディスク (VMDK) が検出されて表示されます。 デフォルトでは、これらの VMDK は仮想マシンと同じ SLA ポリシーに割り当てられます。オプションで、VMDK を個別に除外してさらに詳細なポリシーを定義することができます。107 ページの『ジョブの SLA ポリシーからの VMDK の除外』の説明に従ってください。

タスクの結果

ジョブは、選択した SLA ポリシーで定義されたとおりに実行されます。あるいは、「**ジョブと操作**」をクリックしてから「**ポリシーとジョブのリスト**」タブをクリックして、ジョブを手動で実行することもできます。手順については、80 ページの『バックアップ・ジョブの開始』を参照してください。

関連概念

243 ページの『IBM Spectrum Protect Plus の保護』

災害復旧シナリオの基礎データベースをバックアップして、IBM Spectrum Protect Plus アプリケーションを保護します。構成設定、登録済みリソース、リストア・ポイント、バックアップ・ストレージ設定、検索データ、およびジョブ情報が、関連した SLA ポリシーで定義された vSnap サーバーにバックアップされます。

バックアップ・ジョブの開始

SLA ポリシーによって設定されたスケジュールの外で、オンデマンドでバックアップ・ジョブを開始できます。

手順

バックアップ・ジョブをオンデマンドで開始するには、以下のステップを実行します。

1. ナビゲーション内で、「**ジョブと操作**」をクリックして、「**スケジュール**」タブを開きます。
   ジョブがスケジュール・ジョブではなくオンデマンド・ジョブの場合は、「**ジョブ・ヒストリー**」タブをクリックします。
2. 次の例に示すように、実行するジョブを選択して、「**アクション**」 > 「**開始**」をクリックします。

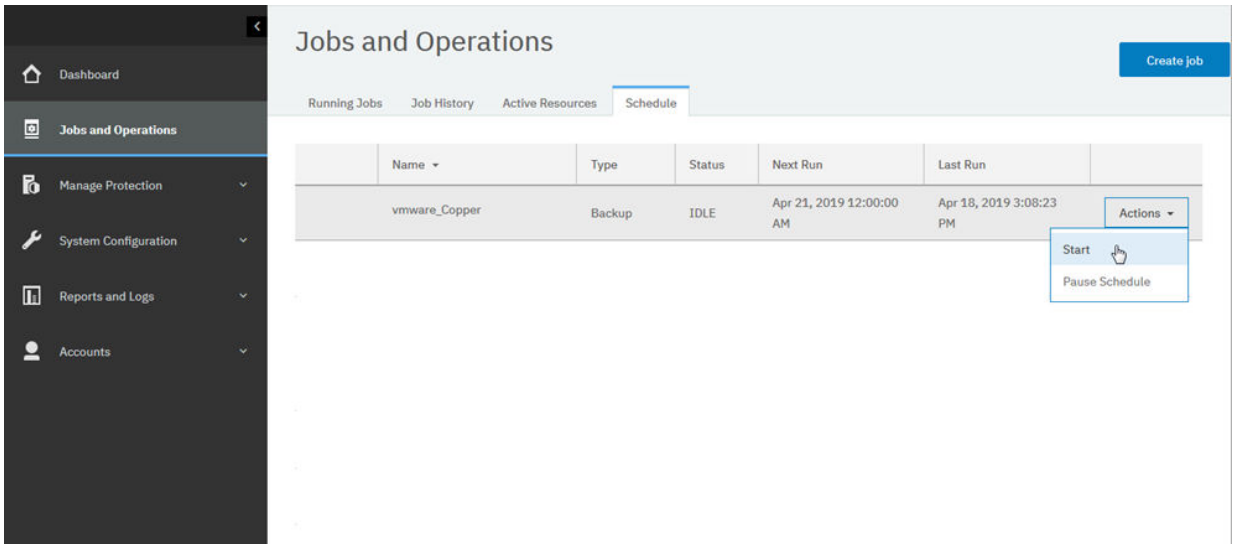


図 *11.* ジョブの開始

3. ジョブ・ログを詳細に表示するには、「**実行中のジョブ**」タブでジョブをクリックします。
   ログ画面に以下の詳細が表示されます。
   - 状況: このメッセージがエラー、警告、または情報メッセージのどれであるかを表示します。
   - 時刻: メッセージのタイム・スタンプを表示します。
   - ID: 該当する場合はメッセージの固有 ID を表示します。

- 説明: メッセージの内容を表示します。

4. 「**ダウンロード (.zip)**」をクリックして、ページからジョブ・ログをダウンロードすることができます。ジョブをキャンセルする場合は、「**アクション**」 > 「**キャンセル**」をクリックします。
5. 開始したいジョブに関連付けられている「**アクション**」メニューをクリックし、「**開始**」をクリックします (以下の例を参照)。

関連概念

247 ページの『ジョブと操作』

「**ジョブと操作**」ウィンドウを使用して、ジョブのモニター、ジョブ・ヒストリーの確認、ジョブのスケジュール、アクティブ・リソースの表示、ジョブとスケジュールの再実行や一時停止を行います。

レポートを実行する

事前定義済みのデフォルトのパラメーターまたはカスタム・パラメーターを使用してレポートを実行します。

手順

レポートを実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. レポート・タイプを展開して、実行するレポートを選択します (以下の例を参照)。

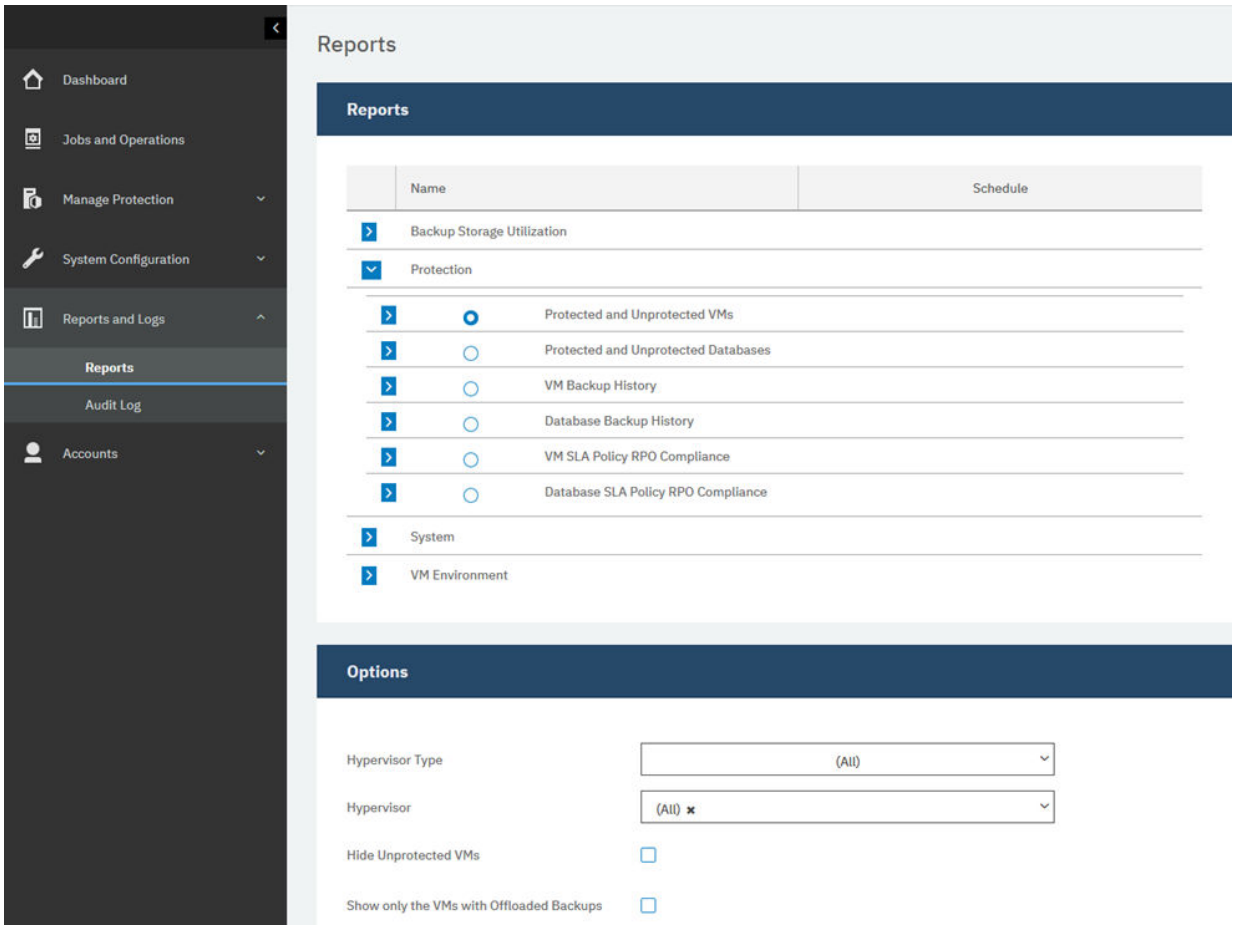


図 12. 実行するレポートの選択

3. カスタム・パラメーターまたはデフォルトのパラメーターのどちらかを使用してレポートを実行します。

- カスタム・パラメーターを使用してレポートを実行するには、「**オプション**」セクションでパラメーターを設定して、「**実行**」をクリックします。パラメーターは、各レポートに固有のものです。
- デフォルトのパラメーターを使用してレポートを実行するには、「**実行**」をクリックします。

関連概念

285 ページの『レポートおよびログの管理』

IBM Spectrum Protect Plus は事前定義された複数のレポートを用意しています。これらのレポートは、お客様のレポート作成要件を満たすようにカスタマイズすることができます。IBM Spectrum Protect Plus でユーザーが実行するアクションのログも提供されます。

第 5 章 IBM Spectrum Protect Plus コンポーネントの更新

IBM Spectrum Protect Plus 仮想アプライアンス、vSnap サーバー、および VADP プロキシー・サーバーを更新して、最新の機能や機能拡張を取得することができます。 ソフトウェア・パッチや更新のインストールには、IBM Spectrum Protect Plus 管理コンソール、またはこれらのコンポーネントのコマンド・ライン・インターフェースを 使用します。

使用可能な更新ファイルや、それらの更新ファイルを IBM ダウンロード・サイトから取得する方法については、技術情報 879861 を参照してください。

IBM Spectrum Protect Plus のコンポーネントを更新する前に、それらのコンポーネントのハードウェア要件とソフトウェア要件を検討して、前のバージョン以降に生じた変更がないか確認してください。

以下の制約事項とヒントを確認してください。

- IBM Spectrum Protect Plus 仮想アプライアンスにない vSnap サーバーは別途更新する必要があります。
- 管理コンソールを使用した更新処理では、IBM Spectrum Protect Plus の機能や基礎のインフラストラクチャー・コンポーネント (オペレーティング・システムやファイル・システムを 含む) が更新されます。これらのコンポーネントの更新に、別の方法を使用しないでください。
- IBM Spectrum Protect Plus の基礎コンポーネントが、IBM Spectrum Protect Plus 更新パッケージで提供されている場合を除いて、そのコンポーネントを更新しないでください。インフラストラクチャーの更新は、IBM の更新機能によって管理されます。管理コンソールは、IBM Spectrum Protect Plus の機能や基礎のインフラストラクチャー・コンポーネント (オペレーティング・システムやファイル・システムを 含む) を更新するための 1 次手段です。

次のアクションを実行してください。

- コンポーネントを更新する前に、243 ページの『IBM Spectrum Protect Plus アプリケーションのバックアップ』で説明されているように IBM Spectrum Protect Plus 環境をバックアップしておくことが重要です。
- IBM Spectrum Protect Plus が更新された後、前のバージョンにロールバックするには、仮想マシンのスナップショットが必要です。IBM Spectrum Protect Plus を更新する前に、ご使用の環境の仮想マシン・スナップショットを作成してください。後で前のバージョンに IBM Spectrum Protect Plus をロールバックしたい場合は、仮想マシン・スナップショットが必要です。アップグレードが正常に完了したら、仮想マシン・スナップショットを削除してください。

IBM Spectrum Protect Plus 仮想アプライアンスの更新

仮想アプライアンスを 更新するには、IBM Spectrum Protect Plus 管理コンソールを使用します。IBM Spectrum Protect Plus の更新は、オフラインで実行することも、外部インターネット・アクセス権限があればオンラインで実行することもできます。

始める前に

IBM Spectrum Protect Plus V10.1.2 以降から現行バージョンに直接更新することができます。V10.1.1 を使用している場合は、V10.1.2 に更新してから現行バージョンに更新する必要があります。V10.1.1 から V10.1.2 への更新方法については、 Updating the IBM Spectrum Protect Plus virtual appliance to version 10.1.2 を参照してください。

更新プロセスを始める前に、以下のステップを実行します。

1. 更新を実行する前に、IBM Spectrum Protect Plus 環境がバックアップされていることを確認してください。環境のバックアップについて詳しくは、243 ページの『IBM Spectrum Protect Plus アプリケーションのバックアップ』を参照してください。

© Copyright IBM Corp. 2017, 2019

2. オフライン更新の場合、CC1QHML.iso という名前の前提条件 IBM Spectrum Protect Plus 更新を、管理コンソール用のブラウザーを実行中のコンピューター上のディレクトリーにダウンロードします。この更新ファイルが最初にインストールされます。
3. 更新手順中に実行しているジョブがないことを確認します。「アイドル」または「完了」という状況になっているジョブについてはスケジュールを一時停止してください。

仮想アプライアンスの必須オペレーティング・システム更新を含め、ダウンロード・イメージのリストについては、技術情報 879861 を参照してください。

このタスクについて

インターネットへのアクセス権限がある場合は、更新手順のオンライン実行を選択できます。インターネットへのアクセス権限がない場合は、オフライン更新手順を実行できます。

手順

IBM Spectrum Protect Plus 仮想アプライアンスを更新するには、以下のステップを実行します。

1. サポートされている Web ブラウザーで、次のアドレスにある管理コンソールにアクセスします。

   ```
   https://hostname:8090/
   ```

   ここで、*hostname* は、アプリケーションがデプロイされている仮想マシンの IP アドレスです。
2. ログイン・ウィンドウで、「**認証タイプ**」リストから以下のいずれかの認証タイプを選択します。

認証タイプ	ログイン情報
IBM Spectrum Protect Plus	SYSADMIN 特権を持つ IBM Spectrum Protect Plus ユーザーとしてログインするには、ご使用の管理者ユーザー名とパスワードを入力します。admin ユーザー・アカウントを使用してログインする場合は、ユーザー名とパスワードのリセットを求めるプロンプトが出されます。 ユーザー名を、admin、root、または test にリセットすることはできません。
システム (推奨)	システム・ユーザーとしてログインするために、server admin パスワードを入力します。デフォルトのパスワードは sppDP758 です。最初のログイン時にこのパスワードの変更を求めるプロンプトが表示されます。

3. 「**更新とホット・フィックスの管理**」をクリックして、更新管理ページを開きます。

   FTP サイト (public.dhe.ibm.com) にアクセスできる場合は、管理者コンソールで使用可能な更新が自動的に確認されてリストされます。
4. 「**更新の実行 (Run Update)**」をクリックして、使用可能な更新をインストールします。
   - 更新が正常にインストールされたら、ステップ 6 に進みます。
   - ISO ファイルから更新をインストールする場合は、「**ここをクリック**」をクリックして、オフライン更新を実行します。ステップ 5 に進みます。

   注 : オンライン更新を実行したいのにオフライン・モードしか表示されない場合は、インターネット接続を確認してから FTP サイト (public.dhe.ibm.com) へのアクセスをもう一度試してください。
5. 以下のように、実行する更新を選択します。
   - オンライン・モード: リポジトリーが使用可能にされると、更新が自動的にリストされます。「**更新の実行**」をクリックします。
   - オフライン・モード:「**ファイルの選択**」をクリックして、ダウンロード済みファイルを表示します。該当のファイルには iso または rpm という拡張子が付いています (例: <filename>.iso)。「**更新イメージ (または) ホット・フィックスのアップロード**」をクリックします。

注 : 一度に 1 つの更新ファイルしか選択できません。

更新が完了すると、アプリケーションがデプロイされている 仮想マシンが自動的に再始動します。

重要 : IBM Spectrum Protect Plus 更新の完了後、ご使用の環境内にある外部 vSnap プロキシー・サーバーおよび VADP プロキシー・サーバーを更新する必要があります。

6. ブラウザー・キャッシュをクリアします。

   以前のバージョンの IBM Spectrum Protect Plus からの HTML コンテンツは、キャッシュに格納される場合があります。

7. 更新されたバージョンの IBM Spectrum Protect Plus を始動します。
8. ナビゲーション・ペインで、「**ジョブと操作**」をクリックして、「**スケジュール**」タブをクリックします。

   一時停止したジョブを見つけます。

9. 一時停止したジョブの「**アクション**」メニューから、「**スケジュールの解放**」を選択します。

関連タスク

85 ページの『vSnap サーバーの更新』

デフォルトの vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスで 更新されます。仮想アプライアンスまたは物理アプライアンスのどちらかに別々にインストールされている追加の vSnap サーバーを更新する必要があります。

vSnap サーバーの更新

デフォルトの vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスで 更新されます。仮想アプライアンスまたは物理アプライアンスのどちらかに別々にインストールされている追加の vSnap サーバーを更新する必要があります。

始める前に

vSnap サーバーは、バージョン 10.1.2 以降から現行バージョンに直接更新することができます。バージョン 10.1.1 を使用している場合は、バージョン 10.1.2 に更新してから現行バージョンに更新する必要があります。バージョン 10.1.2 への更新方法については、 Updating vSnap servers to version 10.1.2 を参照してください。

vSnap への更新を開始する前に、テスト・リストア・ジョブを完了する必要があります。アップグレードの開始時点で未完了のジョブまたはキャンセルされたジョブは更新が完了すると表示されなくなります。更新の完了後にジョブが表示されない場合は、テスト・リストア・ジョブを再実行してください。

サーバーを更新する前に、vSnap サーバー用のオペレーティング・システムの更新が必要な場合もあります。オペレーティング・システム要件については、11 ページの『コンポーネントの要件』を参照してください。

ご使用の vSnap サーバー用の現行のバージョンとオペレーティング・システムを調べるには、以下のステップを実行します。

1. `serveradmin` ユーザーとして vSnap サーバーにログオンします。IBM Spectrum Protect Plus 10.1.1 を使用している場合は、root アカウントを使用してログインします。
2. vSnap サーバーのバージョンとオペレーティング・システムを調べるには、vSnap コマンド・ライン・インターフェースを 使用して、以下のコマンドを発行します。

```
vsnap system info
```

vSnap サーバーを使用するジョブで、更新手順中に実行しているジョブがないことを確認します。「アイドル」または「完了」という状況になっているジョブについてはスケジュールを一時停止してください。

物理 vSnap サーバー用のオペレーティング・システムの更新

Red Hat Enterprise Linux を実行中のマシンに vSnap サーバーをインストールしてある場合、オペレーティング・システムをバージョン 7.5 または 7.6 に更新してから、vSnap サーバーを更新する必要があります。オペレーティング・システムの更新方法については、Red Hat Enterprise Linux の資料を参照してください。

関連タスク

86 ページの『vSnap サーバーの更新』

デフォルトの vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスで 更新されます。仮想アプライアンスまたは物理アプライアンスのどちらかに別々にインストールされている追加の vSnap サーバーを更新する必要があります。

仮想 vSnap サーバー用のオペレーティング・システムの更新

オペレーティング・システムが CentOS Linux バージョン 7.4 以前である場合、オペレーティング・システムを更新してから、vSnap サーバーを更新する必要があります。オペレーティング・システムを更新するには、 Updating vSnap servers to version 10.1.2 に記載されている手順に従います。バージョン 10.1.2 をインストールすると、CentOS Linux バージョン 7.5 が含まれています。

関連タスク

86 ページの『vSnap サーバーの更新』

デフォルトの vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスで 更新されます。仮想アプライアンスまたは物理アプライアンスのどちらかに別々にインストールされている追加の vSnap サーバーを更新する必要があります。

vSnap サーバーの更新

デフォルトの vSnap サーバーは、IBM Spectrum Protect Plus アプライアンスで 更新されます。仮想アプライアンスまたは物理アプライアンスのどちらかに別々にインストールされている追加の vSnap サーバーを更新する必要があります。

始める前に

更新プロセスを始める前に、以下のステップを実行します。

1. 243 ページの『IBM Spectrum Protect Plus アプリケーションのバックアップ』に記載されているとおりにご使用の IBM Spectrum Protect Plus 環境をバックアップしてあることを確認します。
2. IBM Spectrum Protect Plus 10.1.1 から更新する場合は、バージョン 10.1.2 に更新してから現行バージョンに更新する必要があります。 バージョン 10.1.2 への更新方法については、 Updating vSnap servers to version 10.1.2 を参照してください。
3. vSnap 更新ファイル `CC1QGML.run` をダウンロードして、vSnap サーバー上の一時的な場所にそれをコピーします。ファイルのダウンロードについては、技術情報 879861 を参照してください。

手順

vSnap サーバーを更新するには、次のステップを完了します。

1. **serveradmin** ユーザーとして vSnap サーバーにログオンします。
2. `CC1QGML.run` ファイルが置かれているディレクトリーから、以下のコマンドを発行してそのファイルを実行可能にし、インストーラーを実行します。

   ```
   chmod +x CC1QGML.run
   ```

   ```
   sudo ./CC1QGML.run
   ```

   vSnap パッケージがインストールされます。
3. 更新されたバージョンの IBM Spectrum Protect Plus を始動します。
4. ナビゲーション・ペインで、「**ジョブと操作**」をクリックして、「**スケジュール**」タブをクリックします。

   一時停止したジョブを見つけます。
5. 一時停止したジョブの「**アクション**」メニューから、「**スケジュールの解放**」を選択します。

VADP プロキシーの更新

IBM Spectrum Protect Plus 仮想アプライアンスを更新すると、その仮想アプライアンスに関連付けられているすべての VADP プロキシーが自動的に更新されます。ネットワーク接続の消失といったまれなシナリオでは VADP プロキシーを手動で更新する必要があります。

始める前に

作業を始める前に、243 ページの『IBM Spectrum Protect Plus アプリケーションのバックアップ』に記載されているとおりに、ご使用の IBM Spectrum Protect Plus 環境をバックアップしてあることを確認してください。

手順

VADP プロキシー更新が、IBM Spectrum Protect Plus 仮想アプライアンスの再始動時に外部プロキシーについて使用可能な場合、更新は、ID と関連付けられているすべての VADP プロキシーに自動的に適用されます。VADP プロキシーを ID に関連付けるには、「**システム構成**」 > 「**VADP プロキシー**」にナビゲートします。オプション・アイコン ••• をクリックし、「**オプションの設定**」を選択します。 ユーザー設定を使用して、以前に入力した VADP プロキシー・サーバー用のユーザー名とパスワードを選択します。

VADP プロキシーを手動で更新するには、以下のステップを実行します。

1. IBM Spectrum Protect Plus で「**システム構成**」 > 「**VADP プロキシー**」ページにナビゲートします。
2. 「**VADP プロキシー**」ページに、各プロキシー・サーバーが表示されます。新しいバージョンの VADP プロキシー・ソフトウェアが使用可能な場合、更新アイコン が「**状況**」フィールドに表示されます。
3. そのプロキシーを使用するアクティブ・ジョブがないことを確認してから、更新アイコン をクリックします。

   プロキシー・サーバーは、中断状態になり、最新の更新がインストールされます。更新が完了すると、VADP プロキシーは自動的に再開され、有効な状態になります。

非 root ユーザーとして更新を試行する場合は、VADP プロキシーをプッシュ・インストールまたはプッシュ更新するために、特別な手順を実行する必要があります。

1. /etc/sudoers.d/ ディレクトリー内にファイルを作成します。

   ```
   sudo cd /etc/sudoers.d/
   ```

2. このファイルにテキストを書き込み、完了したらキーボードで CTRL+D を押してファイルを保存します。

   ```
   sudo cat > 99-vadpuser
        Defaults !requiretty
        vadpuser ALL=NOPASSWD: /tmp/cdm_guestapps_vadpuser/runcommand.sh
   <<Press CTRL+D>>
   ```

3. ファイルに対して適切なアクセス権を設定します。

   ```
   sudo chmod 0440 99-vadpuser
   ```

次のタスク

VADP プロキシーを更新後、以下のアクションを実行します。

アクション	方法
VMware バックアップ・ジョブを実行する。	103 ページの『VMware データのバックアップ』を参照してください。 プロキシーは、以下のテキストに似たログ・メッセージによりジョブ・ログに記録されます。 `Run remote vmdkbackup of MicroService: http://<proxy` *`nodename`*`, IP:`*`proxy_IP_address`*

関連タスク

108 ページの『VADP プロキシーの作成』
Linux 環境で IBM Spectrum Protect Plus を使用して VMware バックアップ・ジョブを実行する VADP プロキシーを作成できます。

関連資料

49 ページの『ファイアウォール・ポートの編集』
提供されている例を、リモート VADP プロキシー・サーバーまたはアプリケーション・サーバーでファイアウォール・ポートを開く場合の参照として使用してください。ポート・トラフィックは必要なネットワークまたはアダプターのみに制限する必要があります。

早期可用性更新の適用

早期可用性更新により、IBM Spectrum Protect Plus のリリース間のプログラム診断依頼書 (APAR) および軽微な問題が修正されます。 これらの更新は、Fix Central オンライン Web サイトからまとめて取得可能です。

このタスクについて

早期可用性更新に、すべての IBM Spectrum Protect Plus コンポーネントについての修正が含まれていない可能性があります。

暫定修正の入手およびインストールの方法については、修正が取得可能になった時点で公開されるダウンロード情報を参照してください。

第 6 章 バックアップ操作用の SLA ポリシーの管理

サービス・レベル契約 (SLA) は、バックアップ・ポリシーとも呼ばれ、バックアップ・ジョブのパラメーターを定義します。これらのパラメーターには、バックアップの頻度や保存期間、およびバックアップ・データを複製またはオフロードするオプションがあります。事前定義された SLA ポリシーを使用することもできるし、それらを必要に応じてカスタマイズすることもできます。

使用可能なデフォルトの SLA ポリシーは次のとおりです。各ポリシーは、バックアップの頻度や保存期間を指定します。これらのポリシーをそのまま使用することも、変更することもできます。また、カスタム SLA ポリシーを作成することもできます。

ゴールド
このポリシーは 4 時間ごとに実行され、保存期間は 1 週間です。

シルバー
このポリシーは毎日実行され、保存期間は 1 カ月です。

ブロンズ
このポリシーは毎日実行され、保存期間は 1 週間です。

バックアップ・ポリシーを表示して管理する場合、およびポリシーによって保護されている仮想マシンとデータベースをモニターする場合は、ナビゲーション・ペインの「**保護の管理**」 > 「**ポリシーの概要**」をクリックします。

クラウド・オフロード・ソース、オフロード宛先タイプ、またはターゲット・オフロード・サーバー・オプションを変更して既存の SLA ポリシーを編集する場合、関連したジョブは、次のジョブ実行時に、増分バックアップではなく、フル基本バックアップを開始します。

IBM Spectrum Protect Plus V10.1.4 のインストール済み環境では、デモ SLA 構成をテスト用に使用できます。このデモンストレーション機能は、以下の要素で構成されています。

- 「**デモ**」という名前のデモンストレーション・サイト
- 「**デモ**」という名前の SLA ポリシー
- デモ SLA 用のローカル vSnap 構成

バックアップ操作およびリストア操作をテストするためにデモ・サイトを使用するよう選択できます。デモ SLA ポリシーを実行すると、データはローカル vSnap 構成にバックアップされます。

注 : 組み込み vSnap は、デモ・サイトによってのみ使用できるように設定されています。組み込み IBM Spectrum Protect Plus vSnap を他のサイトで使用しないでください。

SLA ポリシーの作成

カスタム SLA ポリシーを作成して、ご使用の環境に固有のバックアップ頻度、保存、複製、およびオフロード・ポリシーを定義できます。

このタスクについて

仮想マシンが複数の SLA ポリシーに関連付けられている場合は、作成したポリシーが同時に実行するようスケジュールされていないことを確認します。SLA ポリシーがかなりの時間を空けて実行されるようにスケジュールするか、または複数の SLA ポリシーを結合して単一の SLA ポリシーにします。

vSnap サーバーへの最初のバックアップが終了する前にスナップショット複製タスクが開始された場合、ジョブ・ログでのエラーは、データベースにリカバリー・ポイントが存在しないことを示します。 vSnap サーバーへの最初のバックアップが終了した後で、複製タスクを再度実行して、SLA ポリシーに構成されているとおりにスナップショットを複製します。

手順

SLA ポリシーを作成する場合、以下のステップを実行します。

© Copyright IBM Corp. 2017, 2019

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ポリシーの概要**」をクリックします。
2. 「**SLA ポリシーの追加**」をクリックします。
   「**新規 SLA ポリシー**」ペインが表示されます。
3. 「**名前**」フィールドに、SLA ポリシーを分かりやすく記述する名前を入力します。
4. 「**メイン・ポリシー**」の「**操作の保護**」セクションで、バックアップ操作について以下のオプションを設定します。これらの操作は、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**ディスク**」ウィンドウで定義された vSnap サーバー上で発生します。

   保存
   バックアップ・スナップショットの保存期間を指定します。

   スケジュールの無効化
   頻度や開始時刻を定義せずにメイン・ポリシーを作成する場合は、このチェック・ボックスを選択します。 スケジュールなしで作成されたポリシーは、オンデマンドで実行できます。

   頻度
   バックアップ操作の頻度を入力します。

   開始時刻
   バックアップ操作を開始したい日時を入力します。

   ターゲット・サイト
   データのバックアップに使用するターゲット・バックアップ・サイトを選択します。

   サイトには、vSnap サーバーを 1 つ以上含めることができます。サイト内に複数の vSnap サーバーがある場合は、IBM Spectrum Protect Plus サーバーが vSnap サーバーへのデータの配置を管理します。

   このリストには、vSnap サーバーに関連付けられたサイトのみが表示されます。 IBM Spectrum Protect Plus に追加されていても、vSnap サーバーに関連付けられていないサイトは表示されません。

   暗号化ディスク・ストレージのみを使用します
   このチェック・ボックスは、ご使用の環境に暗号化されたサーバーと暗号化されていないサーバーが混在する場合にデータを暗号化 vSnap サーバーにバックアップするために選択してください。

   制約事項 : このオプションが選択され、使用可能な暗号化された vSnap サーバーが存在しない場合、関連したジョブは失敗します。
5. 「**複製ポリシー**」で、以下のいずれかを設定して、1 つの vSnap サーバーから別の vSnap サーバーへの非同期複製を有効にします。例えば、1 次バックアップ・サイトから 2 次バックアップ・サイトにデータを複製できます。

   複製パートナーシップの要件 : これらのオプションは、確立された複製パートナーシップに適用されます。複製パートナーシップを追加するには、60 ページの『vSnap サーバー用の複製パートナーシップの構築』に記載されている手順を参照してください。

   バックアップ・ストレージの複製
   複製を有効にするには、このオプションを選択します。

   スケジュールの無効化
   頻度や開始時刻を定義せずに複製関係を作成する場合は、このチェック・ボックスを選択します。

   頻度
   複製操作の頻度を入力します。

   開始時刻
   複製操作を開始したい日時を入力します。

   ターゲット・サイト
   データの複製に使用するターゲット・バックアップ・サイトを選択します。

   サイトには、vSnap サーバーを 1 つ以上含めることができます。サイト内に複数の vSnap サーバーがある場合は、IBM Spectrum Protect Plus サーバーが vSnap サーバーへのデータの配置を管理します。

このリストには、vSnap サーバーに関連付けられたサイトのみが表示されます。IBM Spectrum Protect Plus に追加されていても、vSnap サーバーに関連付けられていないサイトは表示されません。

暗号化ディスク・ストレージのみを使用します
このオプションは、ご使用の環境に暗号化されたサーバーと暗号化されていないサーバーが混在する場合にデータを暗号化 vSnap サーバーに複製するために選択してください。

制約事項 : このオプションが選択され、使用可能な暗号化された vSnap サーバーが存在しない場合、関連したジョブは失敗します。

ソース選択と同じ保存
このオプションは、ソース vSnap サーバーと同じ保存ポリシーを使用する場合に選択します。別の保存ポリシーを設定するには、このオプションをクリアして、別のポリシーを設定してください。

6. 「**追加の保護**」セクションで、以下のオプションを設定して、データのオフロードまたはアーカイブを行います。

ヒント : 「追加の保護」を指定した場合は、コピーの作成を選択します。

クラウド
このオプションは、クラウド・ストレージまたはリポジトリー・サーバーにデータをオフロードする場合に選択します。

重要 : 「**追加の保護**」 > 「**クラウド**」をクリックすると、クラウド・ストレージ・システムまたは IBM Spectrum Protect サーバー にデータの増分コピーが作成されます。

データは、短期間の保護目的で vSnap サーバーにバックアップされてから、長期間の保護目的で、選択したクラウド・ストレージまたはリポジトリー・サーバーにオフロードされます。バックアップ・ボリュームの最初のオフロード時に、スナップショットは完全にバックアップされます。基本スナップショットの最初のオフロードが終了した後、後続のオフロードは段階的に増大し、最後のオフロード以降に累積した変更を取り込みます。クラウドまたはリポジトリーのサーバー・リストア操作は、任意の使用可能な vSnap サーバーから実行できます。

スケジュールの無効化
頻度や開始時刻を定義せずにオフロード関係を作成する場合は、このチェック・ボックスを選択します。

頻度
オフロード操作の頻度を入力します。

開始時刻
オフロード操作を開始したい日時を入力します。

ソース選択と同じ保存
このオプションは、ソース vSnap サーバーと同じクラウド・オフロード・バックアップ用保存ポリシーを使用する場合に選択します。別の保存ポリシーを設定するには、このオプションをクリアして、別のポリシーを設定してください。

制約事項 : Write Once Read Many (WORM) 保存を使用するサーバーが「**ターゲット・オフロード・サーバー**」フィールドで選択されている場合、オフロード保存オプションは無効です。

ソース
オフロード操作用のソースをクリックします。

メイン・ポリシーの宛先
オフロード操作用のソースは、「**メイン・ポリシー**」セクションで定義されたターゲット・サイトです。

複製ポリシーの宛先
オフロード操作用のソースは、「**複製ポリシー**」セクションで定義されたターゲット・サイトです。

このオプションは、「**バックアップ・ストレージの複製**」が選択されている場合にのみ使用できます。

宛先
「**クラウド・サーバー**」または「**リポジトリー・サーバー**」をクリックします。

ターゲット
データのオフロード先にするクラウド・ストレージ・システムまたはリポジトリー・サーバーをクリックします。

このリストには、IBM Spectrum Protect Plus に追加した 2 次ストレージ・システムが含まれています。2 次ストレージを追加していない場合、またはこれから追加する場合は、サポートされるクラウド・ストレージ・システムとリポジトリー・サーバー、およびそれらを IBM Spectrum Protect Plus に追加する方法について、253 ページの『2 次バックアップ・ストレージの管理』を参照してください。

アーカイブ
データを長期保護のためにクラウド・ストレージまたはリポジトリー・サーバーにアーカイブするには、このオプションを選択します。

重要 :「**追加の保護**」 >「**アーカイブ**」をクリックすると、IBM Spectrum Protect サーバー を使用してクラウド・ストレージ・システムまたは磁気テープにデータのフルコピーが作成されます。

この操作では、選択されたアーカイブ・ストレージに完全なイメージがオフロードされます。

スケジュールの無効化
頻度も開始時刻も定義せずにアーカイブ関係を作成するには、このチェック・ボックスを選択します。

頻度
アーカイブ操作の頻度を入力します。

開始時刻
アーカイブ操作を開始する日時を入力します。

保存
アーカイブ・スナップショットの保存期間を日、月、または年の単位で指定します。

ソース
アーカイブの宛先のソースをクリックします。

メイン・ポリシーの宛先
アーカイブ操作のソースは、「**メイン・ポリシー**」セクションで定義されたターゲット・サイトです。

複製ポリシーの宛先
アーカイブ操作のソースは、「**複製ポリシー**」セクションで定義されたターゲット・サイトです。

このオプションは、「**バックアップ・ストレージの複製**」が選択されている場合にのみ使用できます。

宛先
「**クラウド・サーバー**」または「**リポジトリー・サーバー**」をクリックします。

ターゲット
データのアーカイブ先にするクラウド・ストレージ・システムまたはリポジトリー・サーバーをクリックします。

このリストには、定義済みのアーカイブ・バケットを持つクラウド・ターゲットのみが表示されます。クラウド・ストレージ・システムのアーカイブ・バケットを追加するには、253 ページの『クラウド・ストレージの管理』に記載されている手順に従います。

7.「**保存**」をクリックします。これで SLA ポリシーは、バックアップ・ジョブ定義に適用できるようになりました。

次のタスク

SLA ポリシーを作成後、以下のアクションを実行してください。

アクション	方法
SLA ポリシーに対してユーザー許可を割り当てます。	298 ページの『役割の作成』を参照してください。

アクション	方法
SLA ポリシーを使用するバックアップ・ジョブ定義を作成します。	95 ページの『第 7 章 ハイパーバイザーの保護』および 137 ページの『第 8 章 アプリケーションの保護』に記載されているバックアップのトピックを参照してください。

関連概念

5 ページの『バックアップ・ストレージ・データの複製』
バックアップ・データの複製を有効にすると、vSnap サーバーからのデータが、別の vSnap サーバーに非同期で複製されます。例えば、1 次サイト上の vSnap サーバーから、2 次サイト上の vSnap サーバーにバックアップ・データを複製できます。

6 ページの『2 次バックアップ・ストレージへのオフロード』
vSnap サーバーは、スナップショットの 1 次バックアップ・ロケーションです。すべての IBM Spectrum Protect Plus 環境に少なくとも 1 つの vSnap サーバーがあります。オプションで、スナップショットを vSnap サーバーから 2 次バックアップ・ストレージにオフロードできます。

SLA ポリシーの編集

ご使用の IBM Spectrum Protect Plus 環境で変更を反映するよう、SLA ポリシー用のオプションを編集します。

手順

SLA ポリシーを編集する場合、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ポリシーの概要**」をクリックします。
2. ポリシーに関連付けられている編集アイコン をクリックします。
   「**SLA ポリシーの編集**」ペインが表示されます。
3. ポリシー・オプションを編集してから、「**保存**」をクリックします。

SLA ポリシーの削除

SLA ポリシーは、廃止されたら削除してください。

始める前に

SLA ポリシーに関連付けられたジョブがないことを確認してください。

手順

SLA ポリシーを削除する場合、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ポリシーの概要**」をクリックします。
2. SLA ポリシーに関連付けられている削除アイコン をクリックします。
3. 「**はい**」をクリックしてポリシーを削除します。
4. デモ SLA ポリシーを削除する場合は、「**システム構成**」 > 「**サイト**」と進んで、サイト名の付いたデモを削除します。

   注:

   デモ・サイトを削除した場合、ユーザー資格情報を使用してローカル・ホスト vSnap を別の有効なサイトに登録する必要があります。

第 7 章 ハイパーバイザーの保護

IBM Spectrum Protect Plus で保護するハイパーバイザーを登録してから、ハイパーバイザーに関連した仮想マシンとリソースのバックアップとリストアを 行うジョブを作成する必要があります。

VMware データのバックアップとリストア

VMware データを保護するには、最初に IBM Spectrum Protect Plus に vCenter Server インスタンスを追加してから、インスタンスのコンテンツに対するバックアップ操作とリストア操作のジョブを作成します。

システム要件

ご使用の VMware 環境が 22 ページの『ハイパーバイザー要件』 のシステム要件を満たしていることを確認してください。

VMware タグのサポート

IBM Spectrum Protect Plus は、VMware 仮想マシンのタグをサポートします。タグは vSphere で適用され、ユーザーがメタデータを仮想マシンに割り当てることができるようにします。仮想マシンのタグは、vSphere で適用され、IBM Spectrum Protect Plus インベントリーに追加されると、ジョブ定義の作成時に「**表示**」 > 「**タグとカテゴリー**」フィルターを 使用して表示できます。VMware のタグ付けについて詳しくは、Tagging Objects を参照してください。

暗号化のサポート

暗号化された仮想マシンのバックアップとリストアは、vSphere 6.5 以降の環境でサポートされます。暗号化された仮想マシンは、仮想マシン・レベルでバックアップされ、元の位置にリストアできます。別の位置にリストアしようとする場合、暗号化された仮想マシンは暗号化なしにリストアされます。リストアの完了後に vCenter Server を使用して手動で暗号化する必要があります。

暗号化された仮想マシンに対する操作を有効にするには、以下の vCenter Server 特権が必要です。

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

vCenter Server インスタンスの追加

vCenter Server インスタンスが IBM Spectrum Protect Plus に追加されると、そのインスタンスのインベントリーがキャプチャーされるため、バックアップとリストアのジョブを 実行したり、レポートを実行したりできるようになります。

手順

vCenter Server インスタンスを追加するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. 「**vCenter の管理**」をクリックします。
3. 「**vCenter の追加**」をクリックします。
4. 「**vCenter プロパティー**」セクションのフィールドにデータを設定します。

   ホスト名/IP
   解決可能な IP アドレスまたは解決可能なパスとマシン名を入力します。

   既存のユーザーの使用
   vCenter Server インスタンスについて以前に入力済みのユーザー名とパスワードを選択できます。

© Copyright IBM Corp. 2017, 2019

ユーザー名
vCenter Server インスタンスのユーザー名を入力します。

パスワード
vCenter Server インスタンスのパスワードを入力します。

ポート
vCenter Server インスタンスの通信ポートを入力します。暗号化された Secure Sockets Layer (SSL) 接続を有効にするには、「**SSL の使用**」チェック・ボックスを選択します。通常、デフォルト・ポートは、非 SSL 接続の場合は 80 で、SSL 接続の場合は 443 です。

5. 「**オプション**」セクションで、以下のオプションを構成します。

ESX サーバーごと、および SLA ごとに同時に処理する VM の最大数
ESX サーバーを処理するための同時 VM スナップショットの最大数を設定します。

6. 「**保存**」をクリックします。IBM Spectrum Protect Plus により、ネットワーク接続が確認され、vCenter Server インスタンスがデータベースに追加され、インスタンスがカタログされます。

接続が失敗したことを示すメッセージが表示される場合は、項目を確認してください。項目が正確であっても接続が失敗する場合は、ネットワーク管理者に連絡して接続を確認してください。

次のタスク

vCenter Server インスタンスを追加した後、以下のアクションを実行します。

アクション	方法
ハイパーバイザーにユーザー許可を割り当てます。	298 ページの『役割の作成』を参照してください。

関連概念

303 ページの『ID の管理』
IBM Spectrum Protect Plus の一部の機能には、リソースにアクセスするための資格情報が必要です。例えば、IBM Spectrum Protect Plus は、カタログ作成、データ保護、データ・リストアのようなタスクを実行するために、登録時に指定されたローカル・オペレーティング・システム・ユーザーとして Oracle サーバーに接続します。

関連タスク

103 ページの『VMware データのバックアップ』
スナップショットを使用して仮想マシン、データ・ストア、フォルダー、vApp、データ・センターなどの VMware リソースをバックアップするには、バックアップ・ジョブを使用します。

111 ページの『VMware データのリストア』
VMware リストア・ジョブは、インスタント VM リストアおよびインスタント・ディスク・リストアのシナリオをサポートします。これらのシナリオは、選択済みのソースに基づいて自動的に作成されます。

仮想マシンの特権

VMware プロバイダーに関連付けられている仮想マシンには、vCenter Server 特権が必要です。これらの特権は、vCenter 管理者役割に含まれています。

プロバイダーに関連付けられているユーザーに、インベントリー・オブジェクトの管理者役割が割り当てられていない場合、必要な以下の特権がある役割がユーザーに割り当てられなければなりません。 必ず、特権が子オブジェクトに伝搬されるようにしてください。手順については、インベントリー・オブジェクトへの許可の追加に関する VMware 資料を参照してください。

vCenter Server オブジェクト	必要な特権
アラーム	• アラームの確認 • アラーム・ステータスの設定

vCenter Server オブジェクト	必要な特権
暗号化操作	• ディスクの追加 • 直接アクセス • 暗号化 • 新規暗号化 • 暗号化ポリシーの管理
データ・センター	• データ・センターの作成 • データ・センターの再設定
データ・ストア	• スペースの割り振り • データ・ストアの参照 • データ・ストアの設定 • 低レベルのファイル操作 • ファイルの削除 • 仮想マシン・ファイルの更新
データ・ストア・クラスター	• データ・ストア・クラスターの設定
Distributed Switch	• 作成 • 削除 • ホスト操作 • 変更 • 移動 • Network I/O Control の操作 • ポリシー操作 • ポート構成オプション • ポート設定の操作 • VSPAN の操作
ESX Agent Manager	• 設定 • 変更 • 表示
拡張機能	• 拡張機能の登録
フォルダー	• フォルダーの作成 • フォルダーの削除 • フォルダーの移動 • フォルダー名の変更

vCenter Server オブジェクト	必要な特権
グローバル	• タスクのキャンセル • 診断 (トラブルシューティングに 使用、操作には不要) • メソッドを無効にする • メソッドを有効にする • ライセンス • ログ・イベント • カスタム属性の管理 • カスタム属性の設定 • 設定
ホスト > 構成	• 詳細設定 • ストレージ・パーティション構成
インベントリー・サービス > vSphere タギング	• vSphere タグの割り当てまたは割り当て解除 • vSphere タグの作成 • vSphere タグ・カテゴリーの作成 • カテゴリーの UsedBy フィールドの変更 • タグの UsedBy フィールドの変更
ネットワーク	• ネットワークの割り当て • 構成 • ネットワークの移動 • 削除
リソース	• 推奨の適用 • vApp のリソース・プールへの割り当て • 仮想マシンのリソース・プールへの割り当て • リソース・プールの作成 • パワーオフ状態の VM の移行 • パワーオン状態の VM の移行 • リソース・プールの変更 • リソース・プールの移動 • vMotion のクエリー • リソース・プールの削除 • リソース・プール名の変更
セッション	• セッションの表示および停止
ストレージ・ビュー	• サービスの構成 • 表示
タスク	• タスクの作成 • タスクの更新

vCenter Server オブジェクト	必要な特権
仮想マシン > 構成	• 既存ディスクの追加 • 新規ディスクの追加 • デバイスの追加または削除 • 詳細 • CPU カウントの変更 • リソースの変更 • managedBy の設定 • ディスク変更の追跡 • ディスク・リース • 接続設定の表示 • 仮想ディスクの拡張 • ホストの USB デバイス • メモリ • デバイス設定の変更 • Fault Tolerance の互換性のクエリー • 所有していないファイルのクエリー • Raw デバイス • パスからの再ロード • ディスクの削除 (仮想ディスクの切り離しと削除) • 名前変更 • ゲスト情報のリセット • 注釈の設定 • 設定 • スワップ・ファイルの配置 • 仮想マシンのアンロック • 仮想マシンの互換性のアップグレード
仮想マシン > ゲストの操作	• ゲスト操作の変更 • ゲスト操作のプログラム実行 • ゲスト操作のクエリー

vCenter Server オブジェクト	必要な特権
仮想マシン > 相互作用	• 質問への回答 • 仮想マシン上でのバックアップ操作 • CD メディアの設定 • フロッピー・メディアの設定 • コンソールでの相互作用 • スクリーン・ショットの作成 • すべてのディスクの最適化 • デバイス接続 • Fault Tolerance を無効にする • Fault Tolerance を有効にする • VIX API によるゲスト・オペレーティング・システム管理 • USB HID スキャン・コードの挿入 • ワイプまたは圧縮操作の実行 • パワーオフ • パワーオン • VM 上でのセッション記録 • VM 上での再生セッション • リセット • Fault Tolerance の再開 • 中断 • Fault Tolerance のサスペンド • フェイルオーバーのテスト • セカンダリー VM の再起動テスト • Fault Tolerance をオフにする • Fault Tolerance をオンにする • VMware Tools のインストール
仮想マシン > インベントリー	• 既存のものから作成 • 新規作成 • 移動 • 登録 • 削除 • 登録抹消

vCenter Server オブジェクト	必要な特権
仮想マシン > プロビジョニング	• ディスク・アクセスの許可 • 読み取り専用ディスク・アクセスの許可 • 仮想マシンのダウンロードの許可 • 仮想マシン・ファイルのアップロードの許可 • テンプレートのクローン作成 • 仮想マシンのクローン作成 • 仮想マシンからのテンプレートの作成 • カスタマイズ • テンプレートのデプロイ • テンプレートとしてマークを付ける • 仮想マシンとしてマークを付ける • カスタマイズ仕様の変更 • ディスクの昇格 • カスタマイズ仕様の読み取り
仮想マシン > サービス構成	• 通知の許可 • グローバル・イベント通知のポーリングの許可 • サービス設定の管理 • サービス設定の変更 • サービス設定のクエリー • サービス設定の読み取り
仮想マシン > スナップショット管理	• スナップショットの作成 • スナップショットの削除 • スナップショット名の変更 • スナップショットまで戻る
仮想マシン > vSphere Replication	• 複製の構成 • 複製の管理 • 複製のモニター

vCenter Server オブジェクト	必要な特権
vApp	• vApp への VM の追加 • vApp へのリソース・プールの割り当て • 別の vApp への vApp の割り当て • クローン • 作成 • 削除 • エクスポート • インポート • 移動 • パワーオフ • パワーオン • 名前変更 • 中断 • 登録抹消 • OVF 環境の表示 • vApp アプリケーションの設定 • vApp インスタンスの設定 • vApp managedBy の設定 • vApp リソースの設定

VMware リソースの検出
VMware リソースは、vCenter Server インスタンスが IBM Spectrum Protect Plus に追加されると、自動的に検出されます。しかし、インベントリー・ジョブを実行して、インスタンスが追加された後で行われた変更を検出することができます。

手順

インベントリー・ジョブを実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. vCenters Server インスタンスのリストで、インスタンスを選択するか、必要なリソースにナビゲートできるインスタンスのリンクをクリックします。例えば、インスタンス内の個別の仮想マシンについてインベントリー・ジョブを実行したい場合は、インスタンス・リンクをクリックしてから、仮想マシンを選択してください。
3. 「**インベントリーの実行**」をクリックします。

vCenter Server 仮想マシンへの接続のテスト
vCenter Server 仮想マシンへの接続をテストすることができます。テスト機能は、仮想マシンとの通信を検証し、IBM Spectrum Protect 仮想アプライアンスと 仮想マシンとの間でドメイン・ネーム・サーバー (DNS) 設定をテストします。

手順

接続をテストするには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. vCenters Server インスタンスのリストで、vCenter Server 仮想マシンが個々の仮想マシンにナビゲートできるリンクをクリックします。
3. 仮想マシンを選択してから、「**オプションの選択**」をクリックします。
4. 「**既存のユーザーの使用**」を選択します。

5.「**ユーザーの選択**」リストでユーザーを選択します。
6.「**テスト**」をクリックします。

VMware データのバックアップ

スナップショットを使用して仮想マシン、データ・ストア、フォルダー、vApp、データ・センターなどの VMware リソースをバックアップするには、バックアップ・ジョブを使用します。

始める前に

バックアップ・ジョブ定義を作成する前に、以下の手順と考慮事項を確認してください。

- バックアップするプロバイダーを登録します。詳しい手順については、95 ページの『vCenter Server インスタンスの追加』を参照してください。
- SLA ポリシーを構成します。詳しい手順については、73 ページの『バックアップ・ポリシーの作成』を参照してください。
- IBM Spectrum Protect Plus ユーザーがバックアップおよびリストアの操作を実装できるようにするには、その前に役割をそのユーザーに割り当てる必要があります。「**アカウント**」ペインを使用して、ハイパーバイザーおよびバックアップ/リストア操作へのアクセス権限をユーザーに付与してください。役割および関連の許可は、ユーザー・アカウントの作成時に割り当てられます。詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』および 301 ページの『ユーザー・アカウントの管理』を参照してください。
- 仮想マシンが複数の SLA ポリシーに関連付けられている場合は、それらのポリシーを並行実行のスケジュールに入れないでください。SLA ポリシーの相互の実行間隔を相当離してスケジュールに入れるか、全体を結合して単一の SLA ポリシーにしてください。
- ご使用の vCenter が仮想マシンの場合は、データ保護に最大の効果が得られるように、その vCenter を専用データ・ストアに置いて別個のバックアップ・ジョブでバックアップしてください。
- VMware 仮想マシンをバックアップする場合、IBM Spectrum Protect Plus は .vmx、.vmxf、および .nvram の各ファイルを必要に応じてダウンロードし、それらのファイルを必要に応じて vSnap に転送します。この処理を正常に実行するには、IBM Spectrum Protect Plus アプライアンスがすべての保護対象 ESXi ホストに対して解決とアクセスのための手段を持っている必要があります。また、ESXi ホストと通信する際には、正しい IP アドレスが返される必要があります。
- VM が SLA ポリシーで保護されている場合、VM のバックアップは、VM が vCenter から削除された後でも、SLA ポリシーの保存パラメーターに基づいて保存されます。
- 場合によっては、VMware バックアップ・ジョブが「マウント失敗」エラーで失敗することもあります。この問題を解決するには、NFS.MaxVolumes (vSphere 5.5 以降) および NFS41.MaxVolumes (vSphere 6.0 以降) の値を使用して、NFS マウントの最大数を少なくとも 64 増やします。Increasing the default value that defines the maximum number of NFS mounts on an ESXi/ESX host の指示に従ってください。
- 既存の VM が vMotion の場合、IBM Spectrum Protect Plus は必要に応じてリベースを実行します。

手順

VMware バックアップ・ジョブを定義するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. バックアップするリソースを選択します。

   検索機能を使用して使用可能なリソースを検索し、表示されたリソースを「**表示**」フィルターで切り替えます。使用可能なオプションは、「**VM とテンプレート**」、「**VM**」、「**データ・ストア**」、「**タグとカテゴリー**」、および「**ホストおよびクラスター**」です。タグは vSphere に適用され、ユーザーがメタデータを仮想マシンに割り当てるために使用できます。
3.「**SLA ポリシーの選択**」をクリックし、お客様のバックアップ・データ基準に合う 1 つ以上の SLA ポリシーをジョブ定義に追加します。
4. デフォルト・オプションを使用してジョブ定義を作成するには、「**保存**」をクリックします。

   ジョブは、選択した SLA ポリシーで定義されたとおりに実行されます。ジョブを手動で実行するには、「**ジョブと操作**」 > 「**スケジュール**」をクリックします。ジョブを選択して、「**アクション**」 > 「**開始**」をクリックします。

ヒント:「**実行**」ボタンは単一のハイパーバイザー・バックアップについてのみ有効であり、該当のハイパーバイザーに SLA ポリシーが適用されている必要があります。

ジョブ定義を保存してから、「**表示**」フィルターで「**VM とテンプレート**」を選択すると、仮想マシン内で使用可能な仮想マシン・ディスク (VMDK) が検出されて表示されます。 デフォルトでは、これらの VMDK は仮想マシンと同じ SLA ポリシーに割り当てられます。さらにきめ細かいバックアップ操作が必要な場合は、VMDK を SLA ポリシーから個別に除外することができます。手順については、107 ページの『ジョブの SLA ポリシーからの VMDK の除外』を参照してください。

5. ジョブ定義を作成する前にオプションを編集するには、「**オプションの選択**」をクリックします。

「**バックアップ・オプション**」セクションで、以下のジョブ定義オプションを設定します。

読み取り専用データ・ストアをスキップします

読み取り専用としてマウントされているデータ・ストアをスキップします。

インスタント・アクセス用にマウントされた一時データ・ストアをスキップします

一時インスタント・アクセス・データ・ストアをバックアップ・ジョブ定義から除外します。

VADP プロキシー

負荷のバランスを取るための VADP プロキシーを選択します。

優先度

選択済みリソースのバックアップ優先度を設定します。優先度設定の高いリソースがジョブで最初にバックアップされます。「**VMware バックアップ**」セクションで優先度付けするリソースをクリックしてから、「**優先度**」フィールドにバックアップ優先度を設定してください。 最高優先度には 1 を、最低優先度には 10 を設定します。優先度の値を設定していない場合、デフォルトで優先度 5 が自動的に割り当てられます。

「**スナップショット・オプション**」セクションで、以下のジョブ定義オプションを設定します。

VM スナップショット・アプリケーション/ファイル・システムを整合させてください

仮想マシン・スナップショットのアプリケーションまたはファイル・システムの整合性をオンにする場合に、このオプションを有効にします。システム状態とすべての VSS 準拠アプリケーション (Microsoft Active Directory、Microsoft Exchange、Microsoft SharePoint、Microsoft SQL など) が静止します。VMDK および仮想マシンを即時にマウントして、静止したアプリケーションに関連するデータをリストアできます。

VM スナップショットの再試行回数

IBM Spectrum Protect Plus がアプリケーションまたはファイルと整合する仮想マシンのスナップショットを取り込む場合、ジョブがキャンセルされる前に可能な試行回数を設定します。「**静止スナップショットが失敗した場合は、静止解除スナップショットにフォールバックします**」オプションが有効になっていると、再試行回数が過ぎた後で静止解除スナップショットが取られます。

静止スナップショットが失敗した場合は、静止解除スナップショットにフォールバックします

アプリケーション整合スナップショットが失敗した場合にアプリケーションまたはファイル・システムと整合しないスナップショットにフォールバックする 場合に、このオプションを有効にします。このオプションを選択すると、環境の問題によってアプリケーションまたはファイル・システムに整合するスナップショットの取り込みが禁止されている場合、静止解除スナップショットが取られます。

「**エージェント・オプション**」セクションで、以下のジョブ定義オプションを設定します。

SQL ログの切り捨て

バックアップ・ジョブの実行時に SQL Server のアプリケーション・ログを切り捨てるには、「**SQL ログの切り捨て**」オプションを有効にします。バックアップ・ジョブ定義のゲスト OS ユーザー名とゲスト OS パスワードのオプションを使用して、関連の仮想マシンの資格情報を設定する必要があります。仮想マシンがドメインに接続される場合、ユーザー ID は *domain¥name* のフォーマットに従います。ユーザーがローカル管理者の場合は、*local_administrator* のフォーマットが使用されます。

このユーザー ID にはローカル管理者特権が必要です。SQL Server サーバーでは、システム・ログイン資格情報には以下の許可が必要です。

- SQL Server の sysadmin 許可を有効にする必要があります。
- 「**サービスとしてログオン**」権限を設定する必要があります。この権限について詳しくは、Add the Log on as a service Right to an Account を参照してください。

IBM Spectrum Protect Plus は、ログ切り捨て機能用のログ・ファイルを生成し、それらのファイルを IBM Spectrum Protect アプライアンスの以下の場所にコピーします。

```
/data/log/guestdeployer/latest_date/latest_entry/vm_name
```

ここで、*latest_date* はバックアップ・ジョブとログ切り捨てが発生した日付、*latest_entry* はジョブの汎用固有 ID (UUID)、*vm_name* はログ切り捨てが発生した VM のホスト名または IP アドレスです。

制約事項 : ファイルの索引付けおよびファイル・リストアは、クラウド・リソースまたはリポジトリー・サーバーにオフロードされたリストア・ポイントからはサポートされません。

カタログ・ファイル・メタデータ

関連付けられたスナップショットに対するファイルの索引付けをオンにします。ファイルの索引付けが完了すると、IBM Spectrum Protect Plus の「**ファイル・リストア**」ペインを使用して、個々のファイルをリストアできます。SSH 鍵を使用するか、バックアップ・ジョブ定義の「**ゲスト OS ユーザー名**」オプションおよび「**ゲスト OS パスワード**」オプションを使用して、関連の仮想マシンの資格情報を設定する必要があります。DNS またはホスト名のいずれかを使用して IBM Spectrum Protect Plus アプライアンスから仮想マシンにアクセスできることを確認してください。

制約事項 : Windows プラットフォームの場合、SSH 鍵は有効な権限メカニズムではありません。

ファイルの索引付けおよびファイル・リストアは、クラウド・リソースまたはリポジトリー・サーバーにオフロードされたリストア・ポイントからはサポートされません。

除外するファイル

ファイルの索引付けの実行時にスキップするディレクトリーを入力してください。 これらのディレクトリー内のファイルは、IBM Spectrum Protect Plus カタログに追加されず、ファイル・リカバリーに使用できません。ディレクトリーを除外するには、完全一致を使用するか、あるいは、パターンの前 (*test) またはパターンの後 (test*) ワイルドカード・アスタリスクを指定します。単一パターン内で複数のアスタリスク・ワイルドカードを指定することもできます。パターンでは、標準の英数字のほか、特殊文字 -、_、および * を使用できます。複数のフィルターはセミコロンで区切ります。

既存のユーザーの使用

プロバイダーについて以前に入力済みのユーザー名とパスワードを選択します。

ゲスト OS ユーザー名/パスワード

一部のタスク (ファイル・メタデータのカタログ、ファイル・リストア、IP 再構成など) では、関連の仮想マシンについて資格情報を設定する必要があります。ユーザー名とパスワードを入力し、DNS またはホスト名のいずれかを使用して IBM Spectrum Protect Plus アプライアンスから仮想マシンにアクセスできることを確認してください。

6. ハイパーバイザー仮想マシンへの接続のトラブルシューティングを 行うには、「**テスト**」機能を使用します。

   「**テスト**」機能では、仮想マシンとの通信を検証し、IBM Spectrum Protect Plus アプライアンスと 仮想マシンとの間の DNS 設定をテストします。接続をテストするには、単一の仮想マシンを選択してから「**オプションの選択**」をクリックします。「**既存のユーザーの使用**」を選択し、リソースについて以前に入力済みのユーザー名とパスワードを使用します。「**テスト**」ボタンは、「**オプション**」セクションの「**保存**」ボタンの右側に表示されています。「**テスト**」をクリックします。
7. 「**保存**」をクリックします。
8. 追加オプションを構成するには、「**SLA ポリシー状況**」セクションでジョブと関連付けられている「**ポリシー・オプション**」をクリックします。以下の追加のポリシー・オプションを設定します。

   事前スクリプトと事後スクリプト

   事前スクリプトまたは事後スクリプトを実行します。事前スクリプトと事後スクリプトは、ジョブの実行の前または後に実行できるスクリプトです。Windows ベースのマシンはバッチ・スクリプトと PowerShell スクリプトをサポートし、Linux ベースのマシンはシェル・スクリプトをサポートします。

「**事前スクリプト**」セクションまたは「**事後スクリプト**」セクションで、アップロード済みのスクリプトと、そのスクリプトを実行するスクリプト・サーバーを選択してください。スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページを使用して構成します。

ジョブに関連付けられたスクリプトが失敗した場合でもジョブを続行するには、「**スクリプト・エラーの場合もジョブ/タスクを続行**」を選択します。

このオプションを有効にすると、事前スクリプトまたは事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、バックアップ操作またはリストア操作が試行され、事前スクリプト・タスク状況は「完了」と報告されます。事後スクリプトがゼロ以外の戻りコードで完了した場合、事後スクリプト・タスク状況は「完了」と報告されます。

このオプションを無効にすると、バックアップまたはリストアは試行されず、事前スクリプトまたは事後スクリプトのタスク状況は「失敗」と報告されます。

バックアップの前にインベントリーを実行します。

バックアップ・ジョブを開始する前に、インベントリー・ジョブを実行し、選択されたリソースの最新データを取り込みます。

リソースの除外

単一または複数の除外パターンを使用して、バックアップ・ジョブから特定のリソースを除外します。リソースを除外するには、完全一致を使用するか、あるいは、パターンの前 (*test) またはパターンの後 (test*) ワイルドカード・アスタリスクを指定します。

単一パターン内で複数のアスタリスク・ワイルドカードを指定することもできます。パターンでは、標準の英数字のほか、特殊文字 -、_、および * を使用できます。

複数のフィルターはセミコロンで区切ります。

リソースのフルバックアップの 強制

バックアップ・ジョブ定義内にある特定の仮想マシンまたはデータベースへの基本バックアップ操作を強制的に実行します。複数のリソースはセミコロンで区切ります。

9. 構成した追加オプションを保存するには、「**保存**」をクリックします。

次のタスク

バックアップ・ジョブを定義した後で、以下のアクションを実行できます。

アクション	ハウツー
Linux 環境を使用している場合は、VADP プロキシーを作成して負荷の共有を有効にすることを検討する。	108 ページの『VADP プロキシーの作成』を参照してください。
VMware リストア・ジョブ定義を作成する。	111 ページの『VMware データのリストア』を参照してください。

関連概念

250 ページの『バックアップ操作とリストア操作のスクリプトの構成』
事前スクリプトと事後スクリプトは、バックアップ・ジョブとリストア・ジョブがジョブ・レベルで実行される前または後に実行できるスクリプトです。サポートされるスクリプトには、Linux ベースのマシン用のシェル・スクリプトや、Windows ベースのマシン用の Batch および PowerShell スクリプトがあります。スクリプトはローカル側で作成され、「**スクリプト**」ページを使用して環境にアップロードされてから、ジョブ定義に適用されます。

関連タスク

248 ページの『ジョブの開始』

いずれのジョブも、スケジュールで実行するよう設定されている場合でも、オンデマンドで実行できます。

ジョブの SLA ポリシーからの VMDK の除外

バックアップ・ジョブ定義を保存した後で、仮想マシン内の VMDK をジョブに割り当てられた SLA ポリシーから個別に除外できます。

手順

SLA ポリシーから VMDK を除外するには、次のようにします。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. 「**表示**」フィルターで 「**VM とテンプレート**」を選択します。
3. vCenter のリンクをクリックし、次に、除外する VMDK を含む仮想マシンのリンクをクリックします。
4. 1 つ以上の VMDK を選択してから、「**SLA ポリシーの選択**」をクリックします。
5. 選択済みの SLA ポリシーのチェック・ボックスをクリアしてから、「**保存**」をクリックします。

Linux ベースの vCenter Server アプライアンスのバックアップ

Linux ベースの vCenter Server アプライアンスをバックアップするには、破損した vCenter バックアップを避けるよう、vCenter 仮想マシン上の VMware 事前凍結スクリプトおよび事後解凍スクリプトを修正する必要があります。

手順

スクリプトを変更するには、以下のステップを実行します。

1. 仮想マシン上で、`/usr/sbin` ディレクトリーにナビゲートし、`pre-freeze-script` スクリプトの内容を以下の内容で置き換えます。

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y¥/%m¥/%d¥ %H:%M:%S`
echo "${today}: Start of creation consistent state" >> ${log}
#execute freeze command
cmd="echo ¥"SELECT pg_start_backup('${today}', true);¥" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log}
2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y¥/%m¥/%d¥ %H:%M:%S`
echo "${today}: Finished freeze script" >> ${log}
```

2. `post-thaw-script` スクリプトの内容を以下の内容で置き換えます。

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y¥/%m¥/%d¥ %H:%M:%S`
echo "${today}: Release of backup" >> ${log}
#execute release command
cmd="echo ¥"SELECT pg_stop_backup();¥" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log} 2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y¥/%m¥/%d¥ %H:%M:%S`
echo "${today}: Finished thaw script" >> ${log}
```

VADP バックアップ・プロキシーの管理

IBM Spectrum Protect Plus では、Linux 環境で vStorage API for Data Protection (VADP) を使用して、VMware バックアップ・ジョブを実行するプロキシーを作成できます。 これらのプロキシーは、ロード・シェアリングとロード・バランシングを有効にして、システム・リソースに対する要求を軽減します。 スロットルにより、データのスループットを最大化するために、確実に、複数の VADP プロキシーが最適に使用されるようになります。 バックアップされる仮想マシンごとに、IBM Spectrum Protect Plus は、どの VADP プロキシーが一番すいていて、使用可能なメモリーとフリー・タスクが最も多いかを判別します。 フリー・タスクは、使用可能な CPU コア数で判別するか、または「**タスク制限のソフト・キャッピング**」オプションを使用して判別されます。

VADP プロキシーを使用するのに必要なユーザー許可があることを確認してください。VADP プロキシー許可の管理についての説明は、299 ページの『許可タイプ』を参照してください。

VMware 仮想マシンのバックアップには、以下のファイルが含まれます。

- すべてのディスクに対応する VMDK。基本バックアップでは、割り振られているすべてのデータ、またはディスクが NFS データ・ストアにある場合はすべてのデータが取り込まれます。増分バックアップでは、前回の正常なバックアップ以降に変更されたブロックのみが取り込まれます。
- 仮想マシン・テンプレート
- 以下の拡張子がある VMware ファイル
  - .vmx
  - .vmfx (使用可能な場合)
  - .nvram (仮想マシン BIOS の状態を保管)

プロキシーが存在する場合、処理中の負荷全体がホスト・システムからプロキシーにシフトされます。 プロキシーが存在しない場合、負荷全体がホストにとどまります。スロットルにより、データのスループットを最大化するために、確実に、複数の VADP プロキシーが最適に使用されるようになります。 バックアップされる仮想マシンごとに、IBM Spectrum Protect Plus は、どの VADP プロキシーが一番すいていて、使用可能なメモリーとフリー・タスクが最も多いかを判別します。

ジョブの開始前に、プロキシー・サーバーが停止するか、またはその他の理由で使用不能になる場合、他のプロキシーが引き継ぎ、ジョブが完了します。他のプロキシーが存在しない場合、ホストがジョブを引き継ぎます。 ジョブの実行時にプロキシー・サーバーが使用不能になると、ジョブが失敗することがあります。

トランスポート・モードは、VADP プロキシーがデータの移動に使用する方法を示します。トランスポート・モードはプロキシーのプロパティーとして設定されます。大部分のバックアップ・ジョブとリカバリー・ジョブは、1 つ以上のプロキシーを使用するように後で構成されます。

IBM Spectrum Protect Plus の VADP プロキシーは、VMware トランスポート・モード SAN、HotAdd、NBDSSL、および NBD をサポートします。

企業によって異なり、規模、速度、信頼性、複雑度に関する優先順位も環境ごとに異なりますが、以下の一般ガイドラインがトランスポート・モードの選択に適用されます。

- SAN トランスポート・モードは高速で、一般的に信頼性が高いため、直接ストレージ環境ではこのモードを使用する必要があります。
- HotAdd トランスポート・モードは、VADP プロキシーが仮想化される場合に使用する必要があります。このモードは、すべての vSphere ストレージ・タイプをサポートします。
- NBD または NBDSSL トランスポート・モード (LAN) は、物理環境、仮想環境、および混合環境で機能するため、フォールバック・モードです。ただし、このモードでは、ネットワーク接続が低速である場合、データ転送速度が損なわれる可能性があります。NBDSSL モードは NBD モードとほぼ同じですが、NBDSSL を使用する場合、VADP プロキシーと ESXi サーバー間で転送されるデータが暗号化されます。

VADP プロキシーの作成

Linux 環境で IBM Spectrum Protect Plus を使用して VMware バックアップ・ジョブを実行する VADP プロキシーを作成できます。

始める前に

VADP プロキシーを作成する前に以下の考慮事項を確認してください。

- 17 ページの『VADP プロキシー要件』に記載されている IBM Spectrum Protect Plus システム要件を確認します。
- IBM Spectrum Protect Plus バージョンの VADP プロキシー・インストーラーには、Virtual Disk Development Kit (VDDK) バージョン 6.5 が組み込まれています。このバージョンの VADP プロキシー・インストーラーにより、外部 VADP プロキシー・サポートに vSphere 6.5 が提供されます。

手順

VMware VADP プロキシーを作成するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**VADP プロキシー**」をクリックします。
2. 「**プロキシーの登録**」をクリックします。

3. 「**VADP プロキシーのインストール**」ペインで以下のフィールドに入力します。

   ホスト名/IP

   解決可能な IP アドレスまたは解決可能なパスとマシン名を入力してください。

   サイトの選択

   プロキシーに関連付けるサイトを選択します。

   既存のユーザーの使用

   プロバイダー用に以前に入力されたユーザー名とパスワードを選択できるようにします。

   ユーザー名

   VADP プロキシー・サーバーのユーザー名を入力してください。

   パスワード

   VADP プロキシー・サーバーのパスワード名を入力してください。
4. 「**インストール**」をクリックします。
   プロキシーが「**VADP プロキシー**」テーブルに追加されます。
5. 「**登録**」をクリックして、プロキシー・サーバーに登録します。
   「**アクション**」メニューを使用すると、サーバーを登録解除したり一時停止したりできます。 プロキシーを一時停止すると、今後のバックアップ・ジョブがそのプロキシーを使用しないようにするため、一時停止されているプロキシーまたは登録解除されたプロキシーを使用するジョブはローカルで実行され、パフォーマンスに影響する場合があります。プロキシーが一時停止されている間に、保守作業を実行できます。このプロキシーの使用を再開するには、「**アクション**」 > 「**再開**」を選択します。

   正常に登録された後、プロキシー・マシン上でサービス vadp が開始されます。 ログ・ファイル `vadp.log` が `/opt/IBM/SPP/logs` ディレクトリー内に生成されます。
6. 作成するプロキシーごとに、上記のステップを繰り返します。

IBM Spectrum Protect Plus 仮想アプライアンスと 登録済み VADP プロキシーとの間の接続は双方向接続であり、IBM Spectrum Protect Plus 仮想アプライアンスには VADP プロキシーへの接続が、VADP プロキシーには IBM Spectrum Protect Plus 仮想アプライアンスへの 接続が必要です。IBM Spectrum Protect Plus 仮想アプライアンスから VADP プロキシーへの適切な接続を確実なものにするには、以下のステップを実行して、必ず、IBM Spectrum Protect Plus 仮想アプライアンスが VADP プロキシーに ping できるようにします。

1. セキュア・シェル (SSH) ネットワーク・プロトコルを使用して IBM Spectrum Protect Plus 仮想アプライアンスのコマンド・ラインに接続します。
2. `ping <vadp_ip>` を実行します。ここで、<vadp_ip> は、VADP プロキシーの解決可能な IP アドレスです。

ping が失敗する場合は、VADP プロキシーの IP アドレスが解決可能であり、IBM Spectrum Protect Plus アプライアンスでアドレス指定可能であること、および IBM Spectrum Protect Plus アプライアンスから VADP プロキシーまでの経路が存在することを確認してください。ping が正常に実行された場合は、以下の手順を実行して、VADP プロキシーから IBM Spectrum Protect Plus 仮想アプライアンスへ適切に接続されていることを確認してください。

1. セキュア・シェル (SSH) ネットワーク・プロトコルを使用して、VADP プロキシーのコマンド・ラインに接続します。
2. `ping <spectrum_protect_plus_ip>` を実行します。ここで、<spectrum_protect_plus_ip> は IBM Spectrum Protect Plus 仮想アプライアンスの解決可能な IP アドレスです。

ping が失敗する場合は、IBM Spectrum Protect Plus 仮想アプライアンスの IP アドレスが解決可能であり、VADP プロキシーでアドレス指定可能であることを確認してください。VADP プロキシーから IBM Spectrum Protect Plus 仮想アプライアンスまで経路が存在していることを確認します。

次のタスク

VADP プロキシーを作成後、以下のアクションを実行します。

アクション	方法
VMware バックアップ・ジョブを実行する。	103 ページの『VMware データのバックアップ』を参照してください。 プロキシーは、以下のテキストに似たログ・メッセージによりジョブ・ログに記録されます。 `Run remote vmdkbackup of MicroService: http://<proxy>` *nodename*, IP:*proxy_IP_address*

関連タスク

110 ページの『VADP プロキシーのオプションの設定』

Linux 環境で IBM Spectrum Protect Plus を使用して VMware バックアップ・ジョブを実行する VADP プロキシーを作成できます。

VADP プロキシーのオプションの設定

Linux 環境で IBM Spectrum Protect Plus を使用して VMware バックアップ・ジョブを実行する VADP プロキシーを作成できます。

手順

VMware VADP プロキシーのオプションを設定するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**VADP プロキシー**」をクリックします。
2. オプション・アイコン をクリックして、プロキシーの使用可能なオプションを確認します。
3. 「**VADP プロキシー・オプションを設定する**」ペインで以下のフィールドに入力します。

   サイト

   プロキシーにサイトを割り当てます。

   ユーザー

   プロバイダー用に以前に入力されたユーザー名を選択します。VADP プロキシーの自動更新を有効にするには、以前に入力されたユーザー名を選択する必要があります。

   トランスポート・モード

   プロキシーが使用するトランスポート・モードを設定します。 VMware トランスポート・モードについて詳しくは、Virtual Disk Transport Methods を参照してください。

   NBDSSL 圧縮を有効にする

   NBDSSL トランスポート・モードを選択してある場合は、データ転送のパフォーマンスを向上させるために圧縮を有効にします。

   圧縮をオフにするには、「**無効**」を選択します。

   ログの保存日数

   ログが削除される前に保存しておく日数を設定します。

   読み取りおよび書き込みのバッファー・サイズ

   データ転送のバッファー・サイズをバイト単位で設定します。

   NFS ボリュームのブロック・サイズ

   マウントされている NFS ボリュームが使用するブロック・サイズをバイト単位で設定します。

   タスク制限のソフトキャッピング

   プロキシーが処理できる並行 VM の数を設定します。「**すべてのリソースを使用する**」が選択されている場合、以下の式に基づいて、プロキシー上の CPU の数がタスク制限を決定します。

1 CPU = 1 VMDK

CPU は、スレッドを実行できる最小ハードウェア単位です。1 つのプロキシー上の CPU の数は、`lscpu` コマンドを使用して決定されます。

次のタスク

VADP プロキシーの作成後、以下のアクションを実行します。

アクション	方法
VMware バックアップ・ジョブを実行する	103 ページの『VMware データのバックアップ』を参照してください。 プロキシーは、以下のテキストに似たログ・メッセージによりジョブ・ログに記録されます。 `Run remote vmdkbackup of MicroService: http://<proxy` *`nodename`*`, IP:`*`proxy_IP_address`*
VMware バックアップ・ジョブの実行を停止した時点でプロキシーをアンインストールする	プロキシーをアンインストールするには、インストール・ディレクトリー `/opt/IBM/SPP` のアンインストール・サブディレクトリーからホスト・システム上で以下のコマンドを実行します。 `./uninstall_vmdkbackup`

関連タスク

108 ページの『VADP プロキシーの作成』
Linux 環境で IBM Spectrum Protect Plus を使用して VMware バックアップ・ジョブを実行する VADP プロキシーを作成できます。

VADP プロキシーのアンインストール

ご使用の IBM Spectrum Protect Plus 環境から VADP プロキシーを削除することができます。

手順

ご使用の IBM Spectrum Protect Plus から VADP プロキシーをアンインストールするには、以下のステップを実行します。

1. コマンド・プロンプトから、プロキシー・ホスト・システム上のディレクトリー `/opt/IBM/SPP/uninstall` にナビゲートします。
2. 以下のコマンドを実行します。
   `./uninstall_vmdkbackup`

VMware データのリストア

VMware リストア・ジョブは、インスタント VM リストアおよびインスタント・ディスク・リストアのシナリオをサポートします。これらのシナリオは、選択済みのソースに基づいて自動的に作成されます。

始める前に

以下のタスクを実行してください。

- VMware バックアップ・ジョブが少なくとも 1 回実行されていることを確認します。手順については、103 ページの『VMware データのバックアップ』を参照してください。
- IBM Spectrum Protect Plus ユーザーがバックアップおよびリストアの操作を実行できるようにするには、その前に役割をそのユーザーに割り当てる必要があります。「**アカウント**」ペインで、ハイパーバイザーおよびバックアップ/リストア操作へのアクセス権限をユーザーに付与してください。役割および関

連の許可は、ユーザー・アカウントの作成時に割り当てられます。詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』および 301 ページの『ユーザー・アカウントの管理』を参照してください。

- IBM Spectrum Protect リストア・ポイントにリストアされる仮想マシンのサイズは、ソース・プロビジョニングに関係なく、シック・プロビジョン後の仮想マシンのサイズと同じになります。これは、オフロード時に NFS データ・ストアを使用するためです。データのフルサイズがソース 仮想マシンに割り振られない場合でも、フルサイズを転送する必要があります。
- リストア・ジョブに使用する予定の宛先が IBM Spectrum Protect Plus に登録されていることを確認します。この要件は、データを元のホストまたはクラスターにリストアするリストア・ジョブに適用されます。
- 動的ディスクにあるボリュームでの Windows ファイル索引付けおよびファイル・リストアはサポートされていません。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

このタスクについて

VMDK をリストア操作に選択すると、IBM Spectrum Protect Plus は、インスタント・ディスク・リストア・ジョブ用のオプションを自動的に表示して、データおよびアプリケーション・リストア・ポイントへの即時書き込み可能アクセスを提供します。 IBM Spectrum Protect Plus スナップショットがターゲット・サーバーにマップされ、そこで必要に応じてアクセスまたはコピーできるようになります。

その他のソースはすべて、以下のモードで実行可能なインスタント VM リストア・ジョブによってリストアされます。

テスト・モード
テスト・モードでは、一時仮想マシンを作成します。これらの仮想マシンを使用して、開発やテスト、スナップショット検証、および災害復旧検証を、実稼働環境に影響を与えずにスケジュールされた反復可能な方法で行うことができます。テスト・マシンは、テストと検証を完了するために必要な期間は実行され続け、その後にクリーンアップされます。隔離ネットワーキングにより安全な環境を確立し、実動に使用する仮想マシンに干渉せずにジョブをテストすることができます。実稼働環境内での競合を避けるために、テスト・モードで作成された仮想マシンには、固有の名前と ID も与えられます。隔離ネットワークの作成手順については、117 ページの『VMware リストア・ジョブを使用した隔離ネットワークの作成』を参照してください。

クローン・モード
データ・マイニングや隔離ネットワーク内でのテスト環境の複写には、永続コピーや長時間実行コピーが必要なユース・ケースがあります。クローン・モードでは、そのようなユース・ケース用に適した仮想マシンのコピーを作成します。実稼働環境内での競合を避けるために、クローン・モードで作成された仮想マシンには、固有の名前と ID も与えられます。クローン・モードでは、永続仮想マシンまたは長時間実行仮想マシンが作成されるため、リソース使用量に注意する必要があります。

実動モード
実動モードでは、ローカル・サイトで 1 次ストレージまたはリモート災害復旧サイトから災害復旧を実行でき、元のマシン・イメージはリカバリー・イメージに置き換えられます。名前と ID も含め、すべての構成はリカバリーの一部として実行されます。仮想マシンに関連付けられたすべてのコピー・データ・ジョブは、処理を続行します。

手順

VMware リストア・ジョブを定義するには、以下のステップを実行してください。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント：

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**VMware**」をクリックして開くこともできます。

- 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
- ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。

2. 「**ソースの選択**」ページで、以下のアクションを実行します。
   a) 仮想マシン (VM) および仮想ディスク (VDisk) などの使用可能なソースを確認します。「**表示**」フィルターを使用して、表示されたソースを切り替え、ホストとクラスター、VM、またはタグとカテゴリーを表示します。ソースの名前をクリックして、ソースを展開することができます。

   「**検索**」ボックスに名前の全体または一部を入力して、その検索基準に一致する VM を見つけることもできます。名前の全部または一部を表すためにワイルドカード文字 (*) を使用できます。例えば、vm2* は、「vm2」で始まるすべてのリソースを表します。

   b) ソースのリストの横にあるリストア・リストに追加する項目の隣にあるプラス・アイコン をクリックします。同じタイプ (VM または仮想ディスク) の複数の項目を追加できます。

   リストア・リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。

   c) 「**次へ**」をクリックします。
3. 「**ソース・スナップショット**」ページで、リストアする VM または仮想ディスクのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。いくつかのフィールドは、関連フィールドを選択するまで表示されません。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド** 1 回限りのリストア操作を実行します。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。

オプション	説明
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・リストア操作の場合、日付範囲を指定して、その範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・リストア操作の場合は、選択した日付範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、選択したソースごとにリストアするインスタンスを 指定して、「**次へ**」をクリックします。

   オリジナル ESX ホストまたはクラスター
   オリジナルのホストまたはクラスターにデータをリストアするには、このオプションを選択します。

   代替 ESX ホストまたはクラスター
   オリジナルのホストまたはクラスターとは別のローカル宛先にデータをリストアするには、このオプションを選択します。その後、使用可能なリソースから代替ロケーションを選択します。テスト・ネットワークおよび実動ネットワークを代替位置に構成し、隔離ネットワークを作成することができます。隔離ネットワークによって、テストに使用する仮想マシンが実動に使用する仮想マシンに干渉するのを防止できます。「**vCenter**」セクションで、代替位置を選択してください。代替位置は、ホストまたはクラスターのいずれかでフィルタリングできます。

   「**VM フォルダー宛先**」フィールドに、宛先データ・ストア上の仮想マシン・フォルダー・パスを入力します。ディレクトリーは、存在しない場合は作成されることに注意してください。ターゲットのデータ・ストアのルートの仮想マシン・フォルダーには「/」を使用します。

   vCenter がダウンしている場合は ESX ホスト
   vCenter をバイパスしてデータを ESX ホストに直接リストアするには、このオプションを選択します。その他のリストア・シナリオでは、アクションは vCenter を介して実行します。vCenter が利用不可の場合、このオプションは、vCenter 仮想マシン、または vCenter が依存する仮想マシンをリストアします。

5. 「**データ・ストアの設定**」ページで、以下のアクションを実行します。

   - 代替の ESX ホストまたはクラスターにデータをリストアする場合、宛先データ・ストアを選択して、「**次へ**」をクリックします。

- オリジナル ESX ホストまたはクラスターにデータをリストアする場合は、データ・ストアを選択する必要はありません。「**次へ**」をクリックします。

6. 「**ネットワークの設定**」ページで、選択した各ソースに使用するネットワーク設定を指定して、「**次へ**」をクリックします。
   - オリジナルの ESX ホストまたはクラスターにデータをリストアする場合、以下のネットワーク設定を指定します。

     システムで IP 構成を定義できるようにする (Allow system to define IP configuration)
     オペレーティング・システムで宛先 IP アドレスを定義できるようにするには、このオプションを選択します。テスト・モードのリストア操作時に、宛先仮想マシンは、関連付けられている NIC と共に新しい MAC アドレスを受け取ります。新しい IP アドレスは、使用中のオペレーティング・システムに応じて、仮想マシンのオリジナル NIC に基づいて割り当てられるか、DHCP を介して割り当てられます。実動モードのリストア時には、MAC アドレスは変更されません。したがって、IP アドレスを保持する必要があります。

     オリジナルの IP 構成を使用 (Use original IP configuration)
     事前定義の IP アドレス構成を使用してオリジナルのホストまたはクラスターにリストアするには、このオプションを選択します。リストア操作時に、宛先仮想マシンは新しい MAC アドレスを受け取りますが、IP アドレスは保持されます。
   - 代替 ESX ホストまたはクラスターにデータをリストアする場合は、以下の手順を実行します。
     a. 「**実動**」フィールドまたは「**テスト**」フィールドで、実動およびテストのリストア・ジョブ実行用の仮想ネットワークを設定します。隔離ネットワークを作成するには、実稼働環境とテスト環境用の宛先ネットワーク設定を異なる場所に指示する必要があります。隔離ネットワークにより、テストに使用する仮想マシンが実動に使用する仮想マシンに干渉するのを防止できます。テスト・モードおよび実動モードに関連付けられたネットワークは、関連付けられたモードでリストア・ジョブが実行される場合に使用されます。
     b. 開発、テスト、または災害復旧のユース・ケースに転用する仮想マシンに、IP アドレスまたはサブネット・マスクを設定します。サポートされるマッピング・タイプは、IP から IP、IP から DHCP、サブネットからサブネットです。複数の NIC を含む仮想マシンがサポートされます。

        以下のいずれかのアクションを実行します。

        – ご使用のオペレーティング・システムが宛先サブネットおよび IP アドレスを定義できるようにするには、「**宛先の VM ゲスト OS のためにシステム定義のサブネットおよび IP アドレスを使用します**」をクリックします。
        – 事前定義のサブネットおよび IP アドレスを使用するには、「**宛先の VM ゲスト OS のためにオリジナルのサブネットおよび IP アドレスを使用します**」をクリックします。
        – 新規マッピング構成を作成するには、「**宛先の VM ゲスト OS のためにサブネットおよび IP アドレスのマッピングを追加します**」を選択して、「**マッピングの追加**」をクリックし、「**ソース・サブネットまたは IP アドレスを追加します**」フィールドにサブネットまたは IP アドレスを入力します。

          次のネットワーク・プロトコルのいずれかを選択してください。

          - 「**DHCP**」を選択すると、選択済みソースで DHCP が使用可能であれば、IP および関連の構成情報が自動的に選択されます。
          - 特定のサブネット・アドレスまたは IP アドレス、サブネット・マスク、ゲートウェイ、および DNS を入力するには、「**静的**」を選択します。「**サブネット/IP アドレス**」、「**サブネット・マスク**」、および「**ゲートウェイ**」は必須フィールドです。ソースとしてサブネットを入力した場合、宛先としてもサブネットを入力する必要があります。

          静的 IP が使用されているが適切なサブネット・マッピングが検出されない場合、またはソース仮想マシンの電源がオフになっていて関連付けられた NIC が複数ある場合、仮想マシンの IP 再構成はスキップされます。Windows 環境では、仮想マシンが DHCP のみを使用する場合、その仮想マシンの IP 再構成はスキップされます。Linux 環境では、すべてのアドレスは静的と見なされ、IP マッピングのみが使用可能です。

7. 「**リストア方式**」で、ソースの選択内容に合わせて使用するリストア方式を選択します。テスト・モード、実動モード、またはクローン・モードで、VMware リストア・ジョブをデフォルトで実行するよう

に設定します。ジョブが作成された後、「**ジョブ・セッション**」ペインを使用して、そのジョブを実動モードまたはクローン・モードで実行できます。「**VM の名前変更 (オプション)**」フィールドに新しい VM 名を入力することで、リストアされた VM の名前を変更することもできます。「**次へ**」をクリックして先に進みます。

8. 「**ジョブ・オプション (オプション)**」ページで、高度なオプションを構成して、「**次へ**」をクリックします。

   IA® クローン・リソースを永続にします
   仮想ディスクを永続ストレージに移行して一時リソースをクリーンアップするには、このオプションを有効にします。このアクションは、バックグラウンドでリソースの vMotion 操作を開始することによって行われます。vMotion 操作の宛先は VM 構成データ・ストアです。この操作の実行中でも、インスタント・アクセス・ディスクを読み取り/書き込み操作に使用できます。

   リカバリー後の電源オン
   リカバリーの実行後に仮想マシンの電源状態を切り替えます。仮想マシンは、ソースのステップで設定されたように、リカバリーされた順序で電源オン状態になります。

   制約事項 : リストアされた仮想マシン・テンプレートは、リカバリー後に電源オンにできないことに注意してください。

   仮想マシンを上書きします
   選択済み仮想マシンをリストア・ジョブが上書きすることを許可するには、このオプションを有効にします。デフォルトでは、このオプションは無効になっています。

   失敗した場合でもリストアを続行します
   直前のリソース・リカバリーが失敗した場合、シリーズ内でリソースのリカバリーを切り替えます。このオプションを無効にすると、リソースのリカバリーが失敗した場合はリストア・ジョブが停止します。

   ジョブが失敗したとき、即時にクリーンアップを実行します
   仮想マシンのリカバリーが失敗した場合にリストア・ジョブの一部として割り振り済みのリソースを自動的にクリーンアップするには、このオプションを有効にします。

   処理待ちの古いセッションの上書きと強制クリーンアップを許可します。
   リカバリー・ジョブのスケジュール済みセッションで既存の保留セッションでの関連リソースのクリーンアップを強制して、新規セッションを実行できるようにする場合に、このオプションを有効にします。既存のテスト環境をクリーンアップせずに実行を続ける場合は、このオプションを無効にしてください。

   VM タグのリストア
   vSphere を使用して仮想マシンに適用されるタグをリストアするには、このオプションを有効にします。

   欠落しているディスクの VMX ファイルを修正します
   ディスクを個別にバックアップから除外した場合、関連の仮想マシンが始動できなくなります。このオプションを有効にすると、除外したディスクの項目が VMX 構成ファイルから除去され、リストア後の仮想マシンがインスタント VM リストア・ジョブの一部として始動できるようになります。

   仮想マシン名に接尾部を付加します
   リストアされた仮想マシンの名前に付加する接尾部を入力します。

   仮想マシン名の前に接頭部を付加します
   リストアされた仮想マシンの名前に付加する接頭部を入力します。

9. オプション: 「**スクリプトの適用**」ページで、以下のスクリプト・オプションを選択して、「**次へ**」をクリックします。

   - 「**事前スクリプト**」を選択して、アップロード済みのスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択します。スクリプトが実行されるアプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。「**システム構成**」 > 「**スクリプト**」ページに移動して、スクリプトおよびスクリプト・サーバーを構成します。
   - 「**事後スクリプト**」を選択して、アップロード済みのスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択します。スクリプトが実行さ

れるアプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。「**システム構成**」 > 「**スクリプト**」ページにナビゲートして、スクリプトおよびスクリプト・サーバーを構成します。

- ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。このオプションが有効になっている場合、事前スクリプトがゼロ以外の戻りコードで完了すると、バックアップまたはリストアのジョブの実行は続行され、事前スクリプト・タスクの状況は「完了」として返されます。事後スクリプトがゼロ以外の戻りコードで完了すると、事後スクリプト・タスクの状況は「完了」として返されます。このオプションが選択されない場合は、バックアップまたはリストアのジョブは実行されず、事前スクリプトまたは事後スクリプトのタスクの状況は「失敗」状況として返されます。

10. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
    - オンデマンド・ジョブを実行するには、「**次へ**」をクリックします。
    - 反復ジョブをセットアップするには、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
11. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。

    オンデマンド・ジョブは即時に開始されます。繰り返しジョブは、設定された開始時刻に開始されます。

次のタスク

ジョブが完了したら、「**リストア**」ペインの「ジョブ・セッション」セクションまたは「アクティブ・クローン」セクションの「**アクション**」メニューから、以下のいずれかのオプションを選択します。

クリーンアップ

仮想マシンを破棄して、関連のすべてのリソースをクリーンアップします。これはテスト用に使用される一時仮想マシンであるため、仮想マシンが破棄されるとすべてのデータが失われます。

実動に移行 (vMotion)
実動ネットワークとして定義されたデータ・ストアと仮想ネットワークに、vMotion を介して仮想マシンをマイグレーションします。

クローン (vMotion)
テスト・ネットワークとして定義されたデータ・ストアと仮想ネットワークに、vMotion を介して仮想マシンをマイグレーションします。

関連タスク

95 ページの『vCenter Server インスタンスの追加』
vCenter Server インスタンスが IBM Spectrum Protect Plus に追加されると、そのインスタンスのインベントリーがキャプチャーされるため、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

VMware リストア・ジョブを使用した隔離ネットワークの作成

隔離ネットワーキングにより安全な環境を確立し、実動に使用する仮想マシンに干渉せずにジョブをテストすることができます。隔離ネットワーキングは、テスト・モードおよび実動モードで実行されているジョブで使用できます。

始める前に

VMware リストア・ジョブを作成して実行します。手順については、111 ページの『VMware データのリストア』を参照してください。

手順

隔離ネットワークを作成するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**VMware**」をクリックします。
2. 「**リストア**」ペインで、VMware リソース (仮想マシン、VM テンプレート、データ・ストア、フォルダー、vApp など) の使用可能なリストア・ポイントを確認します。検索機能とフィルターを使用して、特

定のリカバリー・サイトのタイプで選択項目を調整します。「**リストア**」ペイン内の項目を展開すると、個々のリストア・ポイントが日付別に表示されます。

3. リストア・ポイントを選択して、「リストア・リストに追加」アイコン  をクリックして、リストア・ポイントを「リソース・リスト」に追加します。「リストア・リスト」から項目を削除するには、削除アイコン  をクリックします。
4. 「**オプション**」をクリックして、ジョブ定義オプションを設定します。
5. 「**代替 ESX ホストまたはクラスター**」を選択して、「vCenter」リストから代替のホストまたはクラスターを選択します。
6. 「**ネットワーク設定**」セクションを展開します。「**実動**」フィールドまたは「**テスト**」フィールドで、実動およびテストのリストア・ジョブ実行用の仮想ネットワークを設定します。隔離ネットワークを作成するには、実稼働環境とテスト環境用の宛先ネットワーク設定を異なる場所に配置する必要があります。隔離ネットワークにより、テストに使用する仮想マシンが実動に使用する仮想マシンに干渉するのを防止できます。テストおよび実動に関連付けられたネットワークは、関連付けられたモードでリストア・ジョブを実行するときに使用されます。ターゲット・マシンの IP アドレスは、以下のオプションを使用して構成できます。

   宛先の VM ゲスト OS のためにシステム定義のサブネットおよび IP アドレスを使用します
   オペレーティング・システムで宛先 IP アドレスを定義できるようにする場合に選択します。テスト・モードのリストア時に、宛先仮想マシンは、関連付けられている NIC と共に新しい MAC アドレスを受け取ります。 新しい IP アドレスは、使用中のオペレーティング・システムに応じて、仮想マシンのオリジナル NIC に基づいて割り当てられるか、DHCP を介して割り当てられます。実動モードのリストア操作時には、MAC アドレスは変更されません。したがって、IP アドレスを保持する必要があります。

   宛先の VM ゲスト OS のためにオリジナルのサブネットおよび IP アドレスを使用します
   事前定義の IP アドレス構成を使用してオリジナルのホストまたはクラスターにリストアする 場合に選択します。リストア時に、宛先仮想マシンは新しい MAC アドレスを受け取りますが、IP アドレスは保持されます。

   リストア用のネットワーク設定を代替または長距離の ESX ホストまたはクラスターに設定します。

   「**実動**」フィールドまたは「**テスト**」フィールドで、実動およびテストのリストア・ジョブ実行用の仮想ネットワークを設定します。隔離ネットワークを作成するには、実稼働環境とテスト環境用の宛先ネットワーク設定を異なる場所に配置する必要があります。隔離ネットワークにより、テストに使用する仮想マシンが実動に使用する仮想マシンに干渉するのを防止できます。テストおよび実動に関連付けられたネットワークは、関連付けられたモードでリストア・ジョブを実行するときに使用されます。

   開発、テスト、または災害復旧のユース・ケースに転用する仮想マシンに、IP アドレスまたはサブネット・マスクを設定します。サポートされるマッピング・タイプは、IP から IP、IP から DHCP、サブネットからサブネットです。複数の NIC を含む仮想マシンがサポートされます。

   デフォルトでは、「**宛先の VM ゲスト OS のためにシステム定義のサブネットおよび IP アドレスを使用します**」オプションは有効になっています。事前定義のサブネットおよび IP アドレスを使用するには、「**宛先の VM ゲスト OS のためにオリジナルのサブネットおよび IP アドレスを使用します**」を選択します。

   新規マッピング構成を作成するには、「**宛先の VM ゲスト OS のためにサブネットおよび IP アドレスのマッピングを追加します**」を選択して、「**マッピングの追加**」をクリックします。 「**ソース**」フィールドにサブネットまたは IP アドレスを入力します。宛先フィールドで「**DHCP**」を選択すると、選択済みクライアントで DHCP が使用可能であれば、IP および関連の構成情報が自動的に選択されます。特定のサブネット・アドレスまたは IP アドレス、サブネット・マスク、ゲートウェイ、および DNS を入力するには、「**静的**」を選択します。「**サブネット / IP アドレス**」、「**サブネット・マスク**」、および「**ゲートウェイ**」は必須フィールドであることに注意してください。ソースとしてサブネットを入力した場合、宛先としてもサブネットを入力する必要があります。

   静的 IP が使用されているが適切なサブネット・マッピングが検出されない場合、またはソース・マシンの電源がオフになっていて関連付けられた NIC が複数ある場合は、仮想マシンの IP 再構成はスキップされます。 Windows 環境では、仮想マシンが DHCP 専用の場合、その仮想マシンの IP 再構成はスキップされます。Linux 環境では、すべてのアドレスは静的と見なされ、IP マッピングのみが使用可能です。

宛先データ・ストア
リストア用の宛先データ・ストアを代替の ESX ホストまたはクラスターに設定します。

VM フォルダー宛先
宛先データ・ストア上の VM フォルダー・パスを入力します。ディレクトリーは、存在しない場合は作成されることに注意してください。ターゲットのデータ・ストアのルート VM フォルダーには「/」を使用します。

7. 「**保存**」をクリックして、ポリシー・オプションを保存します。
8. ジョブが完了したら、「**リストア**」ペインのジョブ・セッションまたは「アクティブ・クローン」セクションの「**アクション**」メニューから、以下のいずれかのオプションを選択します。

クリーンアップ

仮想マシンを破棄して、関連付けられているすべてのリソースをクリーンアップします。これは一時/テスト用の仮想マシンであるため、仮想マシンが破棄されるとすべてのデータが失われます。

実動に移行 (vMotion)

実動ネットワークとして定義されたデータ・ストアと仮想ネットワークに、vMotion を介して仮想マシンをマイグレーションします。

クローン (vMotion)

「テスト」ネットワークとして定義されているデータ・ストアと仮想ネットワークに、vMotion を介して仮想マシンをマイグレーションします。

関連タスク

95 ページの『vCenter Server インスタンスの追加』
vCenter Server インスタンスが IBM Spectrum Protect Plus に追加されると、そのインスタンスのインベントリーがキャプチャーされるため、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

vCenter またはその他の管理 VM にアクセスできない場合のデータのリストア

IBM Spectrum Protect Plus は、vCenter にアクセスできない場合に ESXi ホストを使用して自動的にデータをリストアするためのオプションを提供します。 このオプションは、vCenter 仮想マシン (VM)、または vCenter が依存する VM をリストアします。

このタスクについて

この手順は、ご使用の環境で以下のいずれかの管理サービスが部分的または完全に失われている場合に使用できます。

- vCenter
- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)
- Active Directory (AD)
- ドメイン・ネーム・システム (DNS) サーバー

vCenter を使用せずにデータをリカバリーするには、ESXi ホストに標準スイッチまたは一時バインディング対応の既存の分散スイッチがなければなりません。 これらの要件が満たされていない場合、ESXi ホスト上で新規の標準スイッチを作成する必要があります。 標準スイッチに使用可能なアップリンクがない場合、標準スイッチを分散スイッチから除去する必要があります。

この手順では、vCenter Server (VCS) 環境でリストア操作を実行する場合に、その操作を完了するために必要な追加の手動ステップについて説明します。

VCS 環境内の管理 VM をリカバリーすると、VM へのアクセスが失われる可能性があります。 アクセスが失われるのは、仮想スイッチの誤った構成が原因です。対象の VM 上で以下のステップを実行して、この状態からリカバリーし、リカバリー操作を完了してください。

手順

1. 宛先 ESXi のユーザー・インターフェース ・ホストに接続し、新規の標準仮想スイッチを作成します。この時点で、スイッチに使用できるポート・グループやアップリンクはありません 。
2. SSH プロトコルを使用して、ESXi サーバーに接続します。SDDC-Dswitch-Private という名前の既存の分散仮想スイッチの物理 NIC およびポート・グループを識別して選択します。 以下の例では、ポート ID 64 に属する vmnic0 という名前の仮想ネットワーク・インターフェース ・カード (VNIC) を例に説明しています。 次のコマンドを発行することで、分散仮想スイッチ (DVS) の情報をリストできます。

   ```
   #esxcli network vswitch dvs vmware list
   ```

3. 前のステップで得られた情報に基づいて、次のコマンドを使用して SDDC-Dswitch-Private DVS から NIC およびポート ID (ポート・グループ) を除去します。 ステップ 2 で得られたポート ID を使用します。

   ```
   #esxcfg-vswitch -Q physical_vnic -V port_group SDDC-Dswitch-Private
   ```

4. 次のコマンドを 1 行で発行して、ステップ 1 で作成した標準スイッチに NIC とポート・グループを追加します。

   ```
   #esxcli network vswitch standard uplink add –-uplink-name=physical_vnic --vswitch-
   name=standard_vswitch
   ```

5. ESXi インターフェースで 、ポート・グループを追加し、標準仮想スイッチを選択します。

   仮想スイッチには、1 つのアップリンクと 1 つのポート・グループがなければなりません。
6. 「**vCenter がダウンしている場合は ESX ホスト (ESX host if vCenter is down)**」オプションを有効にして、IBM Spectrum Protect Plus でリストア操作を実行します。
7. IBM Spectrum Protect Plus でリストア操作を定義する場合は、「**オプション**」をクリックし、「**ネットワーキング (Networking)**」の下で、ステップ 1 で作成した新規のネットワーキング・スイッチを選択します。
8. 宛先 ESXI のユーザー・インターフェースを 使用して、リカバリーした VM の電源をオンにします。
9. VM にアクセスできるようになったら、vCenter ユーザー・インターフェースにログインし 、ステップ 5 で作成した一時ポート・グループから元の分散ポート・グループ SDDC-DPortGroup-Mgmt への管理 VM のマイグレーションを開始します。

   「**ネットワーキング (Networking)**」タブで、データ・センターを選択し、「**アクション**」メニューから「**別のネットワークに VM をマイグレーション (Migrate VMs to Another Network)**」をクリックして、マイグレーションを開始します。 ソース・ネットワーク (ステップ 5 で作成した一時スイッチ) と宛先ネットワーク (管理スイッチ) を選択します。
10. すべての VM が元のポート・グループにマイグレーションされたら、以下のアクションを実行して、物理 NIC とポート・グループを元の分散仮想スイッチに再取り込みします。
    a. 次のコマンドを発行して、以前に再割り当てされた標準 vSwitch をネットワーク・カード (vmnic と呼ばれる) から除去します。

       ```
       #esxcli network vswitch standard uplink remove --uplink-name=vmnic --vswitch-name=vSwitch
       ```

       例えば、次のようにします。

       ```
       #esxcli network vswitch standard uplink remove --uplink-name=vmnic0
       ```

       ```
       --vswitch-name=vered_recovery
       ```

    b. 次のコマンドを発行して、ネットワーク・カードを vNetwork 分散スイッチ (vDS) に追加します。

       ```
       #esxcfg-vswitch -P vmnic -V unused_dvPort_ID dvSwitch # add a vDS uplink
       ```

       例えば、次のようにします。

       ```
       #esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
       ```

11. 一時ポート・グループと標準 vSwitch を ESXi ホスト・ユーザー・インターフェースから 除去します。
12. VM がマイグレーションされてアクセス可能になった後、元のホストにアクセス可能な場合は、ESXI ホスト・ユーザー・インターフェースを 使用して古い VM を登録抹消します (削除はしません)。この方法を使用することで、重複する情報 (名前、メディア・アクセス制御 (MAC) アドレス、オペレーティング・システム・レベル ID、VM の汎用固有 ID (UUID) など) が作成されないようにします。 このステップは、新規データ・ストアを使用する場合も実行する必要があります。

    一部のバージョンの vSphere または ESXi では、「**インベントリーから除去 (Remove from inventory)**」オプションを使用して登録抹消操作を実行することができます。これにより、VM は vCenter カタログから登録抹消されますが、VMDK ファイルはデータ・ストア上に残ります。そのため、データ・ストアのストレージ・スペースが使用されます。 VM が完全にリカバリーされ、環境が正常に稼働した後、これらのファイルをデータ・ストアから手動で削除することで、スペースを回復することができます。

Hyper-V データのバックアップとリストア

Hyper-V データを保護するには、最初に IBM Spectrum Protect Plus に Hyper-V サーバーを追加してから、サーバーのコンテンツに対するバックアップ操作とリストア操作のジョブを作成します。

ご使用の Hyper-V 環境が 22 ページの『ハイパーバイザー要件』 のシステム要件を満たしていることを確認してください。

Hyper-V サーバーの追加

Hyper-V サーバーが IBM Spectrum Protect Plus に追加されると、サーバーのインベントリーがキャプチャーされるため、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

始める前に

Hyper-V サーバーを IBM Spectrum Protect Plus に追加する前に、以下の考慮事項と手順に注意してください。

- Hyper-V サーバーは、DNS ネームまたは IP アドレスを使用して登録できます。DNS ネームは、IBM Spectrum Protect Plus によって解決可能でなければなりません。Hyper-V サーバーがクラスターの一部である場合、クラスター内のすべてのノードが DNS を使用して解決可能でなければなりません。DNS を使用できない場合は、サーバーを IBM Spectrum Protect Plus アプライアンス上の `/etc/hosts` ファイルに追加する必要があります。クラスター環境で複数の Hyper-V サーバーがセットアップされている場合、すべてのサーバーを `/etc/hosts` に追加する必要があります。 IBM Spectrum Protect Plus にクラスターを登録する際、フェイルオーバー・クラスター・マネージャーを登録してください。
- クラスター・ノードを含むすべての Hyper-V サーバーで、それらのサーバーの「サービス」リストにある Microsoft iSCSI イニシエーター・サービスが実行されている必要があります。サービスを「自動」に設定し、マシンのブート時にサービスが有効になるようにします。
- Hyper-V サーバーのローカル管理者グループにユーザーを追加します。

手順

Hyper-V サーバーを追加するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**Hyper-V**」をクリックします。
2. 「**Hyper-V サーバーの管理**」をクリックします。
3. 「**Hyper-V サーバーの追加**」をクリックします。
4. 「**サーバー・プロパティー**」ペインのフィールドにデータを設定します。

ホスト名/IP
解決可能な IP アドレスまたは解決可能なパスとマシン名を入力します。

既存のユーザーの使用
サーバーについて以前に入力済みのユーザー名とパスワードを選択できます。

ユーザー名
サーバーのユーザー名を入力します。

パスワード
サーバーのパスワードを入力します。

ポート
追加しているサーバーの通信ポートを入力します。通常、デフォルトのポートは 5985 です。

暗号化された Secure Sockets Layer (SSL) 接続を有効にするには、「**SSL の使用**」チェック・ボックスを選択します。

SLL 接続を有効にするには、Hyper-V サーバーの自己署名 SSL 証明書または認証局 (CA) 証明書を追加する必要があります。証明書のアップロードについては、276 ページの『管理コンソールからの SSL 証明書のアップロード』を参照してください。

「**SSL の使用**」を選択しない場合は、Hyper-V サーバーで追加のステップを実行する必要があります。122 ページの『Hyper-V サーバーに接続するための WinRM の有効化』を参照してください。

5. 「**オプション**」セクションで、以下のオプションを構成します。

Hyper-V サーバーごとに同時に処理する VM の最大数
Hyper-V サーバーを処理するための同時仮想マシン・スナップショットの最大数を設定します。

6. 「**保存**」をクリックします。IBM Spectrum Protect Plus により、ネットワーク接続が確認され、サーバーがデータベースに追加され、サーバーがカタログされます。

接続が失敗したことを示すメッセージが表示される場合は、項目を確認してください。項目が正確であっても接続が失敗する場合は、システム管理者に連絡して接続を確認してください。

次のタスク

Hyper-V サーバーを追加した後、以下のアクションを実行します。

アクション	方法
ハイパーバイザーにユーザー許可を割り当てます。	298 ページの『役割の作成』を参照してください。

関連タスク

123 ページの『Hyper-V データのバックアップ』
スナップショットを使用して Hyper-V データをバックアップするには、バックアップ・ジョブを使用します。

127 ページの『Hyper-V データのリストア』
Hyper-V リストア・ジョブは、インスタント VM リストアおよびインスタント・ディスク・リストアのシナリオをサポートします。これらは、選択されるソースに基づいて自動的に作成されます。

Hyper-V サーバーに接続するための WinRM の有効化

IBM Spectrum Protect Plus Hyper-V サーバー間で暗号化されたネットワーク・トラフィックを有効にするために SSL を使用できない場合は、暗号化されていないネットワーク・トラフィックを許可するように、ホストで WinRM を構成する必要があります。暗号化されていないネットワーク・トラフィックを許可すると、それに伴うセキュリティー・リスクが生じることを理解しておいてください。

手順

Hyper-V ホストに接続するために WinRM を構成するには、以下のようにします。

1. Hyper-V ホスト・システムで、管理者アカウントを使用してログインします。
2. Windows コマンド・プロンプトを開きます。ユーザー・アカウント制御 (UAC) が有効になっている場合は、「管理者として実行」オプションを有効にして実行することで上位の特権でコマンド・プロンプトを開く必要があります。
3. 次のコマンドを入力して、暗号化されていないネットワーク・トラフィックを許可するように WinRM を構成します。

```
winrm s winrm/config/service @{AllowUnencrypted="true"}
```

4. 次のコマンドを使用して、AllowUnencrypted オプションが true に設定されていることを確認します。

```
winrm g winrm/config/service
```

Hyper-V リソースの検出

Hyper-V リソースは、Hyper-V サーバーが IBM Spectrum Protect Plus に追加されると、自動的に検出されます。しかし、インベントリー・ジョブを実行して、サーバーが追加された後で行われた変更を検出することができます。

手順

インベントリー・ジョブを実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**Hyper-V**」をクリックします。
2. Hyper-V サーバーのリストで、サーバーを選択するか、必要なリソースにナビゲートできるサーバーのリンクをクリックします。例えば、サーバー内の個別の仮想マシンについてインベントリー・ジョブを実行したい場合は、サーバー・リンクをクリックしてから、仮想マシンを選択してください。
3. 「**インベントリーの実行**」をクリックします。

Hyper-V サーバー仮想マシンへの接続のテスト

Hyper-V サーバー仮想マシンへの接続をテストすることができます。テスト機能は、仮想マシンとの通信を検証し、IBM Spectrum Protect 仮想アプライアンスと 仮想マシンとの間で DNS 設定をテストします。

手順

接続をテストするには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**Hyper-V**」をクリックします。
2. Hyper-V サーバーのリストで、Hyper-V サーバー仮想マシンが個々の仮想マシンにナビゲートできるリンクをクリックします。
3. 仮想マシンを選択してから、「**オプションの選択**」をクリックします。
4. 「**既存のユーザーの使用**」を選択します。
5. 「**ユーザーの選択**」リストでユーザーを選択します。
6. 「**テスト**」をクリックします。

Hyper-V データのバックアップ

スナップショットを使用して Hyper-V データをバックアップするには、バックアップ・ジョブを使用します。

始める前に

バックアップ・ジョブ定義を作成する前に、以下の手順と考慮事項に注意してください。

- バックアップするプロバイダーを登録します。詳しくは、121 ページの『Hyper-V サーバーの追加』を参照してください。
- SLA ポリシーを構成します。手順については、73 ページの『バックアップ・ポリシーの作成』を参照してください。
- Hyper-V のバックアップとリストアのジョブでは、最新の Hyper-V 統合サービスのインストールが必要になります。

  Microsoft Windows 環境の場合は、Windows サーバー上の Hyper-v でサポートされる Windows ゲスト・オペレーティング・システムを参照してください。

  Linux 環境の場合は、Supported Linux and FreeBSD virtual machines for Hyper-V on Windows を参照してください。
- クラスター・ノードを含むすべての Hyper-V サーバーで、それらのサーバーの「サービス」リストにある Microsoft iSCSI イニシエーター・サービスが実行されている必要があります。サービスを「自動」に設定し、マシンのブート時にサービスが有効になるようにします。
- IBM Spectrum Protect Plus ユーザーがバックアップとリストアの 操作を実行するには、その前に、そのユーザーに役割が割り当てられる必要があります。「**アカウント**」ペインで、ハイパーバイザーおよびバックアップとリストアの操作に対するアクセス権限をユーザーに付与します。役割および関連した許可

は、ユーザー・アカウントの作成時に割り当てられます。詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』および 301 ページの『ユーザー・アカウントの管理』を参照してください。

- 仮想マシンが複数の SLA ポリシーに関連付けられている場合は、それらのポリシーを並行実行のスケジュールに入れないでください。SLA ポリシーの相互の実行間隔を相当離してスケジュールに入れるか、全体を結合して単一の SLA ポリシーにしてください。
- 最初の Hyper-V 基本バックアップが作成された後で IBM Spectrum Protect Plus アプライアンスの IP アドレスが変更された場合、Hyper-V リソースのターゲット IQN が不正な状態のままになっている可能性があります。この問題を修正するには、Microsoft iSCSI イニシエーター・ツールで「**Discovery**」タブをクリックします。以前の IP アドレスを選択して、「**Remove**」をクリックします。「**Target**」タブをクリックして、再接続中のセッションを切断します。
- VM が SLA ポリシーで保護されている場合、VM のバックアップは、VM が削除された後でも、SLA ポリシーの保存パラメーターに基づいて保存されます。

手順

Hyper-V バックアップ・ジョブを定義するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**Hyper-V**」をクリックします。
2. バックアップするリソースを選択します。

   検索機能を使用して使用可能なリソースを検索し、表示されたリソースを「**表示**」フィルターで切り替えます。選択可能なオプションは、「**VM**」および「**データ・ストア**」です。
3. 「**SLA ポリシーの選択**」をクリックして、バックアップ・データ基準に合った 1 つ以上の SLA ポリシーをジョブ定義に追加します。
4. デフォルトのオプションを使用してジョブ定義を作成するには、「**保存**」をクリックします。

   ジョブは、選択した SLA ポリシーで定義されたとおりに実行されます。ジョブを手動で実行するには、「**ジョブと操作**」 > 「**スケジュール**」をクリックします。ジョブを選択して、「**アクション**」 > 「**開始**」をクリックします。

   ヒント:「**実行**」ボタンは単一のハイパーバイザー・バックアップについてのみ有効であり、該当のハイパーバイザーに SLA ポリシーが適用されている必要があります。
5. ジョブを開始する前にオプションを編集するには、テーブル「**オプションの選択**」の編集アイコンをクリックします。

   「**バックアップ・オプション**」セクションで、以下のジョブ定義オプションを設定します。

   読み取り専用データ・ストアをスキップします

   読み取り専用としてマウントされているデータ・ストアをスキップできます。

   インスタント・アクセス用にマウントされた一時データ・ストアをスキップします

   一時インスタント・アクセス・データ・ストアをバックアップ・ジョブ定義から除外できます。

   優先度

   選択済みリソースのバックアップ優先度を設定します。優先度設定の高いリソースがジョブで最初にバックアップされます。「**VMware バックアップ**」セクションで優先度付けするリソースをクリックしてから、「**優先度**」フィールドにバックアップ優先度を設定してください。 最高優先度には 1 を、最低優先度には 10 を設定します。優先度の値を設定していない場合、デフォルトで優先度 5 が自動的に割り当てられます。

   「**スナップショット・オプション**」セクションで、以下のジョブ定義オプションを設定します。

   VM スナップショット・アプリケーション/ファイル・システムを整合させてください

   仮想マシン・スナップショットに対するアプリケーションまたはファイル・システムの整合性をオンにする場合に、このオプションを有効にします。

   VM スナップショットの再試行回数

   IBM Spectrum Protect Plus がジョブをキャンセルする前に仮想マシンのスナップショットを試行する回数を設定します。

   「**エージェント・オプション**」セクションで、以下のジョブ定義オプションを設定します。

SQL ログの切り捨て

バックアップ・ジョブ中に SQL のアプリケーション・ログを切り捨てるには、「**SQL ログの切り捨て**」オプションを有効にします。バックアップ・ジョブ定義の中で「ゲスト OS のユーザー名」オプションと「ゲスト OS のパスワード」オプションを使用して、関連する仮想マシンの資格情報が設定されている必要があることに注意してください。仮想マシンがドメインに接続されている場合、ユーザー ID の形式はデフォルトの *domain¥name* です。ユーザーがローカル管理者である場合は、*local_administrator* 形式が使用されます。

このユーザー ID にはローカル管理者特権が必要です。さらに、SQL Server では、システム・ログイン資格情報に対して、SQL sysadmin 権限が有効になっているほか、「**サービスとしてログオン**」権限が設定されている必要があります。この権限について詳しくは、Add the Log on as a service Right to an Account を参照してください。

IBM Spectrum Protect Plus は、ログ切り捨て機能に関連するログを生成して、IBM Spectrum Protect Plus アプライアンス上の以下の場所にコピーします。

```
/data/log/guestdeployer/latest_date/latest_entry/vm_name
```

ここで、*latest_date* はバックアップ・ジョブとログ切り捨てが行われた日付、*latest_entry* はジョブの汎用固有 ID (UUID)、*vm_name* はログ切り捨てが行われた VM のホスト名または IP アドレスです。

制約事項 : ファイルの索引付けおよびファイル・リストアは、IBM Spectrum Protect サーバーにオフロードされたリストア・ポイントからはサポートされません。

カタログ・ファイル・メタデータ

関連するスナップショットのファイルの索引付けをオンにするには、「カタログ・ファイル・メタデータ」オプションを有効にします。ファイルの索引付けが完了した後、IBM Spectrum Protect Plus の「**ファイル・リストア**」ペインを使用して個々のファイルをリストアできます。バックアップ・ジョブ定義の中で SSH 鍵、または「ゲスト OS のユーザー名」オプションと「ゲスト OS のパスワード」オプションを使用して、関連する仮想マシンの資格情報が設定されている必要があることに注意してください。IBM Spectrum Protect Plus アプライアンスから DNS またはホスト名を使用して仮想マシンにアクセスできることを確認してください。SSH 鍵は、Windows プラットフォームでは有効な許可メカニズムではないことに注意してください。

除外するファイル

ファイルの索引付けの実行時にスキップするディレクトリーを入力します。これらのディレクトリー内のファイルは、IBM Spectrum Protect Plus カタログに追加されず、ファイル・リカバリーに使用できません。 ディレクトリーを除外するには、完全一致を使用するか、あるいは、パターンの前 (*test) またはパターンの後 (test*) にワイルドカード・アスタリスクを指定します。単一パターン内で複数のアスタリスク・ワイルドカードを指定することもできます。パターンでは、標準の英数字のほか、特殊文字 -、_、および * を使用できます。複数のフィルターはセミコロンで区切ります。

既存のユーザーの使用

プロバイダーについて以前に入力済みのユーザー名とパスワードを選択できます。

ゲスト OS のユーザー名/パスワード

一部のタスク (ファイル・メタデータのカタログ、ファイル・リストア、IP 再構成など) では、関連する仮想マシンの資格情報が設定されている必要があります。ユーザー名とパスワードを入力して、IBM Spectrum Protect Plus アプライアンスから DNS またはホスト名を使用して仮想マシンにアクセスできることを確認してください。

デフォルトのセキュリティー・ポリシーでは Windows NTLM プロトコルを使用します。また、Hyper-V 仮想マシンがドメインに接続されている場合、ユーザー ID の形式はデフォルトの *domain¥name* です。ユーザーがローカル管理者である場合は、*local_administrator* 形式が使用されます。

6. ハイパーバイザー仮想マシンへの接続のトラブルシューティングを 行うには、「**テスト**」機能を使用します。

「**テスト**」機能により、仮想マシンとの通信が検査され、IBM Spectrum Protect Plus アプライアンスと仮想マシンの間の DNS 設定がテストされます。接続をテストするには、単一の仮想マシンを選択して、「**オプションの選択**」をクリックします。「**既存のユーザーの使用**」を選択して、リソースについて以前

に入力済みのユーザー名とパスワードを選択します。「**テスト**」ボタンは、「**オプション**」セクションの「**保存**」ボタンの右側に表示されます。「**テスト**」をクリックします。

7. 「**保存**」をクリックします。
8. 追加のオプションを構成するには、「**SLA ポリシーのステータス**」セクションで、ジョブに関連付けられている「**ポリシー・オプション**」フィールドをクリックします。追加のポリシー・オプションを設定します。

   事前スクリプトと事後スクリプト

   事前スクリプトまたは事後スクリプトを実行します。事前スクリプトおよび事後スクリプトは、ジョブの実行前または実行後にジョブ・レベルで実行できるスクリプトです。Windows ベースのマシンはバッチ・スクリプトと PowerShell スクリプトをサポートし、Linux レベルのマシンはシェル・スクリプトをサポートしています。

   「**事前スクリプト**」セクションまたは「**事後スクリプト**」セクションで、アップロード済みのスクリプトと、スクリプトが実行されるスクリプト・サーバーを選択します。スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成されます。

   ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。

   このオプションが有効になっている場合、事前スクリプトまたは事後スクリプトの処理がゼロ以外の戻りコードで完了すると、バックアップまたはリストアの操作は試行され、事前スクリプト・タスクの状況は「完了」として報告されます。事後スクリプトがゼロ以外の戻りコードで完了すると、事後スクリプト・タスクの状況は「完了」として報告されます。

   このオプションが無効になっている場合は、バックアップまたはリストアは試行されず、事後スクリプトまたは事後スクリプトのタスク状況は「失敗」として報告されます。

   バックアップ前にインベントリーを実行

   バックアップ・ジョブを開始する前に、インベントリー・ジョブを実行し、選択されたリソースの最新データを取り込みます。

   リソースの除外

   単一または複数の除外パターンを使用して、特定のリソースをバックアップ・ジョブから除外します。リソースを除外するには、完全一致を使用するか、あるいは、パターンの前 (*test) またはパターンの後 (test*) にワイルドカード・アスタリスクを指定します。

   単一パターン内で複数のアスタリスク・ワイルドカードを指定することもできます。パターンでは、標準の英数字のほか、特殊文字 -、_、および * を使用できます。

   複数のフィルターはセミコロンで区切ります。

   リソースのフルバックアップを 強制します

   バックアップ・ジョブ定義の特定の仮想マシンまたはデータベースに対して基本バックアップ操作を強制的に実行します。複数のリソースはセミコロンで区切ります。
9. 構成した追加のオプションを保存するには、「**保存**」をクリックします。

次のタスク

バックアップ・ジョブを定義した後、以下のアクションを実行します。

アクション	方法
Hyper-V リストア・ジョブ定義を作成します。	127 ページの『Hyper-V データのリストア』を参照してください。

関連概念

250 ページの『バックアップ操作とリストア操作のスクリプトの構成』
事前スクリプトと事後スクリプトは、バックアップ・ジョブとリストア・ジョブがジョブ・レベルで実行される前または後に実行できるスクリプトです。サポートされるスクリプトには、Linux ベースのマシン用のシェル・スクリプトや、Windows ベースのマシン用の Batch および PowerShell スクリプトがあります。

スクリプトはローカル側で作成され、「**スクリプト**」ページを使用して環境にアップロードされてから、ジョブ定義に適用されます。

関連タスク

248 ページの『ジョブの開始』
いずれのジョブも、スケジュールで実行するよう設定されている場合でも、オンデマンドで実行できます。

Hyper-V データのリストア

Hyper-V リストア・ジョブは、インスタント VM リストアおよびインスタント・ディスク・リストアのシナリオをサポートします。これらは、選択されるソースに基づいて自動的に作成されます。

始める前に

以下のタスクを実行してください。

- Hyper-V バックアップ・ジョブが少なくとも 1 回実行されていることを確認します。手順については、123 ページの『Hyper-V データのバックアップ』を参照してください。
- リストア・ジョブに使用する予定の宛先が IBM Spectrum Protect Plus に登録されていることを確認します。この要件は、データを元のホストまたはクラスターにリストアするリストア・ジョブに適用されます。
- 最新の Hyper-V 統合サービスがインストールされていることを確認します。

  Microsoft Windows 環境の場合は、Windows サーバー上の Hyper-v でサポートされる Windows ゲスト・オペレーティング・システムを参照してください。

  Linux 環境の場合は、Supported Linux and FreeBSD virtual machines for Hyper-V on Windows を参照してください。
- 影響を受けるユーザーにリストア操作に適切な役割が割り当てられていることを確認します。「**アカウント**」ペインで、ハイパーバイザーおよびバックアップ/リストア操作へのアクセス権限をユーザーに付与してください。役割および関連した許可は、ユーザー・アカウントの作成時に割り当てられます。手順については、293 ページの『第 13 章 ユーザー・アクセスの管理』および 301 ページの『ユーザー・アカウントの管理』を参照してください。
- 動的ディスクにあるボリュームでの Windows ファイル索引付けおよびファイル・リストアはサポートされていません。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

このタスクについて

仮想ハード・ディスク (VHDX) をリストア・ジョブの対象に選択すると、IBM Spectrum Protect Plus は、インスタント・ディスク・リストア・ジョブ用のオプションを自動的に表示します。これにより、データおよびアプリケーションのリストア・ポイントへの即時書き込み可能アクセスが提供されます。

IBM Spectrum Protect Plus スナップショットがターゲット・サーバーにマップされ、そこで必要に応じてスナップショットにアクセスしたり、スナップショットをコピーしたりできるようになります。その他のソースはすべて、以下のモードで実行可能なインスタント VM リストア・ジョブを使用してリストアされます。

テスト・モード
テスト・モードでは、一時仮想マシンが作成されます。これらの仮想マシンを使用して、実稼働環境に影響を与えることなく、開発テスト、スナップショット検証、および災害復旧検証をスケジュールに従って繰り返し行うことができます。テスト・マシンは、テストと検証を完了するために必要な期間は実行され続け、その後にクリーンアップされます。隔離ネットワーキングにより安全な環境を確立し、実動に使用する仮想マシンに干渉せずにジョブをテストすることができます。実稼働環境内での競合を避けるために、テスト・モードで作成された仮想マシンには、固有の名前と ID も与えられます。

クローン・モード
データ・マイニングや隔離ネットワーク内でのテスト環境の複写には、永続コピーや長時間実行コピーが必要なユース・ケースがあります。クローン・モードでは、そのようなユース・ケース用に適した仮

想マシンのコピーを作成します。実稼働環境内での競合を避けるために、クローン・モードで作成された仮想マシンには、固有の名前と ID も与えられます。クローン・モードでは、永続仮想マシンまたは長時間実行仮想マシンが作成されるため、リソース使用量に注意する必要があります。

実動モード
実動モードでは、ローカル・サイトで 1 次ストレージまたはリモート災害復旧サイトから災害復旧を実行でき、元のマシン・イメージはリカバリー・イメージに置き換えられます。名前と ID も含め、すべての構成はリカバリーの一部として実行されます。仮想マシンに関連付けられたすべてのコピー・データ・ジョブは、処理を続行します。

制約事項 : Hyper-V では、テスト・モードから実動モードへの移行はサポートされていません。

手順

Hyper-V リストア・ジョブを定義するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ハイパーバイザー**」 > 「**Hyper-V**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント :

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Hyper-V**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。

2. 「**ソースの選択**」ページで、以下のアクションを実行します。
   a) 仮想マシン (VM) および仮想ディスク (VDisk) などの使用可能なソースを確認します。ソースの名前をクリックして、ソースを展開することができます。

   「**検索**」ボックスに名前の全体または一部を入力して、その検索基準に一致する VM を見つけることもできます。名前の全部または一部を表すためにワイルドカード文字 (*) を使用できます。例えば、vm2* は、「vm2」で始まるすべてのリソースを表します。

   b) ソースのリストの横にあるリストア・リストに追加する項目の隣にあるプラス・アイコン をクリックします。同じタイプ (VM または仮想ディスク) の複数の項目を追加できます。

   リストア・リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。

   c) 「**次へ**」をクリックします。

3. 「**ソース・スナップショット**」ページで、リストアする VM または仮想ディスクのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。いくつかのフィールドは、関連フィールドを選択するまで表示されません。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド** 1 回限りのリストア操作を実行します。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。

オプション	説明
	クラウド・オフロード スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・リストア操作の場合、日付範囲を指定して、その範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・リストア操作の場合は、選択した日付範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、選択したソースからリストアされるインスタンスを 選択して、「**次へ**」をクリックします。

   オリジナル Hyper-V ホストまたはクラスター
   オリジナルのホストまたはクラスターにデータをリストアするには、このオプションを選択します。

   代替 Hyper-V ホストまたはクラスター
   オリジナルのホストまたはクラスターとは別のローカル宛先にデータをリストアするには、このオプションを選択します。その後、使用可能なリソースから代替ロケーションを選択します。

「**VM フォルダー宛先**」フィールドに、宛先データ・ストア上の仮想マシン・フォルダー・パスを入力します。ディレクトリーは、存在しない場合は作成されることに注意してください。ターゲットのデータ・ストアのルートの仮想マシン・フォルダーには「/」を使用します。

5. 「**データ・ストアの設定**」ページで、以下のアクションを実行します。
   - 代替の Hyper-V ホストまたはクラスターにデータをリストアする場合、宛先データ・ストアを選択して、「**次へ**」をクリックします。
   - オリジナル ESX ホストまたはクラスターにデータをリストアする場合は、データ・ストアを選択する必要はありません。「**次へ**」をクリックしてください。
6. 「**ネットワークの設定**」ページで、選択した各ソースに使用するネットワーク設定を指定して、「**次へ**」をクリックします。
   - オリジナルの Hyper-V ホストまたはクラスターにデータをリストアする場合、以下のネットワーク設定を指定します。

     システムで IP 構成を定義できるようにする (Allow system to define IP configuration)
     オペレーティング・システムで宛先 IP アドレスを定義できるようにするには、このオプションを選択します。テスト・モードのリストア操作時に、宛先仮想マシンは、関連付けられている NIC と共に新しい MAC アドレスを受け取ります。新しい IP アドレスは、使用中のオペレーティング・システムに応じて、仮想マシンのオリジナル NIC に基づいて割り当てられるか、DHCP を介して割り当てられます。実動モードのリストア時には、MAC アドレスは変更されません。したがって、IP アドレスを保持する必要があります。

     オリジナルの IP 構成を使用 (Use original IP configuration)
     事前定義の IP アドレス構成を使用してオリジナルのホストまたはクラスターにリストアするには、このオプションを選択します。リストア操作時に、宛先仮想マシンは新しい MAC アドレスを受け取りますが、IP アドレスは保持されます。
   - 代替 Hyper-V ホストまたはクラスターにデータをリストアする場合は、以下の手順を実行します。

     a. 「**実動**」フィールドまたは「**テスト**」フィールドで、実動およびテストのリストア・ジョブ実行用の仮想ネットワークを設定します。隔離ネットワークを作成するには、実稼働環境とテスト環境用の宛先ネットワーク設定を異なる場所に指示する必要があります。隔離ネットワークにより、テストに使用する仮想マシンが実動に使用する仮想マシンに干渉するのを防止できます。テスト・モードおよび実動モードに関連付けられたネットワークは、関連付けられたモードでリストア・ジョブが実行される場合に使用されます。

     b. 開発、テスト、または災害復旧のユース・ケースに転用する仮想マシンに、IP アドレスまたはサブネット・マスクを設定します。サポートされるマッピング・タイプは、IP から IP、IP から DHCP、サブネットからサブネットです。複数の NIC を含む仮想マシンがサポートされます。

     以下のいずれかのアクションを実行します。

     – ご使用のオペレーティング・システムが宛先サブネットおよび IP アドレスを定義できるようにするには、「**宛先の VM ゲスト OS のためにシステム定義のサブネットおよび IP アドレスを使用します**」をクリックします。

     – 事前定義のサブネットおよび IP アドレスを使用するには、「**宛先の VM ゲスト OS のためにオリジナルのサブネットおよび IP アドレスを使用します**」をクリックします。

     – 新規マッピング構成を作成するには、「**宛先の VM ゲスト OS のためにサブネットおよび IP アドレスのマッピングを追加します**」を選択して、「**マッピングの追加**」をクリックし、「**ソース・サブネットまたは IP アドレスを追加します**」フィールドにサブネットまたは IP アドレスを入力します。

       次のネットワーク・プロトコルのいずれかを選択してください。

       - 「**DHCP**」を選択すると、選択済みソースで DHCP が使用可能であれば、IP および関連の構成情報が自動的に選択されます。
       - 特定のサブネット・アドレスまたは IP アドレス、サブネット・マスク、ゲートウェイ、および DNS を入力するには、「**静的**」を選択します。「**サブネット/IP アドレス**」、「**サブネット・マスク**」、および「**ゲートウェイ**」は必須フィールドです。ソースとしてサブネットを入力した場合、宛先としてもサブネットを入力する必要があります。

静的 IP が使用されているが適切なサブネット・マッピングが検出されない場合、またはソース仮想マシンの電源がオフになっていて関連付けられた NIC が複数ある場合、仮想マシンの IP 再構成はスキップされます。Windows 環境では、仮想マシンが DHCP のみを使用する場合、その仮想マシンの IP 再構成はスキップされます。Linux 環境では、すべてのアドレスは静的と見なされ、IP マッピングのみが使用可能です。

7. 「**リストア方式**」で、ソースの選択内容に合わせて使用するリストア方式を選択します。Hyper-V リストア・ジョブがデフォルトでテスト・モード、実動モード、またはクローン・モードで実行されるように設定します。ジョブが作成された後、「**ジョブ・セッション**」ペインを使用して、そのジョブを実動モードまたはクローン・モードで実行できます。「**VM の名前変更 (オプション)**」フィールドに新しい VM 名を入力することで、リストアされた VM の名前を変更することもできます。「**次へ**」をクリックして先に進みます。
8. オプション: 「**ジョブ・オプション (オプション)**」ページで、高度なオプションを構成して、「**次へ**」をクリックします。

   IA クローン・リソースを永続にします
   仮想ディスクを永続ストレージに移行して一時リソースをクリーンアップするには、このオプションを有効にします。このアクションは、バックグラウンドでリソースの vMotion 操作を開始することによって行われます。vMotion 操作の宛先は VM 構成データ・ストアです。この操作の実行中でも、インスタント・アクセス・ディスクを読み取り/書き込み操作に使用できます。

   リカバリー後に電源をオンにします
   リカバリーの実行後に仮想マシンの電源状態を切り替えます。仮想マシンは、ソースのステップで設定されたように、リカバリーされた順序で電源オン状態になります。

   制約事項 : リストアされた仮想マシン・テンプレートは、リカバリー後に電源オンにできないことに注意してください。

   仮想マシンを上書きします
   選択済み仮想マシンをリストア・ジョブが上書きすることを許可するには、このオプションを有効にします。デフォルトでは、このオプションは無効になっています。

   失敗した場合でもリストアを続行します
   直前のリソース・リカバリーが失敗した場合にリソースのリカバリーを順番に切り替えます。このオプションを無効にすると、リソースのリカバリーが失敗した場合にリストア・ジョブは停止します。

   ジョブが失敗したとき、即時にクリーンアップを実行します
   仮想マシンのリカバリーが失敗した場合にリストア・ジョブの一部として割り振り済みのリソースを自動的にクリーンアップするには、このオプションを有効にします。

   処理待ちの古いセッションの上書きと強制クリーンアップを許可します。
   リカバリー・ジョブのスケジュール済みセッションで既存の保留セッションでの関連リソースのクリーンアップを強制して、新規セッションを実行できるようにする場合に、このオプションを有効にします。既存のテスト環境をクリーンアップせずに実行を続ける場合は、このオプションを無効にしてください。

   仮想マシン名に接尾部を付加します
   リストアされた仮想マシンの名前に付加する接尾部を入力します。

   仮想マシン名の前に接頭部を付加します
   リストアされた仮想マシンの名前に付加する接頭部を入力します。「保存」をクリックして、ポリシー・オプションを保存します。
9. オプション: 「**スクリプトの適用**」ページで、以下のスクリプト・オプションを選択して、「**次へ**」をクリックします。

   - 「**事前スクリプト**」を選択して、アップロード済みのスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択します。スクリプトが実行されるアプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。「**システム構成**」 > 「**スクリプト**」ページに移動して、スクリプトおよびスクリプト・サーバーを構成します。
   - 「**事後スクリプト**」を選択して、アップロード済みのスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択します。スクリプトが実行されるアプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・

ボックスをクリアします。「**システム構成**」 > 「**スクリプト**」ページにナビゲートして、スクリプトおよびスクリプト・サーバーを構成します。

- ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。このオプションが有効になっている場合、事前スクリプトがゼロ以外の戻りコードで完了すると、バックアップまたはリストアのジョブの実行は続行され、事前スクリプト・タスクの状況は「完了」として返されます。事後スクリプトがゼロ以外の戻りコードで完了すると、事後スクリプト・タスクの状況は「完了」として返されます。このオプションが選択されない場合は、バックアップまたはリストアのジョブは実行されず、事前スクリプトまたは事後スクリプトのタスクの状況は「失敗」状況として返されます。

10. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
    - オンデマンド・ジョブを実行するには、「**次へ**」をクリックします。
    - 反復ジョブをセットアップするには、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
11. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。

    オンデマンド・ジョブは即時に開始されます。繰り返しジョブは、設定された開始時刻に開始されます。

次のタスク

ジョブが完了したら、「**リストア**」ペインの「**ジョブ・セッション**」セクションまたは「**アクティブ・クローン**」セクションの「**アクション**」メニューから、以下のいずれかのオプションを選択します。

クリーンアップ
仮想マシンを破棄して、関連付けられているすべてのリソースをクリーンアップします。これはテスト用に使用される一時仮想マシンであるため、仮想マシンが破棄されるとすべてのデータが失われます。

クローン (マイグレーション)
テスト・ネットワークとして定義されているデータ・ストアと仮想ネットワークに仮想マシンをマイグレーションします。

関連タスク

123 ページの『Hyper-V データのバックアップ』
スナップショットを使用して Hyper-V データをバックアップするには、バックアップ・ジョブを使用します。

121 ページの『Hyper-V サーバーの追加』
Hyper-V サーバーが IBM Spectrum Protect Plus に追加されると、サーバーのインベントリーがキャプチャーされるため、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

ファイルのリストア

IBM Spectrum Protect Plus バックアップ・ジョブによって作成されたスナップショットからファイルをリカバリーします。ファイルは、その元の場所または別の場所にリストアすることができます。

始める前に

ファイルをリストアする前に、以下の手順と考慮事項に注意してください。

- 23 ページの『ファイル索引付けおよびリストア要件』に記載されているファイルの索引付けおよびリストアの要件を確認します。
- カタログ・ファイル・メタデータが使用可能な状態でバックアップ・ジョブを実行します。次のガイドラインに従ってください。
  - バックアップ・ジョブ定義内の「ゲスト OS ユーザー名/パスワード」オプションを使用して、関連付けられている仮想マシンのほか、代替仮想マシン宛先について資格情報が設定されていることを確認してください。

– 仮想マシンには、DNS またはホスト名を使用して IBM Spectrum Protect Plus アプライアンスからアクセスできます。Windows 環境では、デフォルトのセキュリティー・ポリシーは Windows NTLM プロトコルを使用するため、Hyper-V 仮想マシンがドメインに接続される場合、ユーザー ID はデフォルトの *domain¥name* のフォーマットに従います。ユーザーがローカル管理者の場合、フォーマット *local_administrator* が使用されます。
– ファイル・リストアが正常に完了するために、ターゲット・マシン上のユーザー ID が、リストア対象のファイルに対して必要な所有権許可を持っていることを確認します。ファイルが、Windows セキュリティー資格情報に基づいてそのファイルをリストアしているユーザー ID とは異なるユーザーによって作成されたものである場合、そのファイル・リストアは失敗します。

このタスクについて

制約事項 :

- 暗号化された Windows ファイル・システムは、ファイルのカタログ作成やファイル・リストアについてはサポートされていません。
- ファイルの索引付けおよびファイル・リストアは、クラウド・リソースまたはリポジトリー・サーバーにオフロードされたリストア・ポイントからはサポートされません。
- Resilient File System (ReFS) 環境でリストアする場合、バージョンが新しい方の Windows Server からのリストアはサポートされていません。例えば、Windows Server 2016 から Windows Server 2012 へのファイルのリストアです。
- バックアップ・ジョブを定義する際に非デフォルト・ローカル管理者が**ゲスト OS ユーザー名**として入力された場合、ファイルのカタログ作成、バックアップ、ポイント・イン・タイム・リストア、および Windows エージェントを呼び出すその他の操作は失敗します。非デフォルト・ローカル管理者とは、ゲスト OS で作成され、管理者役割を付与されている任意のユーザーです。

  これは、[HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System]内のレジストリー・キー LocalAccountTokenFilterPolicy が 0 に設定されているか、または未設定の場合に発生します。パラメーターが 0 に設定されているか、または未設定の場合、ローカル非デフォルト管理者は WinRM と対話できません。WinRM は、IBM Spectrum Protect Plus がファイルのカタログ作成のために Windows エージェントをインストールしたり、このエージェントにコマンドを送信したり、その結果を取得したりするのに使用するプロトコルです。

  「カタログ・ファイル・メタデータ」が有効な状態でバックアップされている Windows ゲスト上で LocalAccountTokenFilterPolicy レジストリー・キーを 1 に設定してください。このキーが存在しない場合は、[HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion ¥Policies¥System]にナビゲートし、値 1 をもつ LocalAccountTokenFilterPolicy という DWord レジストリー・キーを追加してください。

タイム・ゾーンの違いから生じる問題を回避するために、NTP サーバーを使用して、リソース全体でタイム・ゾーンを同期してください。例えば、ご使用の環境内にあるストレージ・アレイ、ハイパーバイザー、およびアプリケーション・サーバーについてタイム・ゾーンを同期することができます。

タイム・ゾーンが同期していない場合、アプリケーションの登録、メタデータのカタログ作成、インベントリー、バックアップ、リストア、ファイル・リストアといったジョブ中にエラーが発生する可能性があります。タイマー・ドリフトの識別および解決について詳しくは、Time in virtual machine drifts due to hardware timer drift を参照してください。

Hyper-V の考慮事項

ファイルのカタログ作成およびファイル・リストアに適格であるのは、SCSI ディスク上のボリュームのみです。

Linux の考慮事項

データが LVM ボリューム上にある場合、*lvm2-lvmetad* サービスが使用不可になっている必要があります。このサービスは、ボリューム・グループ・スナップショットまたはクローンのマウントおよび放棄を行う IBM Spectrum Protect Plus の機能を妨害する可能性があるためです。このサービスを使用不可にするには、以下のステップを実行します。

1. 次のコマンドを実行します。

```
systemctl stop lvm2-lvmetad
```

```
systemctl disable lvm2-lvmetad
```

2. /etc/lvm/lvm.conf を編集して、以下の設定を指定します。

```
use_lvmetad = 0
```

データが XFS ファイル・システム上にあり、xfsprogs パッケージのバージョンが 3.2.0 からバージョン 4.1.9 までのものである場合、ファイル・リストアは、xfsprogs での既知の問題により失敗する可能性があります。この問題は、UUID が変更された場合にクローンまたはスナップショットのファイル・システムが破損する原因です。この問題を解決するには、xfsprogs をバージョン 4.2.0 以上に更新してください。詳しくは、Debian Bug report logs を参照してください。

手順

ファイルをリストアするには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ファイル・リストア**」をクリックします。
2. ファイルを名前で検索するために検索ストリングを入力してから、検索アイコン をクリックします。検索機能の使用法について詳しくは、311 ページの『付録 A 検索ガイドライン』を参照してください。
3. オプション: フィルターを使用して、特定の仮想マシン、ファイルが保護されていた日付範囲、および仮想マシンのオペレーティング・システム・タイプ全体で検索を微調整することができます。

   検索は、「**フォルダー・パス**」フィールドから特定のフォルダーに限定することもできます。「**フォルダー・パス**」フィールドでは、ワイルドカードがサポートされています。ワイルドカードを、ストリングの先頭、中間、または終わりに配置します。例えば、*Downloads と入力すると、先行するパスを入力せずに Downloads フォルダー内を検索できます。
4. デフォルトのオプションを使用してファイルをリストアするには、「**リストア**」をクリックします。ファイルはその元の場所にリストアされます。
5. ファイルをリストアする前にオプションを編集するには、「**オプション**」をクリックします。ファイル・リストアのオプションを設定します。

   既存のファイル/フォルダーを上書きする

   既存のファイルまたはフォルダーを、リストアされたファイルまたはフォルダーで置き換えます。

   宛先

   既存のファイルまたはフォルダーを、リストアされたファイルまたはフォルダーで置き換えることを選択します。

   ファイルを元の場所にリストアするには、「**元の場所にファイルをリストアする**」を選択します。

   ファイルを元の場所とは異なるローカル宛先にリストアするには、「**代替の場所にファイルをリストアする**」を選択します。次に、ナビゲーション・メニューまたは検索機能を使用して、使用可の名リソースから代替の場所を選択します。

   制約事項 : ファイルを代替の場所にリストアできるのは、バックアップ・ジョブ定義の「**ゲスト OS ユーザー名/パスワード**」オプションで代替仮想マシンに対して資格情報が設定されている場合のみです。

   「**宛先フォルダー**」フィールドに、代替宛先での仮想マシンのフォルダー・パスを入力してください。ディレクトリーが存在しない場合は、ディレクトリーが作成されます。

   「**保存**」をクリックしてオプションを保存します。
6. 定義済みのオプションを使用してファイルをリストアするには、「**リストア**」をクリックします。

関連タスク

103 ページの『VMware データのバックアップ』

スナップショットを使用して仮想マシン、データ・ストア、フォルダー、vApp、データ・センターなどの VMware リソースをバックアップするには、バックアップ・ジョブを使用します。

111 ページの『VMware データのリストア』
VMware リストア・ジョブは、インスタント VM リストアおよびインスタント・ディスク・リストアのシナリオをサポートします。これらのシナリオは、選択済みのソースに基づいて自動的に作成されます。

第 8 章 アプリケーションの保護

IBM Spectrum Protect Plus で保護するデータベース・アプリケーションを登録してから、アプリケーションに関連したデータベースとリソースのバックアップとリストアを 行うジョブを作成する必要があります。

注 : IBM Spectrum Protect Plus は、アプリケーションを SPP に登録する際に、アプリケーション・サーバー上にフォルダーを作成できます。 IBM Spectrum Protect Plus によって作成されたフォルダーは、製品が適切に機能するために保持される必要があり、削除してはなりません。 SPP が作成したフォルダーを削除する必要がある場合は、アプリケーションを SPP から登録抹消してください。 SPP は、登録に関連付けられたフォルダーのクリーンアップを 実行します。

Db2

IBM Db2 インスタンスを IBM Spectrum Protect Plus に正常に追加した後、Db2 データの保護を開始できます。Db2 データをバックアップして保守するための SLA ポリシーを作成します。

ご使用の Db2 環境がシステム要件を満たしていることを確認します。詳しくは、30 ページの『Db2 の要件』を参照してください。

ヒント : Db2 データが複数のホストがある複数区画環境に保管されている場合、各ホスト全体で Db2 データを保護できます。保護のためにすべてのインスタンスとデータベースが検出されるように、複数区画環境内の各ホストが IBM Spectrum Protect Plus に追加されなければなりません。詳しくは、140 ページの『Db2 アプリケーション・サーバーの追加』を参照してください。

Db2 の前提条件

IBM Spectrum Protect Plus を使用して Db2 リソースの保護を開始する前に、IBM Spectrum Protect Plus Db2 アプリケーション・サーバー の前提条件がすべて満たされていなければなりません。

IBM Spectrum Protect Plus Db2 アプリケーション・サーバー の要件は、Db2 要件にあります。

スペースの前提条件

バックアップ操作用のボリューム・グループで、Db2 データベース管理システム上に十分なスペースがあり、リストア操作中にファイルをコピーするための 十分なスペースがターゲット・ボリューム上にあることを確認します。スペース所要量について詳しくは、Db2 保護のためのスペース所要量を参照してください。別の位置にデータをリストアしようとする場合は、コピー処理とリストア処理用に追加の専用ボリュームを割り振ります。ターゲット・ホスト上の表スペースとログ用のデータ・パスは、元のホスト上のパスと同じです。 マウントされた vSnap からターゲット・ホストにデータをコピーできるようにするために、このセットアップが必要です。ボリュームのセットアップ内のデータベースごとに、専用のローカル・データベース・ディレクトリーが使用できることを確認してください。

複数区画 Db2 環境

Db2 複数区画データベースを保護するためには、ACS バックアップ・モードが並列モードに設定されている必要があります。ご使用の Db2 環境で区画の並列バックアップ処理を実行するためには、以下の前提条件のいずれかが満たされていることを確認してください。

- Db2 レジストリー変数 **DB2_PARALLEL_ACS** が YES に設定されている (例えば、**db2set DB2_PARALLEL_ACS=**YES)。
- Db2 レジストリー変数 **DB2_WORKLOAD** が SAP に設定されている。

© Copyright IBM Corp. 2017, 2019

制約事項 : DB2_PARALLEL_ACS レジストリー変数は、Db2 の特定のフィックスパック・レベルでのみ使用できます。ご使用のバージョンで **DB2_PARALLEL_ACS** が使用できない場合は、**DB2_WORKLOAD** を SAP に変更する選択が可能です。

その他の構成要件

Db2 環境が以下の基準を満たすように構成されていることを確認してください。

- Db2 アーカイブ・ロギングがアクティブになり、Db2 がリカバリー可能モードです。
- IBM Spectrum Protect Plus エージェント・ユーザーおよび Db2 インスタンス・ユーザーの有効ファイル・サイズ **ulimit** -f が、unlimited に設定されていることを確認します。または、この値を、バックアップ・ジョブやリストア・ジョブ内で最大のデータベース・ファイルのコピーを可能にする十分大きい値に設定します。**ulimit** 設定を変更する場合は、Db2 インスタンスを再始動して、構成を完了します。
- AIX 環境または Linux 環境で IBM Spectrum Protect Plus を実行している場合、インストールされている sudo バージョンが推奨レベルであることを確認します。詳しくは、技術情報 2013790 を参照してください。次に、140 ページの『Db2 の sudo 特権の設定』で説明されているとおりに sudo 特権を設定します。
- Linux 環境で、Linux ユーティリティー・パッケージ `util-linux-ng` または `util-linux` が最新であることを確認します。
- ファイル・パス名内の Unicode 文字を IBM Spectrum Protect Plus は処理できません。すべての名前は ASCII でなければなりません。
- データベース表スペース、オンライン・ログ、およびローカル・データベース・ディレクトリーは、LVM2 または JFS2 のどちらかによって管理される 1 つまたは別々の専用論理ボリューム上に存在できます。2 つのレイアウト例については、以下の図を参照してください。最初の図では、2 つのタイプのボリューム・グループが表示されています。2 番目の図では、データとログ用のすべてのボリュームが 1 つのボリューム・グループ上にあります。

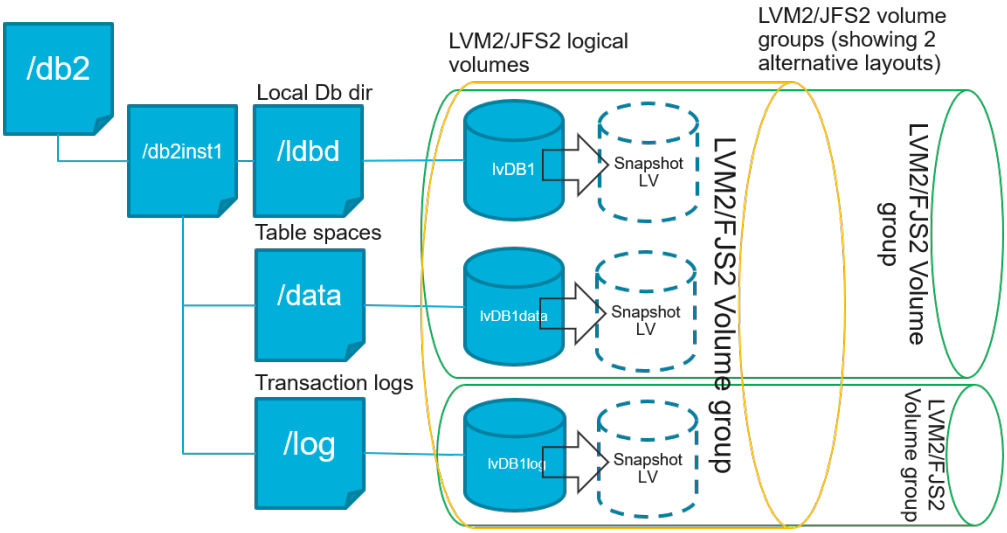


図 *13.* 論理ボリュームのレイアウト例

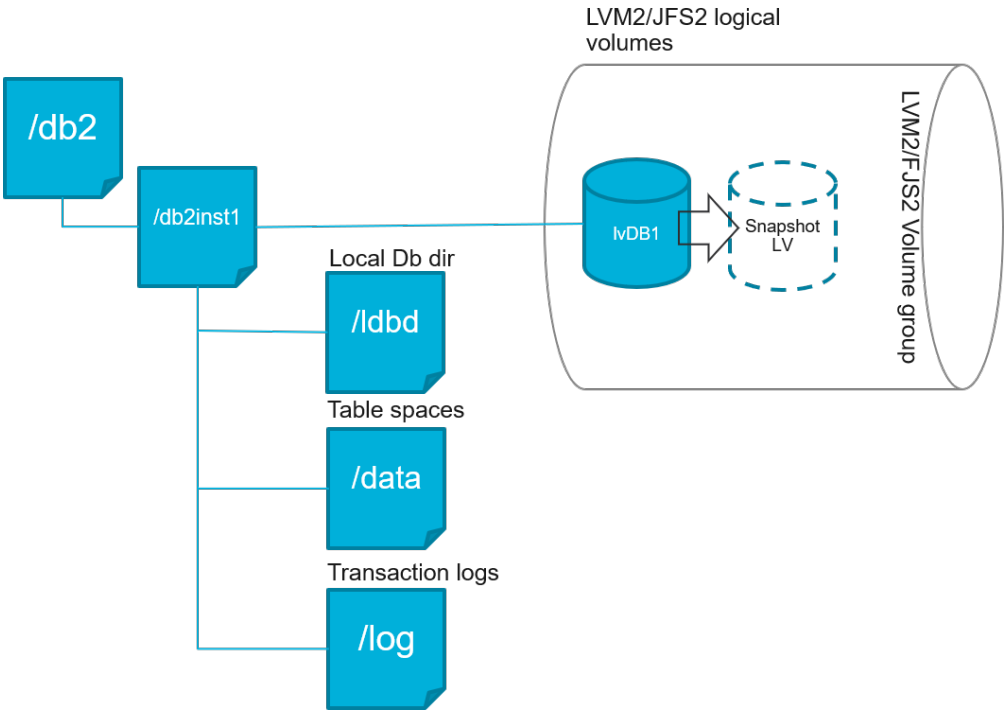


図 *14.* 単一論理ボリュームのレイアウト例

- Db2 論理ボリュームのセットアップに、ネストされたマウント・ポイントが含まれていないことを確認します。

Db2 保護のためのスペース所要量

Db2 データベースのバックアップを開始する前に、ターゲット・ホストとソース・ホスト上、および vSnap リポジトリーに十分な空きディスク・スペースがあることを確認してください。Db2 データベースとログ・ファイルが保管される論理ボリュームの一時論理ボリューム・マネージャー (LVM) スナップショットを作成するためにソース・ホスト上のボリューム・グループに追加の空きディスク・スペースが必要です。保護された Db2 データベースの LVM スナップショットを作成するには、Db2 データがあるボリューム・グループに十分なフリー・スペースがあることを確認してください。

LVM スナップショット

LVM スナップショットは、LVM 論理ボリュームの特定時点コピーです。ソース論理ボリュームから変更されたデータが更新された、省スペース・スナップショットです。LVM スナップショットは、ソース論理ボリュームと同じ ボリューム・グループ内に作成されます。IBM Spectrum Protect Plus Db2 エージェントは、LVM スナップショットを使用して、Db2 データベースの一時的な整合特定時点コピーを作成します。

IBM Spectrum Protect Plus Db2 エージェントが LVM スナップショットを作成し、そのスナップショットがマウントされ、vSnap リポジトリーにコピーされます。ファイル・コピー操作の所要時間は、Db2 データベースのサイズによって異なります。 ファイルのコピー中、Db2 アプリケーションは完全にオンラインのままです。ファイル・コピー操作が終了したら、LVM スナップショットは、クリーンアップ操作で IBM Spectrum Protect Plus Db2 エージェントによって削除されます。

AIX の場合、JFS2 ファイル・システムごとに 15 個以下のスナップショットが存在できます。同じファイル・システムに対して内部と外部の JFS2 スナップショットが同時に存在することはできません。内部スナップショットが JFS2 ボリュームに存在していないことを確認してください。これらのスナップショットは、IBM Spectrum Protect Plus Db2 エージェントが外部スナップショットを作成するときに問題を起こす可能性があります。

データが入っているすべての LVM または JFS2 スナップショット論理ボリュームで、そのサイズの 10% 以上を、ボリューム・グループ内の空きディスク・スペースとして確保してください。ボリューム・グループに十分な空きディスク・スペースがある場合、IBM Spectrum Protect Plus Db2 エージェントは、スナップショット論理ボリューム用にソース論理ボリューム・サイズの最大 25% を予約します。

LVM2 および JFS2
Db2 バックアップ操作を実行すると、Db2 がスナップショットを要求します。このスナップショットは、選択されたデータベースのデータまたはログがある論理ボリュームごとに、論理ボリューム管理 (LVM) システムまたはジャーナル・ファイル・システム (JFS) で作成されます。Linux システムでは、論理ボリュームは、lvm2 コマンドを使用して LVM2 によって管理されます。AIX では、論理ボリュームは、JFS2 によって管理され、JFS2 スナップショット・コマンドを使用して外部スナップショットとして作成されます。

ソフトウェア・ベースの LVM2 または JFS2 スナップショットは、同じボリューム・グループの新規論理ボリュームとして取られます。 これらのスナップショット・ボリュームは、Db2 インスタンスを実行するのと同じマシンに一時的にマウントされるので、vSnap リポジトリーに転送できます。

Linux オペレーティング・システムでは、LVM2 ボリューム・マネージャーが、論理ボリュームのスナップショットを同じボリューム・グループに保管します。AIX オペレーティング・システムでは、JFS2 ボリューム・マネージャーが、論理ボリュームのスナップショットを同じボリューム・グループに保管します。どちらの場合も、論理ボリュームを保管できる十分なスペースがマシン上に必要です。スナップショットが存在する間、データがソース・ボリューム上で変更されるにつれて、論理ボリュームのサイズが大きくなります。複数区画環境において、複数の区画が同じボリュームを共有している場合、各区画についてそのボリュームの追加のスナップショットが作成されます。ボリューム・グループに、必要なスナップショット用に十分なフリー・スペースがあることを確認してください。

Db2 の sudo 特権の設定
IBM Spectrum Protect Plus を使用してデータを保護するには、必要なバージョンの sudo プログラムをインストールする必要があります。Db2 アプリケーション・サーバーの場合、他のアプリケーション・サーバーとは異なる固有の方法で sudo をセットアップする必要があります。

始める前に

インストールする sudo の正確なバージョンを判別するには、技術情報 2013790 を参照してください。

このタスクについて

sudo に必要なスーパーユーザー特権を持つ専用の IBM Spectrum Protect Plus エージェント・ユーザーをセットアップします。この構成により、エージェント・ユーザーはパスワードを使用せずにコマンドを実行できるようになります。

手順

1. 次のコマンドを実行して、アプリケーション・サーバー・ユーザーを作成します。

   ```
   useradd -m <agent>
   ```

   ここで、agent には、IBM Spectrum Protect Plus エージェント・ユーザーの名前を指定します。
2. 次のコマンドを実行して、新規ユーザーのパスワードを設定します。

   ```
   passwd <agent>
   ```
3. エージェント・ユーザーに対してスーパーユーザー特権を有効にするには、!requiretty を設定します。sudo 構成ファイルの末尾に以下の行を追加します。

   ```
   Defaults:<agent> !requiretty
   <agent> ALL=(ALL) NOPASSWD:ALL
   ```

   sudoers ファイルが別のディレクトリー (例えば、/etc/sudoers.d) から構成をインポートするように構成されている場合は、そのディレクトリー内の適切なファイルにこの行を追加できます。

Db2 アプリケーション・サーバーの追加

Db2 データの保護を開始するには、Db2 インスタンスが置かれているホストのアドレスを追加する必要があります。IBM Spectrum Protect Plus で保護するすべてのホストを追加するためにこの手順を繰り返すことができます。Db2 環境が複数のホストがある複数区画環境である場合、各ホストを IBM Spectrum Protect Plus に追加する必要があります。

このタスクについて

Db2 アプリケーション・サーバーを IBM Spectrum Protect Plus に追加するにはマシンのホスト・アドレスが必要です。

手順

1. ナビゲーションで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」を展開します。
2. 「**Db2**」ウィンドウで、「**アプリケーション・サーバーの管理**」をクリックして、「**アプリケーション・サーバーの追加**」をクリックし、ホスト・マシンを追加します。

図 *15. Db2* エージェントの追加

3. 「**アプリケーション・プロパティー**」セクションにホスト・アドレスを入力します。
4. ユーザーを指定するか、SSH 鍵を使用するかを選択します。
   - ユーザーを指定することを選択する場合は、既存のユーザーを選択するか、ユーザー ID とパスワードを入力します。
   - SSH 鍵を使用する場合は、メニューから鍵を選択します。

   注 : ユーザーには、sudo 特権がセットアップされている必要があります。

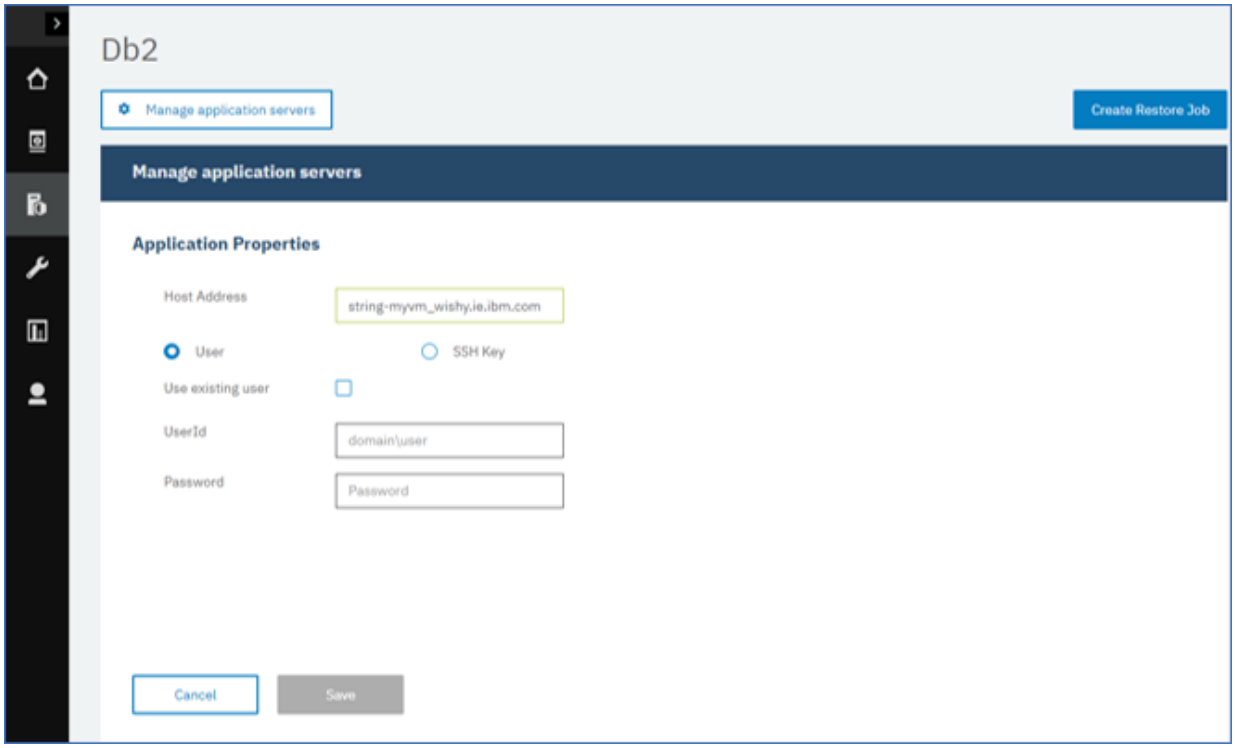


図 *16.* エージェント・ユーザーの管理

ヒント :

検出された Db2 インスタンスはホストごとにリストされます。Db2 インスタンスが区画に分割されている場合、この情報は、ホスト・マシンと区画の数と共にリストされます。 マルチホスト Database Partitioning Feature (DPF) の場合、Db2 インスタンスは単一の装置として表示されます。

5. フォームを保存して、上記のステップを繰り返し、他の Db2 アプリケーション・サーバーを IBM Spectrum Protect Plus に追加します。

Db2 データが複数のホストがある複数区画環境内にある場合、各ホストを追加する必要があります。Db2 ホストごとにこの手順を繰り返します。

次のタスク

Db2 アプリケーション・サーバーを IBM Spectrum Protect Plus に追加した後、インベントリーは各アプリケーション・サーバーで自動的に実行され、それらのインスタンス内の関連データベースを検出します。

データベースが追加されたことを確認するには、ジョブ・ログを調べてください。「**ジョブと操作**」に進みます。「**実行中のジョブ**」タブをクリックして、最新のアプリケーション・サーバー・インベントリー・ログ項目を見つけます。

完了したジョブは「**ジョブ・ヒストリー**」タブに表示されます。「**ソート順**」リストを使用して、開始時刻、タイプ、状況、ジョブ名、または所要時間に基づいてジョブをソートすることができます。ジョブを名前で検索するには、「**名前での検索**」フィールドを使用します。名前ではワイルドカード文字としてアスタリスクを使用できます。

データベースを確実に保護できるようにするには、データベースが検出されている必要があります。インベントリーの実行手順については、Db2 リソースの検出を参照してください。

Db2 リソースの検出

IBM Db2 アプリケーション・サーバーを IBM Spectrum Protect Plus に追加すると、すべての Db2 インスタンスおよびデータベースを削除するインベントリーが自動的に実行されます。インベントリーにより、選択されたホストのすべての Db2 データベースの検出、リスト、保管が行われ、データベースを IBM Spectrum Protect Plus で保護できるようになります。

始める前に

Db2 アプリケーション・サーバーを IBM Spectrum Protect Plus に追加したことを確認してください。手順については、Db2 アプリケーション・サーバーの追加を参照してください。

このタスクについて

Db2 インスタンスについてインベントリーで検出されたすべての Db2 区画がリストされます。 区画は、「**インスタンス**」テーブルに、ホスト名に付加された各ホストの区画番号ごとにリストされます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」を展開します。

   ヒント : さらに多くの Db2 インスタンスを「**インスタンス**」ペインに追加するには、Db2 アプリケーション・サーバーの追加の手順に従ってください。
2. 「**インベントリーの実行**」をクリックします。

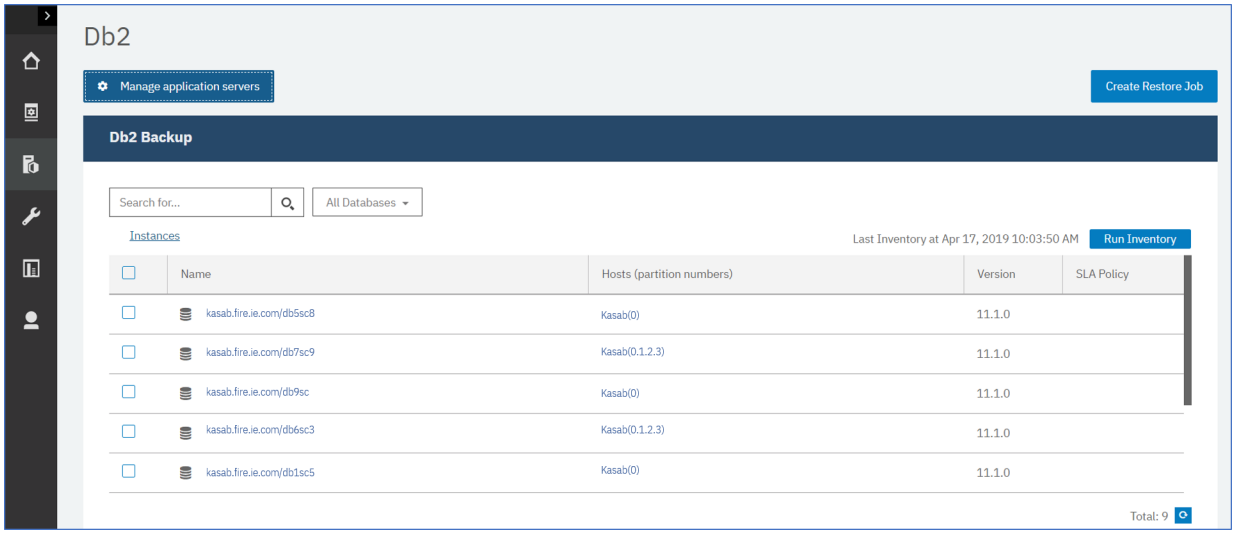


図 *17. Db2* リソースの検出

インベントリーの実行中、ボタンが「**インベントリーが進行中**」に変わります。任意の使用可能なアプリケーション・サーバーでインベントリーを実行できますが、インベントリー・プロセスは一度に 1 つしか実行できません。

ジョブ・ログを表示するには、「**ジョブと操作**」に進みます。「**実行中のジョブ**」タブをクリックして、最新のアプリケーション・サーバー・インベントリー・ログ項目を見つけます。

完了したジョブは「**ジョブ・ヒストリー**」タブに表示されます。「**ソート順**」リストを使用して、開始時刻、タイプ、状況、ジョブ名、または所要時間に基づいてジョブをソートすることができます。ジョブを名前で検索するには、「**名前での検索**」フィールドを使用します。名前ではワイルドカード文字としてアスタリスクを使用できます。

3. インスタンスをクリックして、そのインスタンスで検出されたデータベースを示すビューを開きます。「**インスタンス**」リストでデータベースが欠落している場合は、Db2 アプリケーション・サーバーを確認して、インベントリーを再実行します。場合によっては、特定のデータベースにバックアップに適格ではないというマークが付けられていることがあります。そのデータベースの上にカーソルを移動して理由を調べてください。

   ヒント: インスタンスのリストに戻るには、「**Db2 のバックアップ**」ペインの「**インスタンス**」ハイパーテキストをクリックします。

次のタスク

選択したインスタンスでカタログされている Db2 データベースの保護を開始するには、SLA ポリシーをインスタンスに適用します。 SLA ポリシーの設定手順については、SLA ポリシーの定義を参照してください。

Db2 接続のテスト

Db2 アプリケーション・サーバーを追加した後、接続をテストできます。テストでは、サーバーとの通信と、IBM Spectrum Protect Plus と Db2 サーバーの間の DNS 設定が検証されます。ユーザーの正しい sudo 権限も検査されます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」をクリックします。
2. 「**Db2**」ウィンドウで、「**アプリケーション・サーバーの管理**」をクリックして、テストする「**ホスト・アドレス**」を選択します。

   使用可能な Db2 アプリケーション・サーバーのリストが表示されます。
3. 「**アクション**」をクリックして、「**テスト**」を選択し、物理システム、リモート・システム、およびオペレーティング・システムの接続と設定の検証テストを開始します。

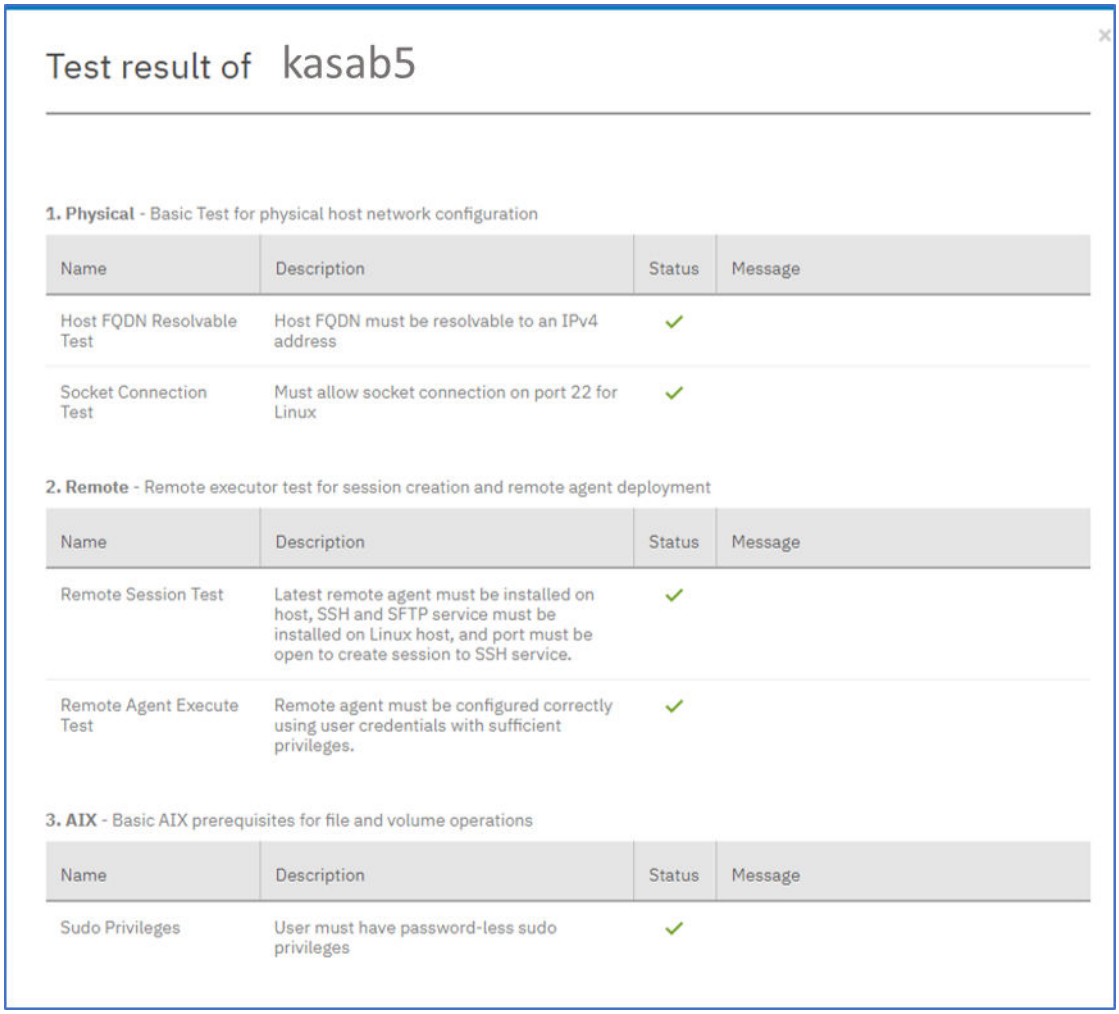


図 *18.* 接続のテスト

テスト・レポートにテストのリストが表示されます。レポートは、物理ホスト・ネットワーク構成のテストと、ホストの SSH と SFTP を検査するホスト上のリモート・サーバー・インストールのテストで構成されています。3 番目のテストでは、オペレーティング・システムの前提条件と正しい sudo 特権が検査されます。

4. 「**OK**」をクリックしてテストを閉じ、テストの失敗を修正した後でテストの再実行を選択します。

Db2 データのバックアップ

データを保護するためにバックアップ・コピーを実行して作成するオプションを指定して、定期的な Db2 バックアップ・ジョブを定義します。アーカイブ・ログの継続的なバックアップを有効にし、必要に応じてロールフォワード・オプションで特定時点コピーをリストアできるようにすることができます。

始める前に

初期バックアップ時に、IBM Spectrum Protect Plus は、新規の vSnap ボリュームおよび NFS 共有を作成します。増分バックアップ時には、以前に作成されたボリュームが再使用されます。IBM Spectrum Protect Plus Db2 エージェントは、バックアップが実行される Db2 サーバーに共有をマウントします。

バックアップ・ジョブ定義を作成する前に、以下の手順と考慮事項を確認してください。

- バックアップするアプリケーション・サーバーを追加します。手順については、Db2 アプリケーション・サーバーの追加を参照してください。
- SLA ポリシーを構成します。手順については、SLA バックアップ・ジョブの定義を参照してください。
- IBM Spectrum Protect Plus ユーザーがバックアップとリストアの操作を実装するには、その前に、そのユーザーに役割とリソース・グループを割り当てる必要があります。「**アカウント**」ペインで、リソース

およびバックアップとリストアの操作に対するアクセス権限をユーザーに付与します。詳しくは、Managing user access を参照してください。

- インベントリー・ジョブをバックアップ・ジョブと同時に実行するようにスケジュールしないでください。
- 多数のバックアップ・ジョブで単一の Db2 データベースのログ・バックアップを構成しないでください。ログ・バックアップが有効になっている状態で単一の Db2 データベースが複数のジョブ定義に追加されると、あるジョブからのログ・バックアップにより、次のジョブでバックアップされる前にログが切り捨てられる可能性があります。このため、特定時点リストア・ジョブが失敗する可能性があります。

手順

1. ナビゲーション・メニューで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」を展開します。
2. 以下のいずれかのアクションを選択して、バックアップするインスタンスまたはデータベースを 選択します。
   - 「**インスタンス**」ペインで、インスタンス名の横にあるチェック・ボックスをクリックしてインスタンス全体を選択します。このインスタンスに追加されるデータベースはすべて、選択する SLA ポリシーに割り当てられます。
   - インスタンス名をクリックして、そのインスタンス内のデータベースのリストからデータベースを選択し、インスタンス内の特定のデータベースを選択します。

   「**インスタンス**」ペインの各項目は、インスタンス名、データベース名、適用された SLA ポリシー、およびログ・バックアップの適格性ごとにリストされます。
3. 「**オプションの選択**」をクリックして、ログ・バックアップを有効または無効にし、バックアップ操作で大容量データの移動にかかる時間を最短に抑えるために並列ストリームを指定します。「**保存**」をクリックして、オプションをコミットします。

   アーカイブ・ログをバックアップするには「**ログ・バックアップを有効にする**」を選択してます。これにより、特定時点リストア・オプションとリカバリー・オプションを使用できるようになります。Db2 のログ・バックアップ設定情報については、ログ・バックアップを参照してください。

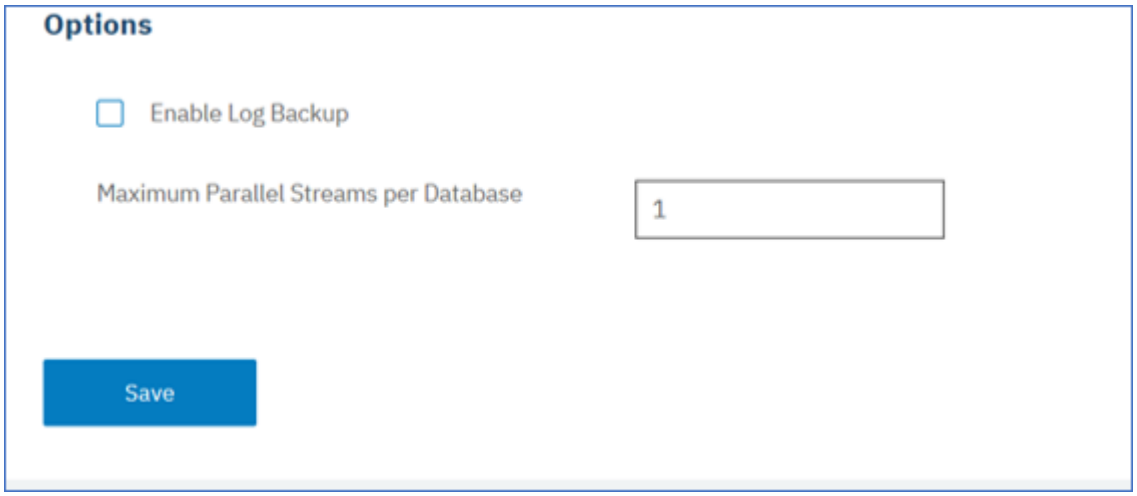


図 19. 「ログ・バックアップを有効にします」オプションが示されている「バックアップ」ペイン

   オプションを保存すると、これらのオプションは、選択されたデータベースまたはインスタンスのすべてのバックアップ・ジョブで使用されます。
4. データベースまたはインスタンスを再び選択して、「**SLA ポリシーの選択**」をクリックし、そのデータベースまたはインスタンスの SLA ポリシーを選択します。
5. SLA オプションを保存します。

   カスタムの保存率と頻度を指定して新規の SLA を定義するか、既存のポリシーを編集するには、「**保護の管理**」 > 「**ポリシーの概要**」を選択します。「**SLA ポリシー**」ペインで、「**SLA ポリシーの追加**」をクリックして、ポリシー設定を定義します。

次のタスク

SLA ポリシーが保存された後、ポリシー名の横にある「**アクション**」をクリックして、「**開始**」を選択することで、いつでも必要に応じてオンデマンド・バックアップを実行できます。ログで、状況が変更され、バックアップが実行中であることが示されます。

SLA バックアップ・ジョブの定義

Db2 インスタンスごとに Db2 データベースがリストされた後、SLA ポリシーを選択して適用し、データの保護を開始します。

手順

1. ナビゲーション・メニューから、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」を展開します。
2. Db2 インスタンスを選択して、そのインスタンスのすべてのデータをバックアップするか、インスタンス名をクリックして、バックアップに使用できるデータベースを表示します。 バックアップする Db2 インスタンス内の個々のデータベースを選択できるようになります。

   すべてのデータが関連付けられているインスタンス全体をバックアップするか、1 つ以上のデータベースをバックアップすることができます。

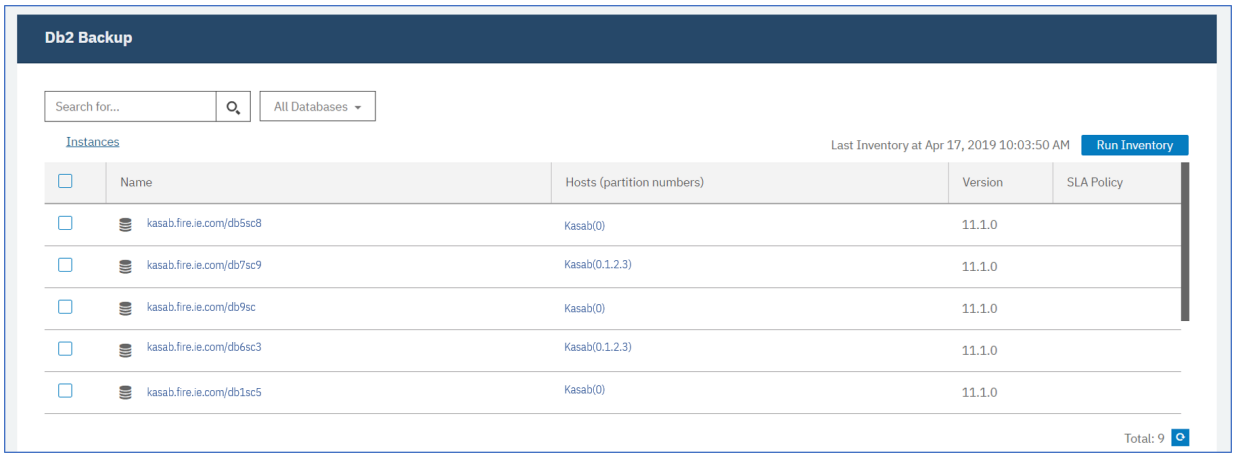


図 *20.* インスタンスを示す「*Db2* バックアップ」ペイン

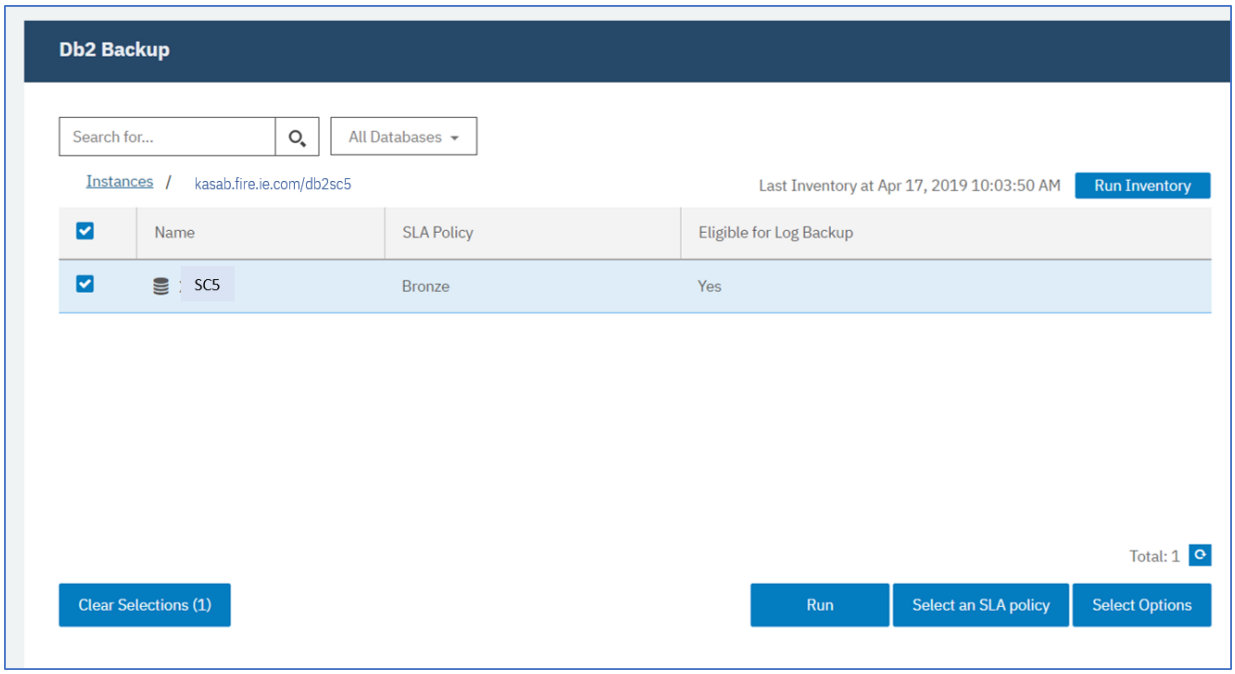


図 *21.* インスタンスのデータベースを示す *Db2* バックアップ・ペイン

3. 「**SLA ポリシーの選択**」をクリックして、SLA ポリシーの「**ゴールド**」、「**シルバー**」、または「**ブロンズ**」を選択します。選択内容を保存します。

   事前定義の選択項目の「ゴールド」、「シルバー」、および「ブロンズ」は、それぞれ頻度と保存率が異なります。「**ポリシーの概要**」 > 「**SLA ポリシー**」にナビゲートして、カスタムの SLA ポリシーを作成したり、既存のポリシーを編集したりすることができます。
4. 「**オプションの選択**」をクリックして、バックアップのオプションを定義します。例えば、以降のリカバリー・オプションのログ・バックアップを有効にしたり、並列ストリームを指定して大容量データベースのバックアップに要する時間を短縮したりすることができます。変更内容を保存します。

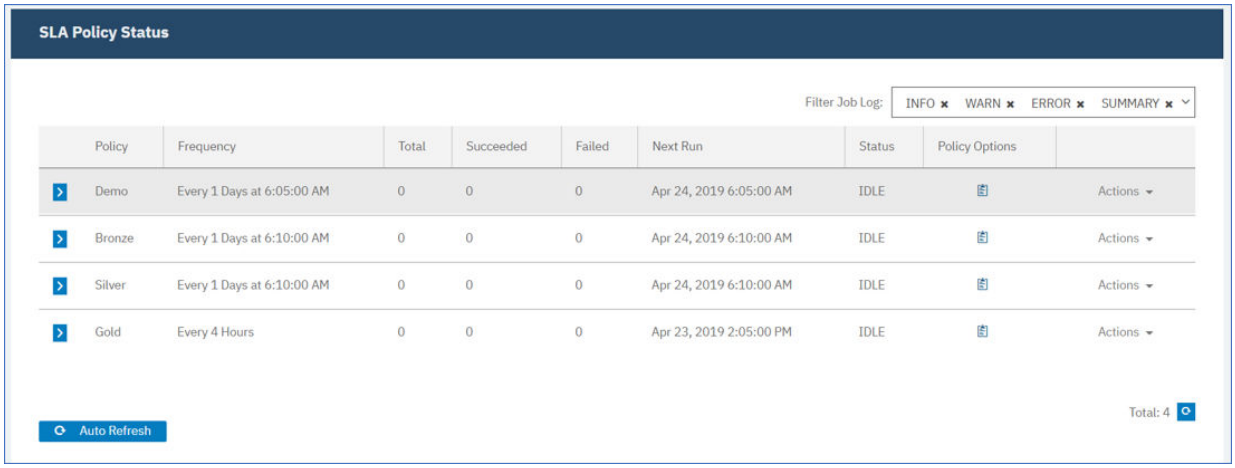


図 *22. バックアップ・オプションおよび SLA ポリシー*

5. 「**SLA ポリシーのステータス**」テーブルの「**ポリシー・オプション**」列のアイコンをクリックして、SLA ポリシーを構成します。

   SLA 構成オプションについて詳しくは、148 ページの『バックアップ・ジョブ用の SLA 構成オプションの設定』を参照してください。
6. スケジュールに入れられたジョブの外部でポリシーを実行する場合は、インスタンスまたはデータベースを選択します。 「**アクション**」をクリックして、「**開始**」を選択します。

   選択した SLA の状況が「**実行**」に変わります。表示されるジョブ・ログでジョブの進行状況を確認できます。

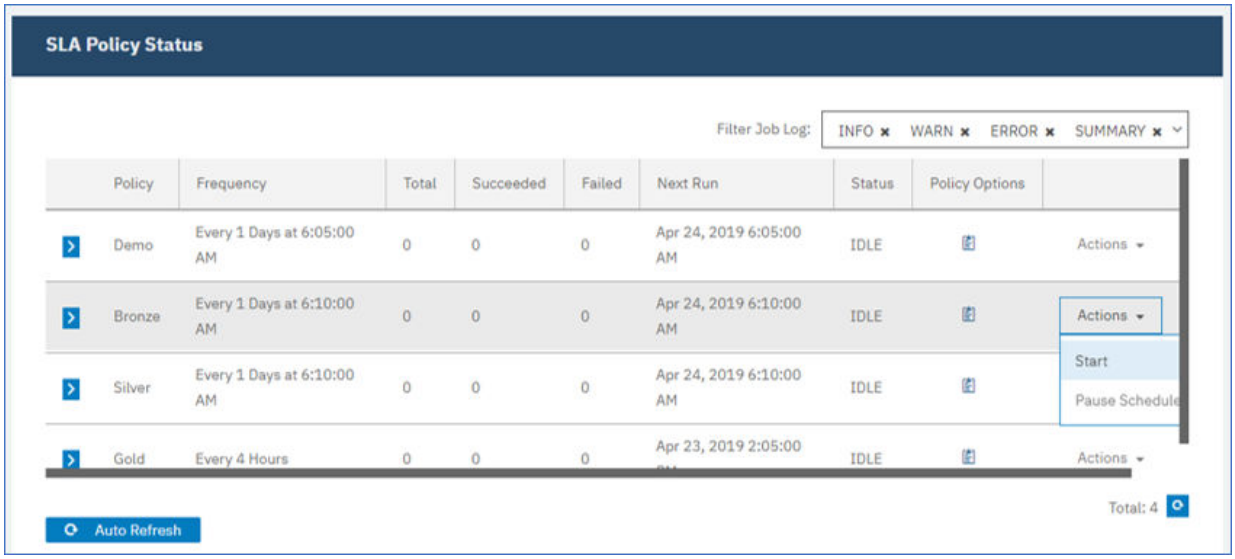


図 *23. SLA ポリシー*

SLA のスケジュールを一時停止するには、「**アクション**」をクリックして、「**スケジュールの一時停止**」を選択します。
ジョブを開始後にキャンセルするには、「**アクション**」 > 「**キャンセル**」をクリックします。

バックアップ・ジョブ用の SLA 構成オプションの設定

バックアップ・ジョブ用の SLA をセットアップした後、そのジョブに対してさらに多くのオプションを構成できます。スクリプトを実行して、バックアップ操作からリソースを除外し、必要に応じてデータベースのフル基本バックアップを強制的に実行することができます。

手順

1. 構成するジョブの「**SLA ポリシーのステータス**」テーブルの「**ポリシー・オプション**」列で、クリップボード・アイコン をクリックして、追加の構成オプションを指定します。
   ジョブが既に構成されている場合は、構成を編集するためのアイコンをクリックします。

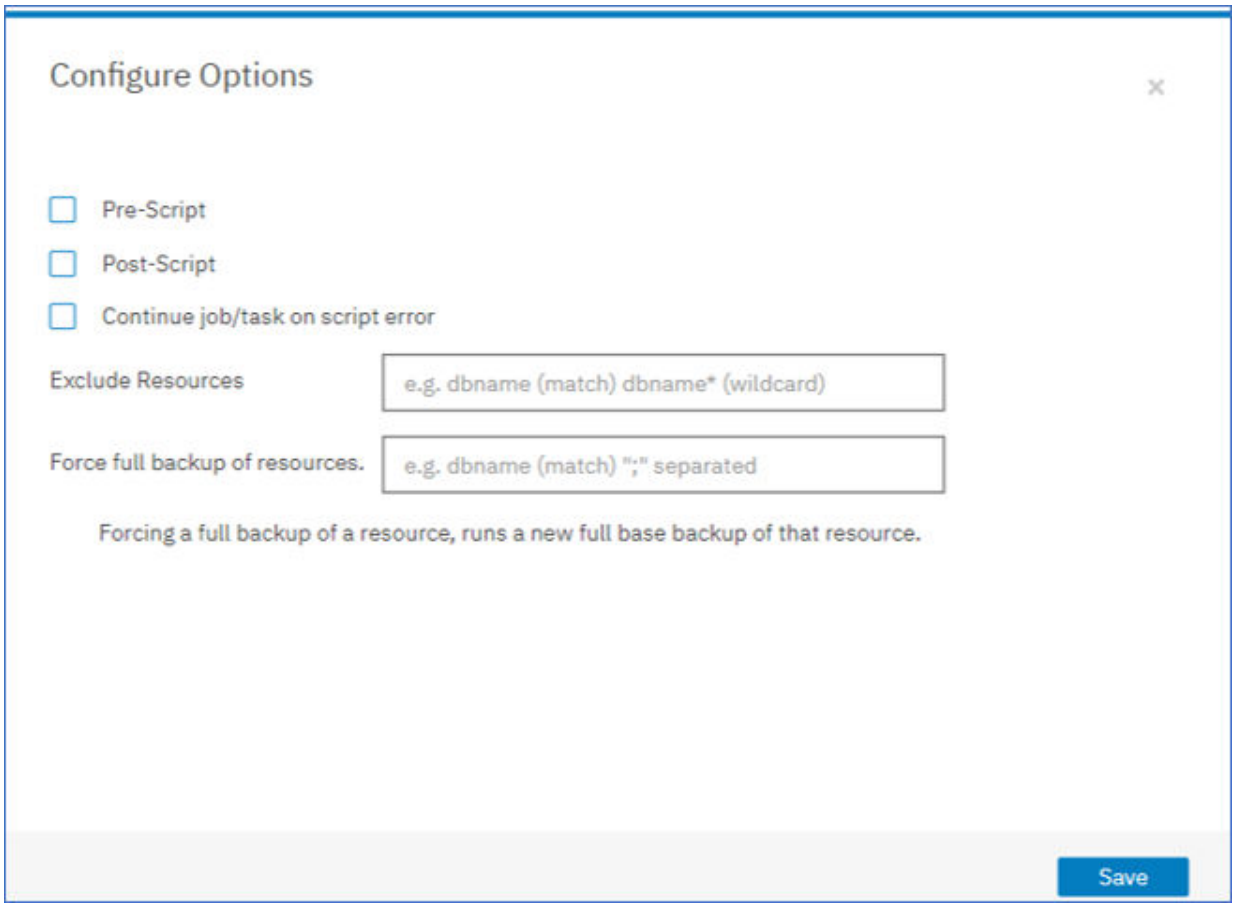


図 *24. SLA* 構成オプションの指定

2. 「**事前スクリプト**」をクリックして、以下のいずれかのオプションを選択し、事前スクリプト構成を定義します。
   - 「**スクリプト・サーバーの使用**」をクリックして、アップロード済みのスクリプトをメニューから選択します。
   - 「**スクリプト・サーバーの使用**」をクリックしないでください。アプリケーション・サーバーをリストから選択して、その場所でスクリプトを実行します。
3. 「**事後スクリプト**」をクリックして、以下のいずれかのオプションを選択し、事後スクリプト構成を定義します。

- 「**スクリプト・サーバーの使用**」をクリックして、アップロード済みのスクリプトをメニューから選択します。
- 「**スクリプト・サーバーの使用**」をクリックしないでください。アプリケーション・サーバーをリストから選択して、その場所でスクリプトを実行します。

スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成されます。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。

4. ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。

   このオプションが選択される場合、スクリプトの処理がゼロ以外の戻りコードで完了すると、バックアップまたはリストアの操作は再試行され、スクリプト・タスクの状況は「完了」として報告されます。このオプションが選択されない場合は、バックアップまたはリストアは再試行されず、スクリプト・タスクの状況は「失敗」として報告されます。
5. バックアップ・ジョブからリソースを除外するには、ジョブから除外するリソースを指定します。「**リソースの除外**」フィールドに正確なリソース名を入力します。名前が不明な場合は、ワイルドカードのアスタリスクをパターンの前 (**text*) またはパターンの後 (*text**) に指定して使用します。標準の英数字と特殊文字 (-、_、*) を使用して複数のワイルドカードを入力できます。 項目はセミコロンで区切ってください。
6. リソースの新規のフルバックアップを 作成するには、そのリソースの名前を「**リソースのフルバックアップを強制します**」フィールドに入力します。複数のリソースはセミコロンで区切ります。

   フルバックアップにより 、そのリソースの新規のフルバックアップが 作成され、1 つのオカレンスでのみ、そのリソースの既存のバックアップが置き換えられます。フルバックアップが 完了すると、そのリソースは以前と同様に増分バックアップされます。

ログ・バックアップ

データベースのアーカイブ・ログには、コミットされたトランザクション・データが入っています。このトランザクション・データを使用すると、リストア操作の実行時にロールフォワード・データ・リカバリーを実行できます。アーカイブ・ログ・バックアップを使用すると、データのリカバリー・ポイント目標が強化されます。

「**ログ・バックアップを有効にします**」オプションを選択して、バックアップ・ジョブまたは SLA ポリシーのセットアップ時にロールフォワード・リカバリーを許可していることを確認します。初回の選択時に、SLA ポリシーのバックアップ・ジョブを実行して、データベース上で IBM Spectrum Protect Plus へのログ・アーカイブをアクティブにする 必要があります。このバックアップにより、vSnap リポジトリーに別個のボリュームが作成されます。このボリュームは、Db2 アプリケーション・サーバーに永続的にマウントされます。バックアップ処理により、ログのアーカイブ目的でそのボリュームを指すように **LOGARCHMETH1** パラメーターまたは **LOGARCHMETH2** パラメーターが更新されます。このボリュームは、「**ログ・バックアップの有効化**」オプションがクリアされ、新しいバックアップ・ジョブが実行されない限り、Db2 アプリケーション・サーバーにマウントされたままになります。

制約事項 : Db2 複数区画環境では、区画全体で **LOGARCHMETH** パラメーターが一致している必要があります。

LOGARCHMETH1 パラメーターまたは **LOGARCHMETH2** パラメーターが、OFF 以外の値を指定して設定される場合、ロールフォワード・リカバリーにアーカイブ・ログを使用できます。「**ログ・バックアップを有効にする**」オプションを選択解除することで、ログ・バックアップ・ジョブをいつでもキャンセルできます。「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」に進み、該当のインスタンスを選択して、「**オプションの選択**」をクリックします。この変更は、次にバックアップ・ジョブが正常に完了した後に有効になり、**LOGARCHMETH** パラメーター値が元の設定に戻されます。

重要 : LOGARCHMETH1 パラメーターが LOGRETAIN に設定されている場合、またはいずれかの **LOGARCHMETH** パラメーターが OFF に設定されている場合に限り、IBM Spectrum Protect Plus はログ・バックアップ・ジョブを有効にすることができます。

LOGARCHMETH1 パラメーターが LOGRETAIN に設定される場合。

IBM Spectrum Protect Plus は、**LOGARCHMETH1** パラメーター値を変更して、ログ・バックアップを有効にします。

LOGARCHMETH1 パラメーターまたは LOGARCHMETH2 パラメーターのどちらかが OFF に設定され、もう一方が DISK、TSM、または VENDOR に設定される場合。

IBM Spectrum Protect Plus は、オフに設定される **LOGARCHMETH** パラメーターを使用してログ・バックアップを有効にします。

両方の LOGARCHMETH パラメーターが DISK、TSM、または VENDOR に設定される場合。

IBM Spectrum Protect Plus がログ・バックアップを有効にしようとする場合、この設定の組み合わせではエラーが生じます。このエラーを解決するには、いずれかのパラメーターを OFF に設定し、「**ログ・バックアップを有効にします**」オプションを選択した状態でバックアップ・ジョブを実行します。

アーカイブ・ログ・バックアップの切り捨て

IBM Spectrum Protect Plus は、データベース・バックアップが正常に行われた後、古いトランザクション・ログを自動的に削除します。このアクションにより、確実に、ログ・アーカイブ・ボリュームの容量は古いログ・ファイルの保存によって損なわれなくなります。切り捨てられたこれらのログ・ファイルは、対応するバックアップの有効期限が切れ、削除されるまで、vSnap リポジトリーに保管されます。データベース・バックアップの保存は、選択した SLA ポリシーで定義されます。SLA ポリシーについて詳しくは、146 ページの『SLA バックアップ・ジョブの定義』を参照してください。

IBM Spectrum Protect Plus は、他のアーカイブ・ログのロケーションの保存を管理しません。

Db2 の設定について詳しくは、IBM Db2 のウェルカム・ページを参照してください。

Db2 データのリストア

Db2 データを vSnap リポジトリーからリストアするには、最新のバックアップまたは以前のバックアップ・コピーのいずれかからデータをリストアするジョブを定義します。データをオリジナル・インスタンスか、別のマシン上の代替インスタンスにリストアしてリカバリー・オプションを指定するよう選択し、ジョブを保存できます。

始める前に

重要 : すべてのリストア操作で、ソース・ホストとターゲット・ホストの DB2 のバージョン・レベルが同じでなければなりません。その要件に加えて、リストア対象のインスタンスと同じ名前のインスタンスがそれぞれのホスト上に存在することを確認する必要があります。この要件は、ターゲット・インスタンスが同じ名前である場合にも、名前が異なる場合にも適用されます。リストア操作が成功するためには、両方のインスタンスが、片方はオリジナルの名前、もう片方は新規名を使用してプロビジョンされる必要があります。

ご使用の Db2 環境に区画化データベースが含まれている場合、すべての区画のデータは、通常のバックアップ・ジョブの実行時にバックアップされます。すべてのインスタンスがバックアップ・ペインにリストされます。複数区画インスタンスは、区画番号とホスト名付きで示されます。

Db2 のリストア・ジョブを作成する前に、以下の要件が満たされていることを確認します。

- 少なくとも 1 つの Db2 バックアップ・ジョブがセットアップされていて正常に実行されている。バックアップ・ジョブのセットアップについての 説明は、144 ページの『Db2 データのバックアップ』を参照してください。
- リストア・ジョブをセットアップしているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当てについて詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

注 : 複数区画データベースを代替ロケーションにリストアする 場合は、ターゲット・インスタンスがオリジナル・インスタンスと同じ区画番号で構成されていることを確認してください。 それらの区画はすべてが単一のホスト上になければなりません。 名前変更された新規インスタンスにデータをリストアする 場合、リストア操作に必要な両方のインスタンスを同数の区画で構成する必要があります。

代替インスタンスへのリストア操作を開始する前に、ソース・マシン上のファイル・システム構造がターゲット・マシンと一致していることを確認してください。このファイル・システム構造には、テーブル・スペース、オンライン・ログ、およびローカル・データベース・ディレクトリーが含まれます。十分なスペースがある専用のボリュームがファイル・システム構造に割り振られていることを確認してください。Db2 は、すべてのリストア操作のソースとターゲットのホストで同じバージョン・レベルでなければならず、同じ名前のインスタンスが各ホスト上になければなりません。 スペース所要量について詳しくは、Db2 保護のためのスペース所要量を参照してください。前提条件およびセットアップについて詳しくは、Db2 の前提条件を参照してください。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」を展開して、「**リストア・ジョブの作成**」をクリックします。
   「スナップショットのリストア」ウィザードがオープンします。
2. オプション: 「**ジョブと操作**」ページから「リストア」ウィザードを起動した場合は、ソース・タイプとして Db2 を選択し、「**次へ**」をクリックします。

   ヒント: 「リストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
3. 「**ソースの選択**」ページで、Db2 インスタンスをクリックして、そのインスタンス内のデータベースを表示します。 データベース名の横にあるプラス・アイコン をクリックして、データベースを選択します。「**次へ**」をクリックして先に進みます。
4. 「**ソースページのスナップショット**」ページで、必要なリストア操作のタイプを選択します。
   - **オンデマンド: スナップショット**: データベース・スナップショットからの 1 回限りのリストア操作を作成します。このジョブは、反復する設定にはできません。
   - **オンデマンド: 特定時点**: データベースの特定時点バックアップからの 1 回限りのリストア操作を作成します。このジョブは、反復する設定にはできません。
   - **反復**: スケジュールで繰り返し実行される反復ジョブを作成します。

   ヒント:

   「**オンデマンド: スナップショット**」の場合、リカバリーしないか、バックアップの最後までリカバリーするかを選択できます。 「**オンデマンド: 特定時点**」リストア・ジョブの場合、使用可能なログの最後までリカバリーするか、特定時点までリカバリーするかを選択できます。
5. 同じページで、次のように「**リストア・ロケーションのタイプ**」を選択します。

位置	説明
サイト	1 次サイトまたは 2 次サイトからデータをリストアするには、このオプションを選択します。サイトは、オンデマンド特定時点リストア・ジョブの唯一の選択項目です。
クラウド・オフロード	クラウド・ストレージからデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。
リポジトリー・オフロード	vSnap リポジトリーからデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。
クラウド・アーカイブ	クラウドでアーカイブされたデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。
リポジトリー・アーカイブ	vSnap リポジトリーでアーカイブされたデータをリストアするには、このオプションを選択します。

位置	説明
	スナップショットに使用するリストア・ポイントを指定します。

オンデマンド・スナップショットの作成時に、探しているスナップショットにタイム・スパンを指定できます。該当する場合、別の vSnap サーバーを操作に使用することができます。

6. リストア操作のロケーションを選択します。以下のいずれかのオプションを選択して、「**次へ**」をクリックします。

オプション	説明
デモ	デモンストレーション vSnap サーバーからデータをリストアする場合、このオプションを選択します。このオプションは、特定のセットアップでのみ選択できます。
1 次	1 次 vSnap サーバーからターゲット宛先にデータをリストアする場合、このオプションを選択します。このロケーションは、リストア・ロケーション・タイプ「サイト」で使用可能です。
2 次	2 次 vSnap サーバーからターゲット宛先にデータをリストアする場合、このオプションを選択します。このロケーションは、リストア・ロケーション・タイプ「サイト」で使用可能です。

リストア・ポイントは、「**リストア・ポイント**」メニューから使用できます。

7. リストア操作に選択した宛先に適切な「**リストア方式**」を選択します。「**次へ**」をクリックして先に進みます。
   - **インスタント・アクセス**: このモードでは、IBM Spectrum Protect Plus が vSnap リポジトリーからボリュームをマウントした後、それ以上のアクションは実行されません。マウントされたボリューム内のファイルからのカスタム・リカバリーにデータを使用します。
   - **実動**: このモードでは、Db2 アプリケーション・サーバーは、最初に vSnap リポジトリー・ボリュームからターゲット・ホスト (代替ロケーションまたはオリジナル・インスタンス) にファイルをコピーします。コピーされたそのデータは、データベースの開始に使用されます。
   - **テスト**: このモードでは、エージェントは、vSnap リポジトリーから直接データ・ファイルを使用して新規データベースを作成します。
   - データベースを別のロケーションにリストアしていて、そのデータベースの名前を変更する場合は、データベース名を追加します。

   ヒント:

   「実動」は、オリジナル・ロケーションへのリストア操作で使用できる唯一の「**リストア方式**」です。選択したリストア操作に適していないオプションは選択できないようになっています。

   オリジナル・インスタンスにデータをリストアするには、オリジナル・インスタンスへのリストアの手順に従ってください。代替インスタンスにデータをリストアするには、代替インスタンスへのリストアの手順に従ってください。

8. 以下のオプションのいずれかを選択して、リストア操作の宛先を設定します。 「**次へ**」をクリックして先に進みます。
   - **オリジナル・インスタンスにリストアする**: このオプションでは、データをオリジナル・サーバーおよびオリジナル・インスタンスにリストアします。
   - **代替インスタンスにリストアする**: このオプションでは、指定された別のロケーションにデータをリストアして、そのロケーションにデータのコピーを作成します。

   代替ロケーションにデータをリストアする場合は、「**インスタンス**」テーブルでインスタンスを 選択してから、「**次へ**」をクリックします。代替インスタンスは、別のマシン上にあるものでなければなりま

せん。適さないインスタンスは選択できません。複数区画データベースの場合、ターゲット・インスタンスは、単一マシン上に同じ区画のセットを持っている必要があります。

9. 「**ジョブ・オプション**」ページで、定義しているリストア操作のリカバリー、アプリケーション、および高度なオプションを選択します。

   ヒント:

   リカバリー・オプションは、インスタント・アクセス・リストア・ジョブでは使用できません。

   - **リカバリーなし**。このオプションでは、リストア操作後のロールフォワード・リカバリーがスキップされます。ロールフォワード操作を手動で実行するかどうかを決定するまで、データベースはロールフォワード保留状態のままになります。
   - **バックアップの最後までリカバリーします**。このオプションでは、バックアップが作成された時点における状態に、選択されたデータベースがリカバリーされます。リカバリー・プロセスでは、Db2 データベース・バックアップに含まれているログ・ファイルが使用されます。
   - **使用可能なログの最後までリカバリーします**。このオプションは、Db2 バックアップ・ジョブ定義にログがバックアップされている場合にのみ使用できます。IBM Spectrum Protect Plus は最新のリストア・ポイントを使用します。ログ・バックアップの一時的なリストア・ポイントが自動的に作成されるため、Db2 データベースをログの最後までロールフォワードできます。このリカバリー・オプションは、特定のリストア・ポイントをリストから選択した場合には使用できません。このオプションは、最新のバックアップを使用するオンデマンドの特定時点リストア・ジョブを実行する場合にのみ使用できます。
   - **特定時点までリカバリーします**。このオプションには、特定時点までのすべてのバックアップ・データが含まれます。このオプションは、Db2 バックアップ・ジョブ定義でログ・バックアップを有効にしている場合にのみ使用できます。 特定の日時 (例えば、2019 年 1 月 1 日 12:18:00 AM) までの特定時点リカバリーを構成します。IBM Spectrum Protect Plus は、選択された特定時点の直前と直後のリストア・ポイントを検出します。リカバリー・プロセス中に、以前のデータ・バックアップ・ボリュームと新しいログ・バックアップ・ボリュームがマウントされます。特定時点が最後のバックアップより後である場合は、一時的なリストア・ポイントが作成されます。このリカバリー・オプションは、特定のリストア・ポイントをリストから選択した場合には使用できません。このオプションは、最新のバックアップを使用するオンデマンド特定時点リストア・ジョブを実行する場合にのみ使用できます。

   ヒント: 「リストア」ウィザードのオプションのステップをスキップするには、「**オプションのステップをスキップする**」を選択して、「**次へ**」をクリックします。

10. オプション: 「**ジョブ・オプション**」ページで、定義しているリストア操作のアプリケーション・オプションを選択します。

    ヒント:

    アプリケーション・オプションは、インスタント・アクセス・リストア・ジョブでは使用できません。

    - **既存のデータベースを上書きします**。このオプションは、リストア・リカバリー・プロセス中に名前が同じ既存のデータベースを置き換えるために使用します。このオプションが選択されない場合、リストア操作中に名前が同じデータベースが検出されると、リストア・ジョブは失敗します。このオプションを選択する場合は、Db2 ログ・ディレクトリーおよび Db2 ミラー・ログ・ディレクトリーにデータが格納されていないことを確認してください。

      重要: 他のデータベースがローカル・データベース・ディレクトリーを共有していないことを確認してください。このオプションが選択される場合、元のデータベースとそのデータが上書きされるためです。

    - **データベースごとの最大並列ストリーム数**。必要に応じて、データのリストア操作を並列ストリームで実行できます。このオプションは、大容量データベースをリストアする場合に役立ちます。
    - **Db2 データベース・メモリー・セットのサイズを KB 単位で指定します**。ターゲット・マシン上のデータベース・リストアに割り振られるメモリーを KB 単位で指定します。この値は、ターゲット・サーバー上の Db2 データベースの共有メモリー・サイズを変更するために使用されます。ソース・サーバーとターゲット・サーバーで同じ共有メモリー・サイズを使用するには、値をゼロに設定します。

11. オプション:「**ジョブ・オプション**」ページで、定義しているリストア操作の高度なオプションを選択します。
    - **ジョブが失敗したとき、即時にクリーンアップを実行します**。このオプションはデフォルトで選択されており、リカバリーが失敗した場合にリストア操作の一部として割り振り済みのリソースを自動的にクリーンアップします。
    - **いずれかが失敗しても、他の選択されたデータベースのリストアを続行する**。 このオプションでは、インスタンスの１つのデータベースを正常にリストアできない場合でも、リストア操作を続行します。リストアされているその他すべてのデータベースに対するプロセスは続行されます。このオプションが選択されていない場合、リソースのリカバリーが失敗すると、リストア・ジョブは停止します。
    - **マウント・ポイント接頭部**。インスタント・アクセス・リストア操作の場合、マウント・ポイントの送信先のパスの接頭部を指定します。
12. 「**スクリプトの適用**」ページでスクリプト・オプションを選択し、「**次へ**」をクリックして先に進みます。
    - 「**事前スクリプト**」を選択して、アップロード済みのスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択します。スクリプトが実行されるアプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。「**システム構成**」 > 「**スクリプト**」ページに移動して、スクリプトおよびスクリプト・サーバーを構成します。
    - 「**事後スクリプト**」を選択して、アップロード済みのスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択します。スクリプトが実行されるアプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。「**システム構成**」 > 「**スクリプト**」ページに移動して、スクリプトおよびスクリプト・サーバーを構成します。
    - ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。このオプションが有効になっている場合、事前スクリプトがゼロ以外の戻りコードで完了すると、バックアップまたはリストアのジョブの実行は続行され、事前スクリプト・タスクの状況は「完了」として返されます。事後スクリプトがゼロ以外の戻りコードで完了すると、事後スクリプト・タスクの状況は「完了」として返されます。このオプションが選択されない場合は、バックアップまたはリストアのジョブは実行されず、事前スクリプトまたは事後スクリプトのタスクの状況は「失敗」状況として返されます。
13. 「**スケジュール**」ページで、リストア・ジョブに名前を付け、ジョブを実行する頻度を選択します。開始時刻をスケジュールし、「**次へ**」をクリックして先に進みます。

    指定するリストア・ジョブがオンデマンド・ジョブの場合、スケジュールを入力するオプションはありません。スケジュールは、定期リストア・ジョブの場合にのみ指定します。
14. 「**確認**」ページで、リストア・ジョブ用の選択を確認します。リストア・ジョブのすべての詳細が正しい場合は、「**実行**」をクリックします。修正する場合は、「**戻る**」をクリックします。

タスクの結果

「**実行**」をクリックしてしばらくすると、「**onDemandRestore**」レコードが「**ジョブ・セッション**」ペインに追加されます。リストア操作の進行状況を表示するには、ジョブを展開します。ダウンロード・アイコン  をクリックして、ログ・ファイルをダウンロードすることもできます。実行中のジョブはすべて、「**ジョブと操作**」「**実行中のジョブ**」ページで表示できます。

オリジナル・インスタンスにデータをリストアするには、オリジナル・インスタンスへのリストアの手順に従ってください。代替インスタンスにデータをリストアするには、代替インスタンスへのリストアの手順に従ってください。

オリジナル・インスタンスへの Db2 データのリストア

データベース・バックアップを元のホスト上のオリジナル・インスタンスにリストアできます。Db2 データベースの最新のバックアップまたは以前のバージョンのバックアップにリストアすることができます。オリジナル・インスタンスにデータベースをバックアップする 場合は、データベースを名前変更することはできません。 このリストア操作では、データの完全な実動リストアが実行され、「**既存のデータベースを**

上書きします」オプションが選択されている場合にはターゲット・サイトで既存のデータが上書きされます。

始める前に

ご使用の Db2 環境に区画化データベースが含まれている場合、すべての区画のデータは、通常のバックアップ・ジョブの実行時にバックアップされます。すべてのインスタンスがバックアップ・ペインにリストされます。複数区画インスタンスは、区画番号とホスト名付きで示されます。

Db2 のリストア・ジョブを作成する前に、以下の要件が満たされていることを確認します。

- 少なくとも 1 つの Db2 バックアップ・ジョブがセットアップされていて正常に実行されている。バックアップ・ジョブのセットアップについての 説明は、144 ページの『Db2 データのバックアップ』を参照してください。
- リストア・ジョブをセットアップしているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当てについて詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」を展開して、「**リストア・ジョブの作成**」をクリックします。
   「スナップショットのリストア」ウィザードがオープンします。
2. オプション: 「**ジョブと操作**」ページから「リストア」ウィザードを起動した場合は、ソース・タイプとして Db2 を選択し、「**次へ**」をクリックします。

   ヒント : 「リストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
3. 「**ソースの選択**」ページで、Db2 インスタンスをクリックして、そのインスタンス内のデータベースを表示します。 データベース名の横にあるプラス・アイコン をクリックして、データベースを選択します。「**次へ**」をクリックして先に進みます。
4. 「**ソースページのスナップショット**」ページで、必要なリストア操作のタイプを選択します。
   - **オンデマンド: スナップショット**: データベース・スナップショットからの 1 回限りのリストア操作を作成します。このジョブは、反復する設定にはできません。
   - **オンデマンド: 特定時点**: データベースの特定時点バックアップからの 1 回限りのリストア操作を作成します。このジョブは、反復する設定にはできません。
   - **反復**: スケジュールで繰り返し実行される反復ジョブを作成します。

   ヒント :

   「**オンデマンド: スナップショット**」の場合、リカバリーしないか、バックアップの最後までリカバリーするかを選択できます。 「**オンデマンド: 特定時点**」リストア・ジョブの場合、使用可能なログの最後までリカバリーするか、特定時点までリカバリーするかを選択できます。
5. 同じページで、次のように「**リストア・ロケーションのタイプ**」を選択します。

位置	説明
サイト	1 次サイトまたは 2 次サイトからデータをリストアするには、このオプションを選択します。サイトは、オンデマンド特定時点リストア・ジョブの唯一の選択項目です。
クラウド・オフロード	クラウド・ストレージからデータをリストアするには、このオプションを選択します。スナップシ

位置	説明
	ョットに使用するリストア・ポイントを指定します。
リポジトリー・オフロード	vSnap リポジトリーからデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア･ポイントを指定します。
クラウド・アーカイブ	クラウドでアーカイブされたデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。
リポジトリー・アーカイブ	vSnap リポジトリーでアーカイブされたデータをリストアするには､このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。

オンデマンド・スナップショットの作成時に、探しているスナップショットにタイム・スパンを指定できます。該当する場合、別の vSnap サーバーを操作に使用することができます。

6. リストア操作のロケーションを選択します。以下のいずれかのオプションを選択して、「**次へ**」をクリックします。

オプション	説明
デモ	デモンストレーション vSnap サーバーからデータをリストアする場合、このオプションを選択します。このオプションは、特定のセットアップでのみ選択できます。
1 次	1 次 vSnap サーバーからターゲット宛先にデータをリストアする場合、このオプションを選択します。このロケーションは、リストア・ロケーション・タイプ「サイト」で使用可能です。
2 次	2 次 vSnap サーバーからターゲット宛先にデータをリストアする場合、このオプションを選択します。このロケーションは、リストア・ロケーション・タイプ「サイト」で使用可能です。

リストア・ポイントは、「**リストア・ポイント**」メニューから使用できます。

7. 「**リストア方式**」ページで、リストア操作として「**実動**」をクリックします。

「**実動**」モードでは、Db2 アプリケーション・サーバーは、最初に vSnap リポジトリー・ボリュームからターゲット・ホストにファイルをコピーします。 コピーされたそのデータは、データベースの開始に使用されます。

ヒント : 実動操作をオリジナル・インスタンスにリストアする場合は、新しいデータベース名は実装されないので入力しないでください。

8. リストア操作の宛先を「**オリジナル・インスタンスにリストア**」に設定して、データをオリジナル・サーバーにリストアします。「**次へ**」をクリックして先に進みます。
9. 150 ページの『Db2 データのリストア』 に説明しているように、オプションを選択します。
10. 「**スケジュール**」ページで、リストア・ジョブに名前を付け、ジョブを実行する頻度を選択します。開始時刻をスケジュールし、「**次へ**」をクリックして先に進みます。

指定するリストア・ジョブがオンデマンド・ジョブの場合、スケジュールを入力するオプションはありません。スケジュールは、定期リストア・ジョブの場合にのみ指定します。

11. 「**確認**」ページで、リストア・ジョブ用の選択を確認します。リストア・ジョブのすべての詳細が正しい場合は、「**実行**」をクリックします。修正する場合は、「**戻る**」をクリックします。

タスクの結果

「**実行**」をクリックしてしばらくすると、「**onDemandRestore**」レコードが「**ジョブ・セッション**」ペインに追加されます。リストア操作の進行状況を表示するには、ジョブを展開します。ダウンロード・アイコン  をクリックして、ログ・ファイルをダウンロードすることもできます。実行中のジョブはすべて、「**ジョブと操作**」「**実行中のジョブ**」ページで表示できます。

代替インスタンスへの Db2 データベースのリストア

Db2 データベースを代替ホスト上の Db2 インスタンスにリストアすることができます。 データベースを別の名前のインスタンスにリストアして、データベースを名前変更することもできます。このプロセスにより、別のホスト上の別のインスタンスにデータベースの正確なコピーが作成されます。リソースを代替ロケーションにリストアする場合、別々のターゲット・ホストを指定せずに、同じリソースを複数回リストアできます。

始める前に

重要 : すべてのリストア操作で、ソース・ホストとターゲット・ホストの DB2 のバージョン・レベルが同じでなければなりません。その要件に加えて、リストア対象のインスタンスと同じ名前のインスタンスがそれぞれのホスト上に存在することを確認する必要があります。この要件は、ターゲット・インスタンスが同じ名前である場合にも、名前が異なる場合にも適用されます。リストア操作が成功するためには、両方のインスタンスが、片方はオリジナルの名前、もう片方は新規名を使用してプロビジョンされる必要があります。

Db2 のリストア・ジョブを作成する前に、以下の要件が満たされていることを確認します。

- 少なくとも 1 つの Db2 バックアップ・ジョブがセットアップされていて正常に実行されている。バックアップ・ジョブのセットアップについての説明は、144 ページの『Db2 データのバックアップ』を参照してください。
- リストア・ジョブをセットアップしているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当てについて詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

代替インスタンスへのリストア操作を開始する前に、ソース・マシン上のファイル・システム構造がターゲット・マシンと一致していることを確認してください。このファイル・システム構造には、テーブル・スペース、オンライン・ログ、およびローカル・データベース・ディレクトリーが含まれます。十分なスペースがある専用のボリュームがファイル・システム構造に割り振られていることを確認してください。Db2 は、すべてのリストア操作のソースとターゲットのホストで同じバージョン・レベルでなければならず、同じ名前のインスタンスが各ホスト上になければなりません。 スペース所要量について詳しくは、Db2 保護のためのスペース所要量を参照してください。前提条件およびセットアップについて詳しくは、Db2 の前提条件を参照してください。

制約事項 : データベース・バックアップのリストア先のローカル・データベース・ディレクトリー上にデータが存在していて、「**既存のデータベースを上書きします**」オプションが選択されていない場合、リストア操作は失敗します。バックアップのリストア先のローカル・データベース・ディレクトリーを他のデータが共有することはできません。「**既存のデータベースを上書きします**」オプションを選択すると、代替ホスト上のローカル・データベース・ディレクトリーから既存のデータが削除されます。

注 : 複数区画データベースを代替ロケーションにリストアする 場合は、ターゲット・インスタンスがオリジナル・インスタンスと同じ区画番号で構成されていることを確認してください。 それらの区画はすべてが単一のホスト上になければなりません。 名前変更された新規インスタンスにデータをリストアする 場合、リストア操作に必要な両方のインスタンスを同数の区画で構成する必要があります。

このタスクについて

リダイレクトされるリストア操作のディスク・パスにインスタンス名とデータベース名が含まれていることを確認してください。この情報は、データベース・パス、コンテナー・パス、ストレージ・パス、ログ・パス、ミラー・ログ・パスのすべてのタイプのパスに必要です。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Db2**」を展開して、「**リストア・ジョブの作成**」をクリックします。
   「スナップショットのリストア」ウィザードがオープンします。
2. オプション: 「**ジョブと操作**」ページから「リストア」ウィザードを起動した場合は、ソース・タイプとして Db2 を選択し、「**次へ**」をクリックします。

   ヒント: 「リストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
3. 「**ソースの選択**」ページで、Db2 インスタンスをクリックして、そのインスタンス内のデータベースを表示します。 データベース名の横にあるプラス・アイコン をクリックして、データベースを選択します。「**次へ**」をクリックして先に進みます。
4. 「**ソースページのスナップショット**」ページで、必要なリストア操作のタイプを選択します。
   - **オンデマンド: スナップショット**: データベース・スナップショットからの 1 回限りのリストア操作を作成します。このジョブは、反復する設定にはできません。
   - **オンデマンド: 特定時点**: データベースの特定時点バックアップからの 1 回限りのリストア操作を作成します。このジョブは、反復する設定にはできません。
   - **反復**: スケジュールで繰り返し実行される反復ジョブを作成します。

   ヒント:

   「**オンデマンド: スナップショット**」の場合、リカバリーしないか、バックアップの最後までリカバリーするかを選択できます。 「**オンデマンド: 特定時点**」リストア・ジョブの場合、使用可能なログの最後までリカバリーするか、特定時点までリカバリーするかを選択できます。
5. 同じページで、次のように「**リストア・ロケーションのタイプ**」を選択します。

位置	説明
サイト	1 次サイトまたは 2 次サイトからデータをリストアするには、このオプションを選択します。サイトは、オンデマンド特定時点リストア・ジョブの唯一の選択項目です。
クラウド・オフロード	クラウド・ストレージからデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。
リポジトリー・オフロード	vSnap リポジトリーからデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。
クラウド・アーカイブ	クラウドでアーカイブされたデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。
リポジトリー・アーカイブ	vSnap リポジトリーでアーカイブされたデータをリストアするには、このオプションを選択します。スナップショットに使用するリストア・ポイントを指定します。

   オンデマンド・スナップショットの作成時に、探しているスナップショットにタイム・スパンを指定できます。該当する場合、別の vSnap サーバーを操作に使用することができます。
6. リストア操作のロケーションを選択します。以下のいずれかのオプションを選択して、「**次へ**」をクリックします。

オプション	説明
デモ	デモンストレーション vSnap サーバーからデータをリストアする場合、このオプションを選択します。このオプションは、特定のセットアップでのみ選択できます。
1 次	1 次 vSnap サーバーからターゲット宛先にデータをリストアする場合、このオプションを選択します。このロケーションは、リストア・ロケーション・タイプ「サイト」で使用可能です。
2 次	2 次 vSnap サーバーからターゲット宛先にデータをリストアする場合、このオプションを選択します。このロケーションは、リストア・ロケーション・タイプ「サイト」で使用可能です。

リストア・ポイントは、「**リストア・ポイント**」メニューから使用できます。

7. リストア操作に選択した宛先に適切な「**リストア方式**」を選択します。「**次へ**」をクリックして先に進みます。
   - **実動**: このモードでは、Db2 アプリケーション・サーバーは、最初に vSnap リポジトリー・ボリュームからターゲット・ホスト (代替ロケーションまたはオリジナル・インスタンス) にファイルをコピーします。コピーされたそのデータは、データベースの開始に使用されます。
   - **テスト**: このモードでは、エージェントは、vSnap リポジトリーから直接データ・ファイルを使用して新規データベースを作成します。
   - **インスタント・アクセス**: このモードでは、IBM Spectrum Protect Plus が vSnap リポジトリーからボリュームをマウントした後、それ以上のアクションは実行されません。マウントされたボリューム内のファイルからのカスタム・リカバリーにデータを使用します。
   - データベースを別のロケーションにリストアしていて、そのデータベースの名前を変更する場合は、データベース名を追加します。
8. リストア操作の宛先を「**代替インスタンスにリストアする**」に設定して、適格なロケーションのリストから選択できる別のロケーションにデータをリストアします。「**次へ**」をクリックして先に進みます。

   代替ロケーションにリストアする場合は、「**インスタンス**」テーブルでインスタンスを選択してから、「**次へ**」をクリックします。適さないターゲット・インスタンスは選択できません。
9. 150 ページの『Db2 データのリストア』 に説明しているように、オプションを選択します。
10. 「**スケジュール**」ページで、リストア・ジョブに名前を付け、ジョブを実行する頻度を選択します。開始時刻をスケジュールし、「**次へ**」をクリックして先に進みます。

    指定するリストア・ジョブがオンデマンド・ジョブの場合、スケジュールを入力するオプションはありません。スケジュールは、定期リストア・ジョブの場合にのみ指定します。
11. 「**確認**」ページで、リストア・ジョブ用の選択を確認します。リストア・ジョブのすべての詳細が正しい場合は、「**実行**」をクリックします。修正する場合は、「**戻る**」をクリックします。

タスクの結果

「**実行**」をクリックしてしばらくすると、「**onDemandRestore**」レコードが「**ジョブ・セッション**」ペインに追加されます。リストア操作の進行状況を表示するには、ジョブを展開します。ダウンロード・アイコン  をクリックして、ログ・ファイルをダウンロードすることもできます。実行中のジョブはすべて、「**ジョブと操作**」「**実行中のジョブ**」ページで表示できます。

Microsoft Exchange Server

Microsoft Exchange Server を正常に登録した後、IBM Spectrum Protect Plus で Microsoft Exchange データの保護を開始できます。SLA ポリシーを定義して、特定のスケジュール、保存ポリシー、およびスクリプトを使用してバックアップ・ジョブを作成します。

Microsoft Exchange Server の前提条件

IBM Spectrum Protect Plus を使用して Microsoft Exchange データベースの保護を開始する前に、Microsoft Exchange アプリケーションのすべての前提条件が満たされていることを確認します。

詳しくは、27 ページの『Microsoft Exchange Server の要件』を参照してください。

仮想化のサポート

IBM Spectrum Protect Plus は、物理 (ベアメタル) サーバーだけでなく、仮想化環境で実行されている Microsoft Exchange Server をサポートします。以下の仮想化環境がサポートされます。

- VMware ESX ゲスト・オペレーティング・システム
- Microsoft Windows Hyper-V ゲスト・オペレーティング・システム

特権

Microsoft Exchange エージェントが IBM Spectrum Protect Plus 環境で動作できるようにするには、該当する特権をセットアップする必要があります。

役割ベースのアクセス制御

IBM Spectrum Protect Plus のセキュリティーのために、Exchange Server にログオンするユーザーは、メールボックスにアクセスし、メールボックスのリストア・タスクを実行するための役割ベースのアクセス制御 (RBAC) 権限を持っている必要があります。

メールボックス・リストア・タスクを実行する各 Exchange ユーザーに以下の管理役割を割り当てる必要があります。

- アクティブ・ディレクトリー許可
- ApplicationImpersonation
- データベース
- 災害時回復
- メールボックスのインポート/エクスポート
- パブリック・フォルダー
- 表示専用構成
- 表示専用の受信者

メールボックス・リストア・タスクを実行させたいユーザーを、上記役割が含まれている Exchange Server 役割グループに配置することを推奨します。

Exchange Server には、いくつかの組み込み役割グループが含まれています。組織の管理役割グループには、デフォルトで、上に列記されている役割のすべてではなくとも、ほとんどが含まれています。

メールボックス・リストア・タスクを実行させたいユーザーを、組織管理役割グループ (上に列記されているすべての役割が含まれていることを確認します) に配置することを推奨します。

あるいは、そのユーザーを、すでに作成してある別の役割グループや、上に列記されている役割が含まれている他の任意の組み込み役割グループに配置することも可能です。

注 : Exchange の Organization Management (組織の管理) 役割グループまたはサブグループに 名前が含まれていないユーザーの場合、リストア操作の実行時にパフォーマンスが低下する可能性があります。

注 : ユーザー名が組織のセキュリティー・ポリシーで許可されている場合に**限り**、Exchange 管理センター (EAC) または Exchange Powershell Cmdlet を使用して Exchange 役割グループを管理できます。

管理役割スコープ

以下の Exchange オブジェクトが Exchange ユーザーの管理役割スコープ内にあることを確認します。

- 必要なデータが含まれている Exchange Server。
- IBM Spectrum Protect Plus によって作成されるリカバリー・データベース。
- アクティブ・メールボックスが含まれるデータベース。
- リストア操作を実行するユーザーのアクティブ・メールボックスが含まれるデータベース。

Exchange ユーザー名が、ローカルの Administrator (管理者) グループのメンバーであり、ドメイン内にアクティブな Exchange メールボックスを持っていることを確認してください。デフォルトで、Windows は、Exchange の Organization Administrators (組織管理者) グループを他のセキュリティー・グループ (ローカルの Administrators グループなど) に追加します。Exchange の Organization Management (組織の管理) グループのメンバーではない Exchange ユーザーの場合、ドメイン・メンバーのコンピューターで「ローカル ユーザーとグループ」ツールを使用して、ユーザー・アカウントをローカルの Administrators (管理者) グループに手動で追加する必要があります。

ドメイン・メンバーのコンピューターで、「**管理ツール**」**>** 「**コンピューターの管理**」**>**「**ローカル ユーザーとグループ**」**ツール**をクリックします。ローカルの Administrators グループも「ローカル ユーザーとグループ」ツールもないドメイン・コントローラー・コンピューターでは、「**管理ツール**」**>**「**Active Directory ユーザーとコンピューター**」**ツール**をクリックして、ドメイン内の Administrators (管理者) グループに手動でユーザー・アカウントを追加します。

暗号化ファイル・システム

IBM Spectrum Protect Plus for Exchange では、暗号化ファイル・システム (EFS) がローカルまたはグループ・ドメイン・ポリシーで使用可能であり、有効な Domain Data Recovery Agent (DRA) 証明書が入手可能であることが必要です。カスタム・グループ・ポリシーが定義され、組織単位にリンクされている場合、Exchange Server が組織単位に含まれていることを確認してください。

Microsoft Exchange アプリケーション・サーバーの追加

Microsoft Exchange Server を登録すると、Exchange データベースのインベントリーが IBM Spectrum Protect Plus に追加されます。インベントリーを使用できるようになると、Exchange データベースのバックアップとリストアを開始して、レポートを実行することができます。

このタスクについて

Microsoft Exchange アプリケーション・サーバーを登録するには、IP アドレスまたはホスト名が必要です。

手順

Microsoft Exchange アプリケーション・サーバーを追加するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」**>**「**アプリケーション**」**>**「**Exchange**」を展開します。
2. 「**Exchange**」ページで、「**アプリケーション・サーバーの管理**」をクリックして、「**アプリケーション・サーバーの追加**」をクリックし、ホスト・システムを追加します。
3. 「**アプリケーション・プロパティー**」フォームに IP アドレスまたはホスト・アドレスを入力します。
4. 活動ディレクトリー・ドメインとユーザー・アカウントの形式 (domain¥user) のユーザー ID と関連するパスワードを入力します。このユーザーには、正しい Exchange 役割と特権が必要です。Exchange 特権について詳しくは、160 ページの『特権』を参照してください。
5. 「**保存**」をクリックして、上記のステップを繰り返し、他の Microsoft Exchange インスタンスを IBM Spectrum Protect Plus に追加します。

   重要 : データベース可用性グループ (DAG) 環境では、すべての Microsoft Exchange アプリケーション・サーバーを DAG に登録します。

次のタスク

Exchange アプリケーション・サーバーを IBM Spectrum Protect Plus に追加すると、各インスタンスでインベントリーが自動的に実行されます。データベースを保護するためには、データベースが検出される必要があります。いつでも手動でインベントリーを実行して更新を検出することができます。手動でインベントリーを実行する手順については、162 ページの『インベントリーの実行による Microsoft Exchange データベースの検出』を参照してください。Exchange データベース・バックアップ・ジョブのセットアップについての説明は、163 ページの『SLA バックアップ・ジョブの定義』を参照してください。

インベントリーの実行による Microsoft Exchange データベースの検出

Microsoft Exchange Server インスタンスを IBM Spectrum Protect Plus に追加すると、インベントリーが自動的に実行されます。ただし、更新を検出したり、各インスタンスのすべての Exchange データベースをリストしたりするために、いつでも Exchange アプリケーション・サーバーでインベントリーを手動で実行できます。

始める前に

Exchange インスタンスを IBM Spectrum Protect Plus に追加したことを確認してください。Exchange インスタンスを追加する手順については、161 ページの『Microsoft Exchange アプリケーション・サーバーの追加』を参照してください。

手順

1. ナビゲーション・ペインで、「**保護の管理**」>「**アプリケーション**」>「**Exchange**」を展開します。
2. 「**インベントリーの実行**」をクリックします。

   インベントリーの実行中、ボタンのラベルが「**インベントリーが進行中**」に変わります。任意の使用可能なアプリケーション・サーバーでインベントリーを実行できますが、インベントリー・プロセスは一度に 1 つしか実行できません。
3. インベントリー・ジョブをモニターするには、「**ジョブと操作**」に進みます。「**実行中のジョブ**」タブをクリックして、最新のアプリケーション・サーバー・インベントリー・ログ項目を見つけます。

   完了したジョブは「**ジョブ・ヒストリー**」タブに表示されます。「**ソート順**」リストを使用して、開始時刻、タイプ、状況、ジョブ名、または所要時間に基づいてジョブをソートすることができます。ジョブを名前で検索するには、「**名前での検索**」フィールドを使用します。名前ではワイルドカード文字としてアスタリスクを使用できます。
4. インベントリー・ジョブが完了したら、「**Exchange バックアップ**」ペインで Exchange インスタンスをクリックし、そのインスタンスで検出されたデータベースを示すビューを開きます。「**インスタンス**」リストでデータベースが欠落している場合は、Microsoft Exchange アプリケーション・サーバーを確認して、インベントリーを再実行します。

   ヒント: インスタンスのリストに戻るには、「Exchange バックアップ」ペインの「**インスタンス**」ハイパーテキストをクリックします。

Microsoft Exchange 接続のテスト

Microsoft Exchange アプリケーション・サーバーを登録してアプリケーション・サーバー・リストに追加した後、接続をテストします。このテストでは、IBM Spectrum Protect Plus とホスト・アプリケーション・サーバーの間の通信が検査されます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 >「**アプリケーション**」 >「**Exchange**」を展開します。
2. 「**Exchange**」ページで、「**アプリケーション・サーバーの管理**」をクリックします。

   使用可能な Microsoft Exchange アプリケーション・サーバーが表示されます。
3. テストする Microsoft Exchange アプリケーション・サーバーの「**アクション**」をクリックして、「**テスト**」をクリックします。

   テスト・レポートに、実行されたテストとその状況のリストが表示されます。各テスト手順には、物理ホスト・ネットワーク構成のテスト、リモート・セッション・テスト、およびユーザー管理者特権などの Windows 前提条件のテストが含まれます。

4.「**OK**」をクリックしてテストを閉じます。すべての問題を修正した後、テストを再実行します。

Microsoft Exchange データベースのバックアップ

Microsoft Exchange データベースを保護する目的で、増分バックアップを作成するために継続的に実行されるバックアップ・ジョブを定義できます。また、スケジュール外でオンデマンド・バックアップ・ジョブも実行できます。

始める前に

バックアップする Exchange データベースが含まれているアプリケーション・サーバーが追加されていることを確認してください。詳しくは、161 ページの『Microsoft Exchange アプリケーション・サーバーの追加』を参照してください。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」を展開します。
2.「**Exchange バックアップ**」ペインで、Microsoft Exchange インスタンスをクリックしてから、バックアップするデータベースを選択します。

   各データベースは、インスタンス名、データベース名、適用された SLA ポリシー、およびログ・バックアップの適格性ごとにリストされます。
3.「**実行**」をクリックします。

   バックアップ・ジョブが始まると、「**ジョブと操作**」 > 「**ジョブの実行**」で詳細を確認できます。

   ヒント：「**実行**」ボタンは単一のデータベース・バックアップについてのみ有効であり、該当のデータベースに SLA ポリシーが適用されている必要があります。
4. 複数のデータベースに対してバックアップ・ジョブを実行するには、「Exchange バックアップ」ペインで該当のデータベースを選択して、「**SLA ポリシーの選択**」をクリックします。

   SLA ポリシーのバックアップ・ジョブの定義およびバックアップ・ジョブ・オプションについて詳しくは、163 ページの『SLA バックアップ・ジョブの定義』を参照してください。

SLA バックアップ・ジョブの定義

Exchange インスタンスごとに Microsoft Exchange データベースがリストされた後、SLA ポリシーを選択して適用し、データの保護を開始します。

このタスクについて

IBM Spectrum Protect Plus は、Exchange バックアップ・ジョブごとに単一または複数の Microsoft Exchange データベースをサポートします。複数のデータベース・バックアップ・ジョブは順次に実行されます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」を展開します。
2. Exchange インスタンスを選択して、そのインスタンスのすべてのデータをバックアップするか、インスタンス名をクリックして、バックアップする個々のデータベースを選択します。
3.「**SLA ポリシーの選択**」をクリックして、SLA ポリシーを選択します。

   事前定義の選択項目は、それぞれ頻度と保存率が異なる「ゴールド」、「シルバー」、および「ブロンズ」です。「ゴールド」は、頻度が最も高く、保存率が最短です。カスタムの SLA ポリシーを作成したり、既存のポリシーを編集したりすることもできます。詳しくは、89 ページの『SLA ポリシーの作成』を参照してください。
4.「**オプションの選択**」をクリックして、バックアップのオプションを定義します。例えば、以降のリカバリー・オプションのログ・バックアップを有効にしたり、並列ストリームを指定して大容量データベースのバックアップに要する時間を短縮したりすることができます。変更内容を保存します。
5.「**SLA ポリシーのステータス**」テーブルの「**ポリシー・オプション**」列のアイコンをクリックして、SLA ポリシーを構成します。

SLA 構成について詳しくは、164 ページの『バックアップ・ジョブ用の SLA 構成オプションの設定』を参照してください。

6. スケジュールに入れられたジョブの外部でポリシーを実行するには、インスタンスまたはデータベースを選択して、「**アクション**」>「**開始**」をクリックします。

   選択した SLA の状況が「**実行**」に変わります。スケジュールを一時停止するには、「**アクション**」>「**スケジュールの一時停止**」をクリックします。ジョブを開始後にキャンセルするには、「**アクション**」>「**キャンセル**」をクリックします。

バックアップ・ジョブ用の SLA 構成オプションの設定

バックアップ・ジョブ用の SLA をセットアップした後、そのジョブに対してさらに多くのオプションを構成できます。追加の SLA オプションには、スクリプトの実行、バックアップ操作からのリソースの除外、必要に応じたフル基本バックアップ・コピーの強制実行があります。

手順

1. 構成するジョブの「**SLA ポリシーのステータス**」テーブルの「**ポリシー・オプション**」列で、クリップボード・アイコンをクリックして、追加の構成オプションを指定します。
2. 事前スクリプト構成を定義するには、「**事前スクリプト**」を選択して、以下のいずれかのアクションを実行します。
   - スクリプト・サーバーを使用するには、「**スクリプト・サーバーの使用**」を選択して、アップロード済みのスクリプトを「**スクリプト**」または「**スクリプト・サーバー**」のリストから選択します。
   - アプリケーション・サーバーでスクリプトを実行するには、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアして、「**アプリケーション・サーバー**」リストからアプリケーション・サーバーを選択します。
3. 事後スクリプト構成を定義するには、「**事後スクリプト**」を選択して、以下のいずれかのアクションを実行します。
   - スクリプト・サーバーを使用するには、「**スクリプト・サーバーの使用**」を選択して、アップロード済みのスクリプトを「**スクリプト**」または「**スクリプト・サーバー**」のリストから選択します。
   - アプリケーション・サーバーでスクリプトを実行するには、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアして、「**アプリケーション・サーバー**」リストからアプリケーション・サーバーを選択します。

   スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。
4. ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。

   このオプションが選択される場合、スクリプトの処理がゼロ以外の戻りコードで完了すると、バックアップまたはリストアの操作は試行され、スクリプト・タスクの状況は「完了」として報告されます。このオプションが選択されない場合は、バックアップまたはリストアは試行されず、スクリプト・タスクの状況は「失敗」として報告されます。
5. バックアップ・ジョブから除外するリソースを指定します。「**リソースの除外**」フィールドに正確なリソース名を入力します。名前が不明な場合は、ワイルドカードのアスタリスクをパターンの前 (**text*) またはパターンの後 (*text**) に指定して使用します。標準の英数字と特殊文字 (-、_、*) を使用して複数のワイルドカードを入力できます。 項目はセミコロンで区切ってください。
6. 特定のリソースのフルバックアップを 作成するには、そのリソースの名前を「**リソースのフルバックアップを強制します**」フィールドに入力します。複数のリソースはセミコロンで区切ります。

   フルバックアップにより、1 つのオカレンスでのみ、そのリソースの既存のバックアップが置き換えられます。その後、そのリソースは以前と同様に増分バックアップされます。
7. 「**保存**」をクリックします。

Microsoft Exchange データベース・ログのバックアップ

Microsoft Exchange データベースのデータベース・トランザクション・ログをバックアップできます。Exchange ログ・バックアップは、Windows タスク・スケジューラーを使用してスケジュールに入れられま

す。ログ・バックアップを使用できるようになると、リストア操作時にロールフォワード・データ・リカバリーを実行して、データが可能な限り最新の特定時点にリカバリーされるようにすることができます。

このタスクについて

ログ・バックアップが有効になっていると、Exchange サーバーでタスク・スケジューラー・タスクが作成されます。このタスクは、SLA ポリシーに従って Exchange ログ・ファイルのバックアップ操作を実行します。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」を展開します。
2. 保護する Microsoft Exchange インスタンスをクリックしてから、ログをバックアップするデータベースを選択します。

   ヒント : 「**ログ・バックアップに適格です**」列に、ログ・バックアップを実行できるデータベースが示されます。データベースがログ・バックアップに適格ではないものとして登録されている場合は、ホバー・ヘルプで説明が示されます。
3. 「**オプションの選択**」をクリックしてから、「**ログ・バックアップを有効にします**」を選択します。
4. ログ・バックアップの頻度を日単位、時間単位、分単位で入力します。
5. 開始日を選択して、ログ・バックアップを開始する時刻を選択し、「**保存**」をクリックします。

タスクの結果

データベース・トランザクション・ログは、選択された頻度で vSnap サーバーにバックアップされます。

制約事項 : データベース・ログは、優先ノードにのみバックアップされます。vSnap サーバーにログ・バックアップを書き込むことができる Microsoft Exchange インスタンスは一度に 1 つのみです。

ログ・バックアップの問題が発生した場合は、IBM Spectrum Protect Plus でアラート通知に表示されます。

データベース可用性グループ内の Exchange データベースのバックアップ

Microsoft Exchange データベース可用性グループ (DAG) のメールボックス・データベースをバックアップして、データベースのアクティブ・コピーまたはパッシブ・コピーのどちらをバックアップに使用するかを指定できます。DAG 環境の Exchange サーバーは、高可用性を得るためにアクティブ・コピーとパッシブ・コピーの間でデータを同期します。

このタスクについて

IBM Spectrum Protect Plus は、インベントリー・ジョブの情報を使用して、Exchange DAG 環境のすべてのデータベースを表示する DAG ビューを提供します。データベースごとに、DAG の 1 つのサーバー上にアクティブ・コピーがあり、他のサーバー上に 1 つ以上のパッシブ・コピーがあります。デフォルトでは、スケジュールされたバックアップは、データベースがアクティブになっているサーバーから 取られますが、別のサーバーを選択してデータベースのパッシブ・コピーをバックアップすることもできます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」>「**アプリケーション**」>「**Exchange**」を展開します。
2. 「**Exchange バックアップ**」ペインで、「**表示**」メニューをクリックして、「**データベース可用性グループ**」を選択します。
3. 表示する Microsoft Exchange DAG をクリックしてから、バックアップするデータベースを選択します。
4. 「**オプションの選択**」をクリックします。「**優先ノードのバックアップ**」 リストで、バックアップを実行するインスタンスを選択します。

   「**優先ノードのバックアップ**」オプションでは、バックアップするデータベースのパッシブ・コピーを選択できます。
5. 「**SLA ポリシーの選択**」をクリックして、SLA ポリシーをリストから選択します。
6. デフォルトのオプションを 使用してジョブ定義を作成するには、「**保存**」をクリックします。

選択された SLA ポリシーおよび優先ノードの選択に従って、DAG データベースのバックアップ・ジョブがスケジュールされます。

7. 選択したポリシーをスケジュール外で実行するには、「**SLA ポリシーのステータス**」ペインで、「**アクション**」>「**開始**」をクリックします。

永久増分バックアップ戦略

IBM Spectrum Protect Plus では、永久増分バックアップ と呼ばれるバックアップ戦略が提供されています。定期的フルバックアップ・ジョブをスケジュールするのではなく、このバックアップ・ソリューションでは、フルバックアップは 最初に 1 回行うだけで済みます。その後、一連の継続的な増分バックアップ・ジョブが行われます。

永久増分バックアップ・ソリューションには、以下の利点があります。

- ネットワークでの送信データ量が削減される
- すべての増分バックアップには、前回のバックアップ以降に変更されたブロックしか含まれていないため、データの増大が削減される
- バックアップ・ジョブの所要時間が短縮される

IBM Spectrum Protect Plus 永久増分バックアップ・プロセスには、以下のステップがあります。

1. 最初のバックアップ・ジョブでは、Exchange アプリケーションの VSS スナップショットが作成されます。その結果、データベース・ファイルはアプリケーション整合状態になります。データベース・ファイル全体が vSnap ロケーションにコピーされます。
2. それ以降のすべてのバックアップでは、Exchange アプリケーションの VSS スナップショットが作成されます。データベース・ファイルはアプリケーション整合状態になります。ただし、データベース・ファイルの変更ブロックのみが vSnap ロケーションにコピーされます。
3. バックアップが実行される各特定時点でバックアップが再構成され、単一のバックアップ時点からのデータベースのリカバリーが可能になります。

Microsoft Exchange データベースのリストア

Microsoft Exchange データベースのデータが失われたり破損したりした場合は、バックアップ・コピーからデータをリストアできます。「スナップショットのリストア」ウィザードを使用して、リストア・ジョブ・スケジュールまたはオンデマンド・リストア操作をセットアップします。元のインスタンスまたは代替インスタンスにデータをリストアするジョブを定義でき、さまざまなタイプのリカバリー・オプションと構成を選択できます。

始める前に

次の要件を満たしているようにしてください。

- 少なくとも 1 つの Microsoft Exchange バックアップ・ジョブが定義されていて正常に実行されている。バックアップ・ジョブの定義についての説明は、163 ページの『SLA バックアップ・ジョブの定義』を参照してください。
- リストア・ジョブを定義しているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当てについて詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

重要 : 高細分度リストア操作では、Exchange アプリケーション・サーバーにログオンし、Microsoft 管理コンソール (MMC) GUI を使用して、メールボックス・バッチ・リストアおよびメールボックス・リストア・ブラウザー・タスクを実行する必要があります。

手順

Microsoft Exchange データベースのデータをリストアするには、以下のいずれかのアクションを実行します。

- 元のインスタンスとロケーションにデータベースをリストアします。
- 別のファイルのロケーションを指定して、元のインスタンスにデータベースをリストアします。
- 代替インスタンスにデータベースをリストアします。
- 高細分度リストア機能を使用して、メールボックス・データをリストアします。
- データベース可用性グループ (DAG) のデータベースをリストアします。

オリジナル・インスタンスへの Microsoft Exchange データベースのリストア
実動モードまたはテスト・モードを使用して、Microsoft Exchange データベースをオリジナル・インスタンスにリストアします。Exchange データベースの最新のバックアップまたは以前のバージョンのバックアップのどちらにリストアするかを選択します。

始める前に
次の要件を満たしているようにしてください。

- 少なくとも 1 つの Microsoft Exchange バックアップ・ジョブが定義されていて正常に実行されている。
- リストア・ジョブを定義しているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当てについて詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。

このタスクについて
実動モードでオリジナル・ロケーションにデータベースをリストアする 場合は、データベースを名前変更することはできません。このリストア操作では、完全な実動リストア操作が実行され、ターゲット・サイトの既存のデータは上書きされます。

手順

Exchange リストア・ジョブを定義するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Exchange**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。
2. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。
   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。複数のデータベースをリストから選択できます。

   選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。
   c) 「**次へ**」をクリックして先に進みます。
3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを 指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。

オプション	説明
	オンデマンド: スナップショット データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。

オプション	説明
	クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、「**オリジナル・インスタンスにリストアする**」を選択して、「**次へ**」をクリックします。
5. 「**リストア方式**」ページで、以下のオプションから選択します。
   - **テスト**。テスト・モードでは、エージェントは、vSnap リポジトリーから直接データ・ファイルを使用して新規データベースを作成します。このリストア・タイプは、テストの目的で使用できます。
   - **実動**。実動モードでは、エージェントはまず vSnap ボリュームから 1 次ストレージにファイルをリストアし、次にそのリストアされたファイルを使用して新規データベースを作成します。

   「テスト」リストアの場合のみ、「**新規データベース名**」フィールドに、リストアするデータベースの新しい名前を入力します。「**新規データベース名**」フィールドは、「実動」リストアを選択する場合にも表示されますが、このフィールドは、オリジナル・インスタンスの新しいデータベース・ロケーションにリストアするために使用します。このタスクの詳細な手順については、170 ページの『オリジナル・インスタンスの新規ロケーションへの Exchange データベースのリストア』を参照してください。
6. オプション: 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   リカバリー・オプション
   以下のリカバリー・オプションから選択します。

   リカバリーなし
   このオプションでは、リストア操作後のロールフォワード・リカバリーがスキップされます。ロールフォワード・リカバリーを手動で実行するかどうかを決定するまで、データベースはロールフォワード保留状態のままになります。

   バックアップの最後までリカバリーします
   選択済みデータベースをリストアして、バックアップの作成時の状態に戻します。

   使用可能なログの最後までリカバリーします
   このオプションでは、データベースがリストアされ、すべての使用可能なログ (アプリケーション・サーバー上に存在する可能性があるバックアップよりも新しいログを含む) が適用され、可能な限り最新の時点までデータベースがリカバリーされます。このオプションは、バックアップ・ジョブで「**ログ・バックアップを有効にする**」を選択している場合にのみ使用できます。

   特定時点までリカバリーします
   ログ・バックアップが使用可能な場合、このオプションでは、データベースがリストアされ、ログ・バックアップ・ボリュームのログが適用され、ユーザーが指定する中間の特定時点までデータベースがリカバリーされます。日時を「**時刻別**」オプションから選択します。

   アプリケーション・オプション
   以下のアプリケーション・オプションを設定します。

   データベースごとの最大並列ストリーム数
   バックアップ・ストレージからのデータベースごとの最大データ・ストリームを設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を 1 に設定すると、複数のデータベースのリストアを並列に実行できます。複数の並列ストリームでリストア速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

   このオプションは、Exchange データベースを元のデータベース名を使用して元の位置にリストアする場合にのみ適用可能です。

高度なオプション
以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
リカバリーが失敗した場合、リストアの一部として、割り振り済みのリソースを自動的にクリーンアップするには、このオプションを有効にします。

7. オプション:「**スクリプトの適用**」ページで、適用する「**事前スクリプト**」または「**事後スクリプト**」を選択するか、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。
   リストア・ジョブが作成され、「**ジョブと操作**」 > 「**実行中のジョブ**」でそのジョブのステータスを確認できます。

オリジナル・インスタンスの新規ロケーションへの Exchange データベースのリストア

Microsoft Exchange データベースをオリジナル・インスタンスにリストアしますが、この手順ではアプリケーション・サーバー上の新規ロケーションにリストアできます。Exchange データベースの最新のバックアップまたは以前のバージョンのバックアップのどちらにリストアするかを 選択します。

このタスクについて

実動リストア操作を使用してデータベースをオリジナル・インスタンスにリストアする場合、リストアするデータベースに新規名を指定して、アプリケーション・サーバー上の新規ファイル・ロケーションにデータベースをリストアできます。実動モードでは、エージェントはまず vSnap ボリュームから 1 次ストレージにファイルをリストアし、次にそのリストアされたファイルを使用して新規データベースを作成します。

手順

Exchange リストア・ジョブを定義するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Exchange**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。
2. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。
   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。複数のデータベースをリストから選択できます。
   選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。
   c) 「**次へ**」をクリックして先に進みます。
3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを 指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。

オプション	説明
	クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、「**オリジナル・インスタンスにリストアする**」を選択して、「**次へ**」をクリックします。
5. 「**リストア方式**」ページで、「**実動**」リストア・オプションをクリックします。

   ヒント: このリストア操作に対しては、実動モードの選択が必須です。

   a) 「**名前**」フィールドで、データベース名を展開して、アプリケーション・サーバー上の既存のデータベースのパス情報を表示します。

   b) 「**新規データベース名**」フィールドに、リストアするデータベースの新しい名前を入力します。

   c) 「**宛先パス**」 フィールドで、Exchange データベース・ファイルの新規ロケーション (.edb の名前を含む) およびログのロケーションを追加します。
   例えば、データベース名が Database_A.edb の場合は、C:¥ExchangeDatabase¥Database_A ¥Database_A.edb と入力して、ログのロケーションとして (「**ソース・パス**」 E01) D:¥ExchangeDatabase¥Logs¥Database_A¥ と入力します。
6. オプション: 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   リカバリー・オプション
   以下のリカバリー・オプションから選択します。

   リカバリーなし
   このオプションでは、リストア操作後のロールフォワード・リカバリーがスキップされます。ロールフォワード・リカバリーを手動で実行するかどうかを決定するまで、データベースはロールフォワード保留状態のままになります。

   バックアップの最後までリカバリーします
   選択済みデータベースをリストアして、バックアップの作成時の状態に戻します。

   使用可能なログの最後までリカバリーします
   このオプションでは、データベースがリストアされ、すべての使用可能なログ (アプリケーション・サーバー上に存在する可能性があるバックアップよりも新しいログを含む) が適用され、可能な限り最新の時点までデータベースがリカバリーされます。このオプションは、バックアップ・ジョブで「**ログ・バックアップを有効にする**」を選択している場合にのみ使用できます。

   特定時点までリカバリーします
   ログ・バックアップが使用可能な場合、このオプションでは、データベースがリストアされ、ログ・バックアップ・ボリュームのログが適用され、ユーザーが指定する中間の特定時点までデータベースがリカバリーされます。日時を「**時刻別**」オプションから選択します。

   アプリケーション・オプション
   以下のアプリケーション・オプションを設定します。

   データベースごとの最大並列ストリーム数
   バックアップ・ストレージからのデータベースごとの最大データ・ストリームを設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を 1 に設定すると、複数のデータベースのリストアを並列に実行できます。複数の並列ストリームでリストア速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

   このオプションは、Exchange データベースを元のデータベース名を使用して元の位置にリストアする場合にのみ適用可能です。

高度なオプション
以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
リカバリーが失敗した場合、リストアの一部として、割り振り済みのリソースを自動的にクリーンアップするには、このオプションを有効にします。

7. オプション:「**スクリプトの適用**」ページで、適用する「**事前スクリプト**」または「**事後スクリプト**」を選択するか、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。
   リストア・ジョブが作成され、「**ジョブと操作**」 > 「**実行中のジョブ**」でそのジョブのステータスを確認できます。

代替インスタンスへの Microsoft Exchange データベースのリストア

Microsoft Exchange データベース・バックアップを選択して、代替ホスト上の Exchange Server インスタンスにリストアすることができます。実動モードまたはテスト・モードで、データベースを代替インスタンスにリストアできます。

始める前に

次の要件を満たしていることを確認してください。

- ファイルをコピーするのに十分なディスク・スペースがあり、専用ボリュームが割り振られている。
- ソース・サーバー上のファイル・システム構造がターゲット・サーバー上のファイル・システム構造と同じである。このファイル・システム構造には、テーブル・スペース、オンライン・ログ、およびローカル・データベース・ディレクトリーが含まれます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Exchange**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。
2. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。
   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。複数のデータベースをリストから選択できます。
   選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。
   c) 「**次へ**」をクリックして先に進みます。
3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。

オプション	説明
	クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、「**代替インスタンスにリストアする**」を選択し、データベースのリストア先にするターゲット・インスタンスを選択して、「**次へ**」をクリックします。
5. 「**リストア方式**」ページで、以下のオプションから選択します。
   - **テスト**。テスト・モードでは、エージェントは、vSnap リポジトリーから直接データ・ファイルを使用して新規データベースを作成します。このリストア・タイプは、テストの目的で使用できます。
   - **実動**。実動モードでは、エージェントはまず vSnap ボリュームから 1 次ストレージにファイルをリストアし、次にそのリストアされたファイルを使用して新規データベースを作成します。

   a) 「**新規データベース名**」フィールドに新しいデータベース名を入力します。

   b) (実動リストアのみ) データベース名を展開して、パス情報を表示します。「**宛先パス**」フィールドで、代替ホスト上の Exchange データベース・ファイルのロケーション (.edb の名前を含む) およびログのロケーションを追加します。

   例えば、データベース名が Database_A.edb の場合は、 C:¥ExchangeDatabase¥Database_A ¥Database_A.edb と入力して、ログのロケーションとして c:¥ExchangeDatabase¥Logs ¥Database_A¥ と入力します。
6. オプション: 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   リカバリー・オプション

   以下のリカバリー・オプションから選択します。

   リカバリーなし

   このオプションでは、リストア操作後のロールフォワード・リカバリーがスキップされます。ロールフォワード・リカバリーを手動で実行するかどうかを決定するまで、データベースはロールフォワード保留状態のままになります。

   バックアップの最後までリカバリーします

   選択済みデータベースをリストアして、バックアップの作成時の状態に戻します。

   使用可能なログの最後までリカバリーします

   このオプションでは、データベースがリストアされ、すべての使用可能なログ (アプリケーション・サーバー上に存在する可能性があるバックアップよりも新しいログを含む) が適用され、可能な限り最新の時点までデータベースがリカバリーされます。このオプションは、バックアップ・ジョブで「**ログ・バックアップを有効にする**」を選択している場合にのみ使用できます。

   特定時点までリカバリーします

   ログ・バックアップが使用可能な場合、このオプションでは、データベースがリストアされ、ログ・バックアップ・ボリュームのログが適用され、ユーザーが指定する中間の特定時点までデータベースがリカバリーされます。日時を「**時刻別**」オプションから選択します。

   アプリケーション・オプション

   以下のアプリケーション・オプションを設定します。

   データベースごとの最大並列ストリーム数

   バックアップ・ストレージからのデータベースごとの最大データ・ストリームを設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を 1 に設定すると、複数のデータベースのリストアを並列に実行できます。複数の並列ストリームでリストア速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

このオプションは、Exchange データベースを元のデータベース名を使用して元の位置にリストアする場合にのみ適用可能です。

高度なオプション
以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
リカバリーが失敗した場合、リストアの一部として、割り振り済みのリソースを自動的にクリーンアップするには、このオプションを有効にします。

7. オプション:「**スクリプトの適用**」ページで、適用する「**事前スクリプト**」または「**事後スクリプト**」を選択するか、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。
   リストア・ジョブが作成され、「**ジョブと操作**」 > 「**実行中のジョブ**」でそのジョブのステータスを確認できます。

高細分度リストア操作を使用した個々のメールボックス項目のリストア

高細分度リストア操作と IBM Spectrum Protect Plus Microsoft 管理コンソール (MMC) GUI を使用して、Microsoft Exchange の個々のメールボックス項目をリストアできます。

始める前に

メールボックスの個別リストア操作を実行するには、役割ベースのアクセス制御 (RBAC) 権限を持っている必要があります。RBAC 権限が割り当てられていない場合は、IBM Spectrum Protect Plus MMC GUI で、欠落している役割のそれぞれについて構成エラーが発生する可能性があります。

ヒント:

IBM Spectrum Protect Plus MMC GUI で役割ベースの構成エラーが発生した場合は、必要な権限を手動で設定してエラーを解決するか (160 ページの『特権』を参照)、IBM Spectrum Protect Plus 構成ウィザードを実行して権限を自動的に構成する (ステップ 179 ページの『14』 を参照) ことができます。

このタスクについて

高細分度リストア操作を開始するには、IBM Spectrum Protect Plus GUI で準備ステップを実行してから、Exchange アプリケーション・サーバーにログインします。次に、IBM Spectrum Protect Plus MMC GUI を使用して、高細分度リストア操作によって作成されるリカバリー・データベースからユーザー・メールボックス・データをリストアします。高細分度リストア操作は、以下のタスクを実行するために使用できます。

- 選択したメールボックス項目を元のメールボックス、同じサーバー上の別のオンライン・メールボックス、あるいは Unicode `.pst` ファイルにリストアできます。
- パブリック・フォルダー・メールボックス・データベース、パブリック・フォルダー・メールボックス、またはメールボックスの一部 (例えば、特定のパブリック・フォルダー) のみをリストアできます。
- アーカイブ・メールボックスまたはメールボックスの一部 (例えば、特定のフォルダー) のみをリストアできます。
- アーカイブ・メールボックスは、Exchange Server 上にあるメールボックス、または Exchange Server の `.pst` ファイルにリストアできます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

- 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Exchange**」をクリックして開くこともできます。
- 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
- ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。

2. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。
   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。

      ヒント: 高細分度リストア操作にデータベースを 1 つのみ選択する必要があります。複数のデータベースを選択すると、高細分度リストア・オプションは、「**リストア方式**」ページで使用できません。

      選択されたソースがデータベース・リストの横にあるリストア・リストに追加されます。リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。
   c) 「**次へ**」をクリックして先に進みます。
3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。

オプション	説明
	リポジトリー・アーカイブ スナップショットがアーカイブされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、「**オリジナル・インスタンスにリストアする**」を選択して、「**次へ**」をクリックします。
5. 「**リストア方式**」ページで、「**高細分度リストア**」をクリックします。
   「**新規データベース名**」フィールドにリカバリー・データベース名が表示されます。 この名前は、既存のデータベース名に接尾部 _RDB が付けられたものです。
6. オプション: 「**ジョブ・オプション**」ページでは、「**バックアップの最後までリカバリーする**」および「**ジョブが失敗したとき、即時にクリーンアップを実行する**」がデフォルトで選択されています。「**次へ**」をクリックして先に進みます。
7. オプション: 「**スクリプトの適用**」ページで、適用する「**事前スクリプト**」または「**事後スクリプト**」を選択するか、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。
   リストア・ジョブが作成され、「**ジョブと操作**」 > 「**実行中のジョブ**」でそのジョブのステータスを確認できます。

10. ナビゲーション・ペインで、「**ジョブと操作**」 > 「**アクティブ・リソース**」をクリックして、リカバリー・データベースとマウント・ポイントの詳細を表示します。

    ヒント: アイコンをクリックして、高細分度リストア・タスクを完了するための次のステップを説明する情報メッセージを表示します。
11. リモート・デスクトップ接続 (RDC) または仮想ネットワーク・コンピューティング (VNC) を使用するか (リモート側から接続している場合)、ローカル側で Exchange Server マシンにログオンして、Exchange アプリケーション・サーバー・インスタンスに接続します。

    高細分度リストア操作により、アプリケーション・サーバーで IBM Spectrum Protect Plus MMC GUI が自動的にインストールされて開始されます。 MMC GUI の開始が失敗する場合は、「**アクティブ・リソース**」情報メッセージに示されているパスを使用して手動で開始します。
12. IBM Spectrum Protect Plus MMC GUI で、「**データの保護およびリカバリー**」ノードをクリックして、「**Exchange Server**」を選択します。
13. Exchange Server インスタンスの「**リカバリー**」タブで、「**表示**」>「**メールボックスのリストア・ブラウザー**」をクリックして、リカバリー・データベースのメールボックスを表示します。
14. オプション: IBM Spectrum Protect Plus 構成ウィザードを実行します。
    a) ナビゲーション・ペインで、「**ダッシュボード**」>「**管理**」>「**構成**」>「**ウィザード**」>「**IBM Spectrum Protect Plus**」 「**構成**」をクリックします。
    b)「**アクション**」ペインで「**開始**」をクリックします。

    構成ウィザードで要件の検査が実行されます。
    c) 要件の検査が実行された後、「**ユーザー役割の検査**」の横にある「**警告**」リンクをクリックします。
    d) メッセージ・ダイアログ・ボックスで、欠落している役割を追加するために、「**はい**」をクリックします。
    e) 構成ウィザードで、「**次へ**」をクリックしてから、「**完了**」をクリックします。
15.「**メールボックスのリストア・ブラウザー**」>「**ソース**」ツリーで、リストアする項目が入ったメールボックスをクリックします。こうすると、個々のフォルダーやメッセージを 参照できます。

    以下のアクションを選択して、リストアするフォルダーやメッセージを 選択します。

表 *19.* メールボックス項目のプレビューおよびフィルタリング

タスク	**アクション**
メールボックス項目をプレビューする	a. プレビュー・ペインに内容を表示するメールボックス項目 (「**受信トレイ**」など) を選択します。 b. プレビュー・ペインで E メール・メッセージなどの個々の項目をクリックして、メッセージ・テキストと詳細を表示します。 c. 項目に添付ファイルがある場合、添付ファイル・アイコンをクリックしてその 内容をプレビューします。

表 19. メールボックス項目のプレビューおよびフィルタリング (続き)	
タスク	**アクション**
メールボックス項目をフィルターに掛ける	フィルター・オプションを使用して、リストアするフォルダーおよびメッセージのリストを絞り込みます。 a.「**フィルター・オプションの表示**」をクリックしてから、「**行の追加**」をクリックします。 b.「**列名**」フィールドの下矢印をクリックして、フィルターに掛ける項目を選択します。 フォルダー名、件名のテキスト、その他のオプションでフィルターに掛けることができます。 **制約事項 :** パブリック・メールボックス・フォルダーは、「**フォルダー名**」列でのみフィルタリングすることができます。 「**すべての内容**」を選択すると、メールボックスの項目は、添付名、送信者、件名、およびメッセージ本文に基づいてフィルターに掛けられます。 c.「**オペレーター**」フィールドで、オペレーター「次の値を含む」を選択します。 d.「**値**」フィールドで、フィルター値を指定します。 e. その他のフィルター基準を指定するには、「**行の追加**」をクリックします。 f.「**フィルターの適用**」をクリックして、メッセージおよびフォルダーをフィルターに 掛けます。

16. リストアするメールボックス項目を選択したら、「**アクション**」ペインで、実行するリストア・タスクをクリックします。以下のオプションから選択します。

    - **オリジナル・メールボックスにフォルダーをリストア**
    - **オリジナル・メールボックスにメッセージをリストア**
    - **メール・メッセージの内容の保存**

    ヒント :「**メール・メッセージの内容の保存**」をクリックすると、 Windows の「ファイルの保存」ウィンドウが表示されます。ロケーションとメッセージの名前を指定して、「**保存**」をクリックします。

    リストア・オプションを選択すると、「**復元の進行状況**」ウィンドウが開き、リストア操作の進行状況が表示され、メールボックス項目がリストアされます。
17. メールボックス項目を別のメールボックスまたは `.pst` ファイルにリストアするには、次のステップを実行します。

    注 : メールボックス全体を別のメールボックスまたは `.pst` ファイルにリストアすることもできます。

    以下の表からアクションを選択してください。

表 *20.* 別のメールボックスまたは *.pst* ファイルへのメールボックス項目のリストア

タスク	**アクション**
メールボックス項目 (またはメールボックス) を別のメールボックスにリストアする	a.「**アクション**」ペインで、「**Exchange メールボックスのオープン**」をクリックします。 b. メールボックスの別名を入力し、それをリストア先として識別します。 c. ソース・メールボックス項目 (またはメールボックス) を結果ペインの宛先メールボックスにドラッグします。 **制約事項 :**「リカバリー可能項目」フォルダー内のメール項目またはサブフォルダーを宛先メールボックスにドラッグすることはできません。
メールボックス項目 (またはメールボックス) を Outlook 個人用フォルダー (.pst) ファイルにリストアする	a.「**アクション**」ペインで、「**非 Unicode PST ファイルのオープン**」をクリックします。 b.「**ファイルを開く**」ウィンドウが開いたら、既存の .pst ファイルを選択するか、.pst ファイルを作成します。 c. ソース・メールボックス項目 (またはメールボックス) を結果ペインの宛先 .pst ファイルにドラッグします。 **制約事項 :**「**メールボックスのリストア・ブラウザー**」ビューは、非 Unicode の .pst ファイルでのみ使用できます。

表 20. 別のメールボックスまたは *.pst* ファイルへのメールボックス項目のリストア (続き)

タスク	アクション
パブリック・フォルダーをリストアする	パブリック・フォルダーを既存のオンライン・パブリック・フォルダー・メールボックスにリストアするには、このアクションを選択します。 メールボックスをフィルタリングし、特定のパブリック・フォルダーを既存のオンライン・パブリック・フォルダーにリストアすることができます。「**リストア対象のフォルダー**」フィールドに、リストアするパブリック・フォルダーの名前を入力します。 • 親フォルダー内のサブフォルダーをリストアするには、*parent_folder_name/sub_folder_name* の形式でフォルダーの絶対パスを指定します。 • 親フォルダー内のすべてのサブフォルダーをリストアするには、*parent_folder_name*/* を使用します。 • フォルダーの絶対パスにスペースが含まれている場合は、フォルダー・パスを二重引用符で囲み、円記号文字 (¥) を付加しないでください。 また、元のメールボックスとは異なるパブリック・フォルダー・メールボックスに、パブリック・フォルダーの全部または一部をリストアすることもできます。「**ターゲット・パブリック・フォルダー・メールボックス**」フィールドに、リストアの宛先となるパブリック・フォルダー・メールボックスを指定します。

18. 「**アクション**」ペインで、「**Exchange メールボックスのクローズ**」または「**PST ファイルのクローズ**」をクリックして、宛先メールボックスまたは .pst ファイルを閉じます。

    ヒント: Microsoft 管理コンソールを有効にして、リストア操作に関連した問題判別に役立つ診断情報を収集できます。このプロセスは、構成ファイル、トレース・ファイル、および MMC GUI の全体的な診断を収集します。詳しくは、以下の技術情報を参照してください。Enabling diagnostic information in the IBM Spectrum Protect Plus MMC GUI(http://www.ibm.com/support/docview.wss?uid=ibm10882270)。
19. 個々の項目のリストア操作が完了したら、IBM Spectrum Protect Plus に戻ります。「**ジョブと操作**」> 「**アクティブ・リソース**」ペインで、「**アクション**」 > 「**高細分度リストアのキャンセル**」をクリックして高細分度リストア・プロセスを終了します。

高細分度リストア操作を使用したメールボックスのリストア

高細分度リストア操作と IBM Spectrum Protect Plus Microsoft 管理コンソール (MMC) GUI を使用して、Microsoft Exchange のメールボックスをリストアできます。

始める前に

メールボックスの個別リストア操作を実行するには、役割ベースのアクセス制御 (RBAC) 権限を持っている必要があります。RBAC 権限が割り当てられていない場合は、IBM Spectrum Protect Plus MMC GUI で、欠落している役割のそれぞれについて構成エラーが発生する可能性があります。

ヒント:

IBM Spectrum Protect Plus MMC GUI で役割ベースの構成エラーが発生した場合は、必要な権限を手動で設定してエラーを解決するか (160 ページの『特権』を参照)、IBM Spectrum Protect Plus 構成ウィザードを実行して権限を自動的に構成する (ステップ 185 ページの『14』 を参照) ことができます。

このタスクについて

高細分度リストア操作を開始するには、IBM Spectrum Protect Plus GUI で準備ステップを実行してから、Exchange アプリケーション・サーバーにログインします。次に、IBM Spectrum Protect Plus MMC GUI を使用して、高細分度リストア操作によって作成されるリカバリー・データベースからユーザー・メールボックス・データリストアします。高細分度リストア操作は、以下のタスクを実行するために使用できます。

- メールボックス全体、または選択したメールボックス項目を元のメールボックス、同じサーバー上の別のオンライン・メールボックス、あるいは Unicode `.pst` ファイルにリストアできます。
- パブリック・フォルダー・メールボックス・データベース、パブリック・フォルダー・メールボックス、またはメールボックスの一部 (例えば、特定のパブリック・フォルダー) のみをリストアできます。
- アーカイブ・メールボックスまたはメールボックスの一部 (例えば、特定のフォルダー) のみをリストアできます。
- アーカイブ・メールボックスは、Exchange Server 上にあるメールボックス、または Exchange Server の `.pst` ファイルにリストアできます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Exchange**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。
2. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。

   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。

   ヒント: 高細分度リストア操作にデータベースを 1 つのみ選択する必要があります。複数のデータベースを選択すると、高細分度リストア・オプションは、「**リストア方式**」ページで使用できません。

   選択されたソースがデータベース・リストの横にあるリストア・リストに追加されます。リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。

   c) 「**次へ**」をクリックして先に進みます。
3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。

オプション	説明
	繰り返し スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、「**オリジナル・インスタンスにリストアする**」を選択して、「**次へ**」をクリックします。
5. 「**リストア方式**」ページで、「**高細分度リストア**」をクリックします。

   「**新規データベース名**」フィールドにリカバリー・データベース名が表示されます。 この名前は、既存のデータベース名に接尾部 _RDB が付けられたものです。
6. オプション: 「**ジョブ・オプション**」ページでは、「**バックアップの最後までリカバリーする**」および「**ジョブが失敗したとき、即時にクリーンアップを実行する**」がデフォルトで選択されています。「**次へ**」をクリックして先に進みます。
7. オプション: 「**スクリプトの適用**」ページで、適用する「**事前スクリプト**」または「**事後スクリプト**」を選択するか、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。

   リストア・ジョブが作成され、「**ジョブと操作**」 > 「**実行中のジョブ**」でそのジョブのステータスを確認できます。
10. ナビゲーション・ペインで、「**ジョブと操作**」 > 「**アクティブ・リソース**」をクリックして、リカバリー・データベースとマウント・ポイントの詳細を表示します。

    ヒント: アイコンをクリックして、高細分度リストア・タスクを完了するための次のステップを説明する情報メッセージを表示します。
11. リモート・デスクトップ接続 (RDC) または仮想ネットワーク・コンピューティング (VNC) を使用するか (リモート側から接続している場合)、ローカル側で Exchange Server マシンにログオンして、Exchange アプリケーション・サーバー・インスタンスに接続します。

    高細分度リストア操作により、アプリケーション・サーバーで IBM Spectrum Protect Plus MMC GUI が自動的にインストールされて開始されます。 MMC GUI の開始が失敗する場合は、「**アクティブ・リソース**」情報メッセージに示されているパスを使用して手動で開始します。
12. IBM Spectrum Protect Plus MMC GUI で、「**データの保護およびリカバリー**」ノードをクリックして、「**Exchange Server**」を選択します。
13. Exchange Server インスタンスの「**リカバリー**」タブで、「**表示**」>「**メールボックスのリストア**」を選択します。

    バックアップに含まれているすべてのデータベースのユーザー・メールボックスのリストが表示されます。
14. オプション: IBM Spectrum Protect Plus 構成ウィザードを実行します。
    a) ナビゲーション・ペインで、「**ダッシュボード**」>「**管理**」>「**構成**」>「**ウィザード**」>「**IBM Spectrum Protect Plus**」 「**構成**」をクリックします。
    b) 「**アクション**」ペインで「**開始**」をクリックします。

    構成ウィザードで要件の検査が実行されます。
    c) 要件の検査が実行された後、「**ユーザー役割の検査**」の横にある「**警告**」リンクをクリックします。
    d) メッセージ・ダイアログ・ボックスで、欠落している役割を追加するために、「**はい**」をクリックします。
    e) 構成ウィザードで、「**次へ**」をクリックしてから、「**完了**」をクリックします。
15. リカバリー・データベースからリストアするメールボックスを 1 つ以上選択します。メールボックスは、メールボックス名、別名、サーバー、データベース、およびメールボックス・タイプ別にリストされます。

    リカバリー・データベース内にあるユーザー・メールボックスのみをリストアできます。

    ヒント: このビューでは、他のデータベースのメールボックスは情報提供のみを目的として表示されます。リストアしたいメールボックスがリカバリー・データベース内にない場合は、このビューを使用

して、ユーザー・メールボックスがどの Exchange データベースに割り当てられていたかを判別します。その後、そのデータベースに対して高細分度リストア・タスクを再び実行できます。

16. リストア操作を実行するには、「**アクション**」ペインで以下のいずれかのリストア・オプションをクリックします。

表 *21.* リストア・オプション

オプション	**アクション**
メールをオリジナル・ロケーションにリストア	メール項目をバックアップ操作時のロケーションにリストアします。
代替ロケーションにメールをリストア	メール項目を別のメールボックスにリストアします。 • 「**代替メールボックスのオプション**」ウィンドウで「**メールボックスの別名**」に名前を入力します。 **ヒント :** 削除されたメール項目またはタスクには、メールボックスの「リカバリー可能項目」フォルダーでフラグが立てられ、それらの項目は、フラグ属性を使用してターゲット・メールボックス内の「**フラグ付きの項目およびタスク (Flagged Items and Tasks)**」ビューにリストアされます。
非 Unicode の PST ファイルにメールをリストア **制約事項 :** • このオプションは、Exchange Server 2013 でのみ使用できます。 • 各フォルダーには、最大 16,383 個のメール項目を含めることができます。	メール項目を非 Unicode 個人用フォルダー (.pst) ファイルにリストアする 1 つのメールボックスを選択して、メール項目を .pst ファイルにリストアする場合、ファイル名の指定を求めるプロンプトが出されます。複数のメールボックスを選択して、メール項目を .pst ファイルにリストアする場合、ディレクトリーのロケーションの指定を求めるプロンプトが表示されます。各メールボックスは、指定されたディレクトリーにあるメールボックスの名前を示す別々の .pst ファイルにリストアされます。 .pst ファイルが存在する場合、そのファイルが使用されます。存在しない場合は、ファイルが作成されます。

表 *21.* リストア・オプション *(*続き*)*

オプション	アクション
Unicode の PST ファイルにメールをリストア	メール項目を Unicode の .pst ファイルにリストアする 1 つのメールボックスを選択して、メール項目を .pst ファイルにリストアする場合、ファイル名の指定を求めるプロンプトが出されます。複数のメールボックスを選択して、メール項目を .pst ファイルにリストアする場合、ディレクトリーのロケーションの指定を求めるプロンプトが表示されます。 **ヒント:** 標準のパス名 (例えば、c:¥PST¥mailbox.pst) または UNC パス (例えば、¥¥server¥c$¥PST ¥mailbox.pst) を入力できます。標準のパスを入力すると、そのパスは UNC パスに変換されます。UNC がデフォルト以外の UNC パスである場合、その UNC パスを直接入力します。 各メールボックスは、指定されたディレクトリーにあるメールボックスの名前を示す別々の .pst ファイルにリストアされます。.pst ファイルが存在する場合、そのファイルが使用されます。存在しない場合は、ファイルが作成されます。
パブリック・フォルダー・メールボックスのリストア	パブリック・フォルダー・メールボックスをオンライン・パブリック・フォルダー・メールボックスにリストアします。 「**リストア対象のフォルダー**」フィールドに、リストアするパブリック・フォルダーの名前を入力します。 • 親フォルダー内のサブフォルダーをリストアするには、*parent_folder_name*/*sub_folder_name* の形式でフォルダーの絶対パスを指定します。 • 親フォルダー内のすべてのサブフォルダーをリストアするには、*parent_folder_name*/* を使用します。 • フォルダーの絶対パスにスペースが含まれている場合は、フォルダー・パスを二重引用符で囲み、円記号文字 (¥) を付加しないでください。 また、元のメールボックスとは異なるパブリック・フォルダー・メールボックスに、パブリック・フォルダー・メールボックスの全部または一部をリストアすることもできます。「**ターゲット・パブリック・フォルダー・メールボックス**」フィールドに、宛先となるパブリック・フォルダー・メールボックスを指定します。

表 21. リストア・オプション (続き)

オプション	アクション
アーカイブ・メールボックスへのメールのリストア	このアクションは、1 次メールボックスまたはアーカイブ・メールボックスに適用されます。これらのタイプのメールボックスの全部または一部を、元のアーカイブ・メールボックスまたは代替アーカイブ・メールボックスにリストアするには、このアクションを選択します。 アーカイブ・メールボックスをフィルタリングし、特定のメールボックス・フォルダーをリストアすることができます。「**リストア対象のフォルダー**」フィールドに、リストアするアーカイブ・メールボックス内のフォルダー名を入力します。 • 親フォルダー内のサブフォルダーをリストアするには、*parent_folder_name*/*sub_folder_name* の形式でフォルダーの絶対パスを指定します。 • 親フォルダー内のすべてのサブフォルダーをリストアするには、*parent_folder_name*/* を使用します。 • フォルダーの絶対パスにスペースが含まれている場合は、フォルダー・パスを二重引用符で囲み、円記号文字 (¥) を付加しないでください。 「**ターゲット・アーカイブ・メールボックス**」フィールドで、宛先となるアーカイブ・メールボックスを指定します。
メールボックスのリストア時にリカバリー可能なメール項目を除外します	オンラインのパブリック・フォルダーまたはアーカイブ・メールボックスを元のメールボックス、代替メールボックス、あるいは Unicode `.pst` ファイルにリストアする場合に、このアクションを適用します。 メールボックスのリストア操作で「リカバリー可能項目」フォルダー内のメール項目を除外するには、値「**はい**」を指定します。 デフォルト値は「**いいえ**」です。

ヒント: Microsoft 管理コンソールを有効にして、リストア操作に関連した問題判別に役立つ診断情報を収集できます。このプロセスは、構成ファイル、トレース・ファイル、および MMC GUI の全体的な診断を収集します。詳しくは、以下の技術情報を参照してください。Enabling diagnostic information in the IBM Spectrum Protect Plus MMC GUI(http://www.ibm.com/support/docview.wss?uid=ibm10882270)。

17. メールボックスのリストア操作が完了したら、IBM Spectrum Protect Plus に戻ります。「**ジョブと操作**」 > 「**アクティブ・リソース**」ペインで、「**アクション**」 > 「**高細分度リストアのキャンセル**」をクリックして高細分度リストア・プロセスを終了します。

データベース可用性グループ・バックアップのリストア

IBM Spectrum Protect Plus では、 Exchange Server データベース可用性グループ (DAG) バックアップをオリジナル・インスタンスまたは代替インスタンスにリストアできます。

このタスクについて

DAG 環境では、アクティブ・データベース・コピーにデータベースをリストアする 必要があります。バックアップ操作の優先ターゲットとしてパッシブ・データベース・コピーを選択した場合は、IBM Spectrum Protect Plus は、デフォルトで、このパッシブ・コピーにデータベースをリストアしようとします。リストア操作は失敗します。この状態では、代替インスタンスにデータベースをリストアして、アクティブ・データベース・コピーを選択することができます。

手順

Exchange リストア・ジョブを定義するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント：

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Exchange**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。
2. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) 「**表示**」メニューをクリックして、「**データベース可用性グループ**」を選択します。
   b) 「**可用性グループ**」リストで、Exchange インスタンスをクリックして、そのインスタンスのリストア・ポイントを表示し、リストアするバックアップ・バージョンを選択します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。
   c) リストア操作のソースとして使用するデータベースの横にある「リストア・リストに追加」アイコン をクリックします。複数のデータベースをリストから選択できます。

   選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リスト・ソースから項目を削除するには、項目の隣にある アイコンをクリックします。
   d) 「**次へ**」をクリックして先に進みます。
3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。

オプション	説明
	クラウド・アーカイブ スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定 (Set destination)**」ページで、データベースをリストアする場所を指定して「**次へ**」をクリックします。

   オリジナル・インスタンスにリストアします
   元のサーバーにデータベースをリストアするには、このオプションを選択します。

   代替インスタンスにリストアします
   オリジナルのサーバーとは別のローカル宛先にデータベースをリストアする場合にこのオプションを選択します。その後、使用可能なサーバーのリストから代替ロケーションを選択します。

   重要 : 宛先を選択する際、宛先としてアクティブ・ノードを選択する必要があります。そうしないと、リストア操作は失敗します。

5. 「**リストア方式**」ページで、以下のオプションから選択します。

   - **テスト**。vSnap リポジトリーから直接、データをリストアする場合、このオプションを選択します。このリストア・タイプは、テストの目的で使用できます。
   - **実動**。フルコピー・データ・リストア操作でデータベース全体をリストアする場合、このオプションを選択します。このリストア操作は、リストアされたデータベースを永続的に使用するために実行します。

「**次へ**」をクリックして先に進みます。

6. オプション:「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   リカバリー・オプション
   以下のリカバリー・オプションから選択します。

   リカバリーなし
   このオプションでは、リストア操作後のロールフォワード・リカバリーがスキップされます。ロールフォワード・リカバリーを手動で実行するかどうかを決定するまで、データベースはロールフォワード保留状態のままになります。

   バックアップの最後までリカバリーします
   選択済みデータベースをリストアして、バックアップの作成時の状態に戻します。

   使用可能なログの最後までリカバリーします
   このオプションでは、データベースがリストアされ、すべての使用可能なログ (アプリケーション・サーバー上に存在する可能性があるバックアップよりも新しいログを含む) が適用され、可能な限り最新の時点までデータベースがリカバリーされます。このオプションは、バックアップ・ジョブで「**ログ・バックアップを有効にする**」を選択している場合にのみ使用できます。

   特定時点までリカバリーします
   ログ・バックアップが使用可能な場合、このオプションでは、データベースがリストアされ、ログ・バックアップ・ボリュームのログが適用され、ユーザーが指定する中間の特定時点までデータベースがリカバリーされます。日時を「**時刻別**」オプションから選択します。

   アプリケーション・オプション
   以下のアプリケーション・オプションを設定します。

   データベースごとの最大並列ストリーム数
   バックアップ・ストレージからのデータベースごとの最大データ・ストリームを設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を 1 に設定すると、複数のデータベースのリストアを並列に実行できます。複数の並列ストリームでリストア速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

   このオプションは、Exchange データベースを元のデータベース名を使用して元の位置にリストアする場合にのみ適用可能です。

   高度なオプション
   以下の高度なジョブ定義オプションを設定します。

   ジョブが失敗したとき、即時にクリーンアップを実行します
   リカバリーが失敗した場合、リストアの一部として、割り振り済みのリソースを自動的にクリーンアップするには、このオプションを有効にします。

7. オプション:「**スクリプトの適用**」ページで、適用する「**事前スクリプト**」または「**事後スクリプト**」を選択するか、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。
   リストア・ジョブが作成され、「**ジョブと操作**」 > 「**実行中のジョブ**」でそのジョブのステータスを確認できます。

インスタンス・アクセス・モードを使用した Exchange データベース・ファイルへのアクセス

インスタント・アクセス・リストア・タイプを使用して Microsoft Exchange データベース・ファイルにアクセスし、データベース・ファイルを vSnap ボリュームからアプリケーション・サーバーにマウントすることができます。

このタスクについて

インスタント・アクセス・モードでは、IBM Spectrum Protect Plus が共有をマウントした後、それ以上のアクションは実行されません。vSnap ボリュームのファイルからのデータのカスタム・リカバリーにデータを使用します。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Exchange**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Exchange**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。

2. 「**ソースの選択**」ページで、以下のステップを実行します。

   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。

   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。複数のデータベースをリストから選択できます。

   選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。

   c) 「**次へ**」をクリックして先に進みます。

3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。

オプション	説明
	クラウド・オフロード スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする 場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア 元のデモンストレーション・サイト。 **1 次** スナップショットのリストア 元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア 元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする 場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを 表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする 場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、データベース・ファイルをマウントする場所を指定して、「**次へ**」をクリックします。

オプション	説明
元の位置にリストアする	オリジナル・サーバーにデータベース・ファイルをマウントする場合に、このオプションを選択します。

オプション	説明
代替の位置にリストアする	オリジナル・サーバーとは異なるローカル宛先にデータベース・ファイルをマウントするには、このオプションを選択します。その後、使用可能なサーバーのリストから代替ロケーションを選択します。

5. 「**リストア方式**」ページで、「**インスタント・アクセス**」を選択して、「**次へ**」をクリックします。
6. オプション: 「**ジョブ・オプション**」ページで、必要に応じて他のオプションを構成し、「**次へ**」をクリックして先に進みます。
7. オプション: 「**スクリプトの適用**」ページで、適用する「**事前スクリプト**」または「**事後スクリプト**」を選択するか、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。スクリプトの処理について詳しくは、スクリプトの構成を参照してください。「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。
   リストア・ジョブが作成され、「**ジョブと操作**」 > 「**実行中のジョブ**」でそのジョブのステータスを確認できます。
10. これで、アプリケーション・サーバーのマウント・ポイント上の Exchange データベース・ファイルにアクセスして、実行したいすべての Exchange 関連アクションまたはカスタム・アクションを実行できるようになりました。

    注 : マウント・ポイント上の Exchange データベース・ファイルは読み取り/書き込みファイルです。ただし、それらを更新しても、オリジナルのバックアップは変更されません。
11. インスタンス・アクセス・リストア操作を終了したら、「**アクティブ・リソース**」ペインに進み、「**アクション**」 > 「**リストアのキャンセル**」をクリックして、マウントされたデータベースを削除し、リストア・プロセスを終了します。

MongoDB

MongoDB インスタンスを IBM Spectrum Protect Plus に正常に追加した後、MongoDB データベース内のデータの保護を開始できます。MongoDB データをバックアップして保守するための SLA ポリシーを作成します。

ご使用の MongoDB 環境がシステム要件を満たしていることを確認します。詳しくは、32 ページの『MongoDB の要件』を参照してください。

MongoDB の前提条件

IBM Spectrum Protect Plus を使用して MongoDB データの保護を開始する前に、IBM Spectrum Protect Plus MongoDB アプリケーション・サーバー のシステム要件と前提条件がすべて満たされていなければなりません。

MongoDB システム要件については、MongoDB システム要件を参照してください。

MongoDB の前提条件を満たすには、以下の検査とアクションを実行してください。

1. MongoDB 保護のためのスペース所要量で説明されているとおり、スペースの前提条件を満たしていることを確認します。
2. command **ulimit** -f コマンドを使用して MongoDB インスタンス・ユーザーのファイル・サイズ制限を unlimited に設定します。または、この値を、バックアップ・ジョブやリストア・ジョブ内で最大のデータベース・ファイルのコピーを可能にする十分大きい値に設定します。**ulimit** 設定を変更する場合は、MongoDB インスタンスを再始動して、構成を完了します。
3. AIX 環境または Linux 環境で MongoDB を実行している場合、インストールされている sudo バージョンが、サポートされているレベルであることを確認します。

バージョン・レベルについて詳しくは、32 ページの『MongoDB の要件』を参照してください。sudo 特権の設定については、197 ページの『sudo 特権の設定』を参照してください。

4. MongoDB データベースが認証によって保護されている場合、役割ベースのアクセス制御をセットアップする必要があります。詳しくは、195 ページの『MongoDB 用の役割』を参照してください。
5. 保護される各 MongoDB インスタンスは、IBM Spectrum Protect Plus で登録されなければなりません。インスタンスが登録されたら、IBM Spectrum Protect Plus はインベントリーを実行して、MongoDB リソースを検出します。保護したいすべてのインスタンスが検出され、正しくリストされていることを確認してください。
6. SSH サービスがサーバー上のポート 22 で実行中であること、および IBM Spectrum Protect Plus が SSH を使用してサーバーに接続できるようにファイアウォールが構成されていることを確認します。SSH の SFTP サブシステムが使用可能でなければなりません。
7. ネストされたマウント・ポイントを構成しないようにします。

制約事項

MongoDB アプリケーション・サーバーには以下の制約事項が適用されます。

- インベントリーの実行時に MongoDB sharded クラスター構成が検出されますが、これらのリソースはバックアップ操作にもリストア操作にも適格ではありません。
- MongoDB ファイル・パス名内の Unicode 文字を IBM Spectrum Protect Plus は処理できません。すべての名前は ASCII でなければなりません。

仮想化

以下のいずれかのゲスト・オペレーティング・システムで実行されている場合、IBM Spectrum Protect Plus を使用して MongoDB 環境を保護します。

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server Kernel-based Virtual Machine (KVM)

MongoDB 用の役割

MongoDB データベースで認証が有効になっている場合、MongoDB エージェント・ユーザーに対して役割ベースのアクセス制御 (RBAC) 役割を定義する必要があります。役割がセットアップされたら、ユーザーは、ユーザーに定義されている役割に従って、IBM Spectrum Protect Plus で MongoDB リソースを保護し、モニターすることができます。

MongoDB 向けの役割ベースのアクセス制御

MongoDB ユーザーごとに、次の例のようなコマンドを使用してアクセス役割を指定します。

```
use admin
db.grantRolesToUser("<username>",
[ { role: "hostManager", db: "admin" },
{ role: "clusterManager", db: "admin" } ] )
```

使用可能な役割は次のとおりです。

hostManager
この役割では、**fsyncLock** コマンドにアクセスできます。このアクセス権は、ジャーナル処理が有効になっていない MongoDB データベースのアプリケーション整合性バックアップに必要です。また、この役割では、シャットダウン・コマンドにもアクセスできます。このコマンドは、リストアが送信される先の MongoDB サーバー・インスタンスをシャットダウンするために、リストア操作時に使用されます。

clusterMonitor
この役割では、MongoDB データベースの状態をモニターし、読み取るためのコマンドにアクセスできます。この役割を持つユーザーから、次のコマンドが使用できます。

- **getCmdLineOpts**

- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

clusterManager
この役割が必要なのは、レプリカ・セットのテスト・リストア操作を実行する場合のみです。**replSetReconfig** コマンドを実行するユーザーは、単一のノード・レプリカ・セットのリストアされたインスタンスを作成できます。この役割では、レプリカ・セットのテスト・リストア操作時に読み取りおよび書き込みアクセスが可能になります。このアクセス権がないと、レプリカ・セット内のノードは、読み取りと書き込みアクセスがない REMOVED 状態のままになります。さらに、この役割では、MongoDB データベースの状態を読み取るためのコマンドにもアクセスできます。この役割には以下のコマンドが使用できます。

- **replSetReconfig**
- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

MongoDB 保護のためのスペース 前提条件
MongoDB データのバックアップを開始する前に、ターゲット・ホストとソース・ホスト上、および vSnap リポジトリーに十分なフリー・スペースがあることを確認してください。MongoDB データが置かれている論理ボリュームの一時論理ボリューム・マネージャー (LVM) バックアップの保管に、追加のスペースが必要です。LVM スナップショットと呼ばれるこれらの一時バックアップは、MongoDB エージェントによって自動的に作成されます。

LVM スナップショット

LVM スナップショットは、LVM 論理ボリュームの特定時点コピーです。ファイル・コピー操作が終了したら、以前の LVM スナップショットは、クリーンアップ操作で IBM Spectrum Protect Plus MongoDB エージェントによって削除されます。

LVM スナップショット論理ボリュームごとに、ボリューム・グループ内で 10% 以上のフリー・スペースを割り振る必要があります。ボリューム・グループに十分なフリー・スペースがある場合、IBM Spectrum Protect Plus MongoDB エージェントは、スナップショット論理ボリューム用にソース論理ボリューム・サイズの最大 25% を予約します。

Linux LVM2
MongoDB バックアップ操作を実行すると、MongoDB がスナップショットを要求します。このスナップショットは、選択されたデータベースのデータまたはログがある論理ボリュームごとに、論理ボリューム管理 (LVM) システムで作成されます。Linux システムでは、論理ボリュームは、LVM2 によって管理されます。

ソフトウェア・ベースの LVM2 スナップショットは、同じボリューム・グループの新規論理ボリュームとして取られます。 これらのスナップショット・ボリュームは、MongoDB インスタンスを実行するのと同じマシンに一時的にマウントされるので、vSnap リポジトリーに転送できます。

Linux では、LVM2 ボリューム・マネージャーが、論理ボリュームのスナップショットを同じボリューム・グループに保管します。論理ボリュームの保管に使用できる十分なスペースが必要です。スナップショットの存続期間中、データがソース・ボリューム上で変更されるにつれて、論理ボリュームのサイズが大きくなります。

sudo 特権の設定

IBM Spectrum Protect Plus を使用してデータを保護するには、必要なバージョンの sudo プログラムをインストールする必要があります。

このタスクについて

sudo に必要なスーパーユーザー特権を持つ専用の IBM Spectrum Protect Plus エージェント・ユーザーをセットアップします。この構成により、エージェント・ユーザーはパスワードを使用せずにコマンドを実行できるようになります。

手順

1. 次のコマンドを実行して、エージェント・ユーザーを作成します。

   ```
   useradd -m agent
   ```

   ここで、*agent* には、IBM Spectrum Protect Plus エージェント・ユーザーの名前を指定します。
2. 次のコマンドを実行して、新規ユーザーのパスワードを設定します。

   ```
   passwd mongodb_agent
   ```
3. エージェント・ユーザーに対してスーパーユーザー特権を有効にするには、`!requiretty` を設定します。sudo 構成ファイルの末尾に以下の行を追加します。

   ```
   Defaults:agent !requiretty
   agent ALL=(ALL) NOPASSWD:ALL
   ```

   あるいは、sudoers ファイルが別のディレクトリー (例えば、`/etc/sudoers.d`) から構成をインポートするように構成されている場合は、そのディレクトリー内の適切なファイルにこの行を追加できます。

MongoDB アプリケーション・サーバーの追加

MongoDB リソースの保護を開始するには、MongoDB インスタンスをホストするサーバーを追加して、インスタンスの資格情報を設定する必要があります。 MongoDB リソースをホストするすべてのサーバーを追加するために、この手順を繰り返します。

このタスクについて

MongoDB アプリケーション・サーバーを IBM Spectrum Protect Plus に追加するにはマシンのホスト・アドレスが必要です。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」を展開します。
2. 「**MongoDB**」ウィンドウで、「**アプリケーション・サーバーの管理**」をクリックして、「**アプリケーション・サーバーの追加**」をクリックし、ホスト・マシンを追加します。

3. 「**アプリケーション・プロパティー**」フォームにホスト・アドレスを入力します。
4. ユーザーまたは SSH 鍵のどちらでホストを登録するかを選択します。

   「**ユーザー**」を選択する場合は、新規のユーザーとパスワードまたは既存のユーザーのどちらでも入力できます。「**SSH 鍵**」を選択する場合は、メニューから SSH 鍵を選択します。

   制約事項 : 指定するユーザーには、sudo 特権がセットアップされている必要があります。

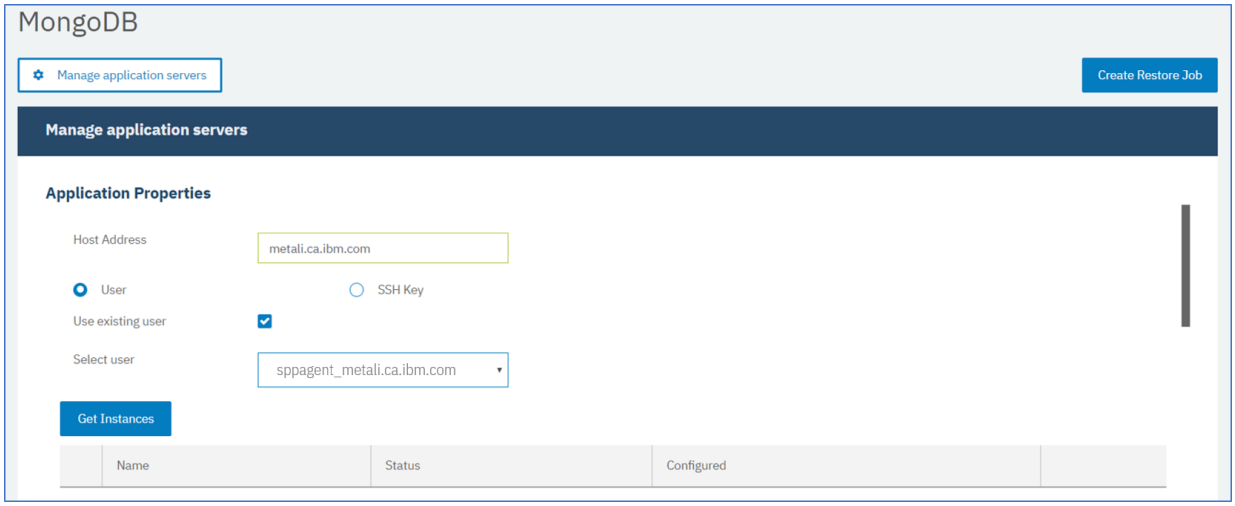


図 *25. MongoDB* エージェントの追加

5. 「**インスタンスの取得**」をクリックし、追加するホスト・サーバーで使用可能な MongoDB インスタンスを検出してリストします。

   各 MongoDB インスタンスは、接続ホスト・アドレス、状況、および構成済みであるかどうかの標識と共にリストされます。

   重要 : 1 つのレプリカ・セットについて複数のアプリケーション・サーバーを登録する場合、表示されるインスタンス名は、インベントリー、バックアップ、またはリストアの操作が行われるたびに変わる可能性があります。そのレプリカ・セットに属している、最近追加されたアプリケーション・サーバーのホスト名がインスタンス名の一部として使用されます。インベントリー操作は、バックアップ操作およびリストア操作の一部として実行されます。

6. アクセス制御を使用している場合は、資格情報を設定してインスタンスを構成します。「**資格情報を設定**」をクリックして、ユーザー ID とパスワードを設定します。あるいは、既存のユーザー・プロファイルを使用することもできます。

   アクセス制御について詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。

   資格情報を設定する際、Salted Challenge Response Authentication Mechanism (SCRAM) またはチャレンジ応答認証を使用して、役割によって保護された MongoDB サーバーに対するアクセス権限を、バックアップとリストアの操作のために MongoDB ユーザー役割に割り当てます。役割によって保護された MongoDB サーバーに割り当てられた MongoDB ユーザーには、リソースを保護するために以下のいずれかのアクセス・レベルが必要です。

   - ホスト・マネージャー: 管理者としてデータベースを管理します。この役割は、スナップショットを取って管理するために必要です。
   - クラスター管理者: 構成情報を取得して、MongoDB レプリカ・セットのテスト・モードのリストア操作を実行します。この役割は、データ照会のために MongoDB レプリカ・セットのテスト・モードのリストア操作を再構成するために必要です。
   - クラスター・モニター: MongoDB リソースの保護をモニターして、構成情報を取得します。

7. オプション: オプションの「**最大同時データベース数**」で、フィールドに数字を入力して設定します。
8. フォームを保存して、上記のステップを繰り返し、他の MongoDB アプリケーション・サーバーを IBM Spectrum Protect Plus に追加します。

次のタスク

MongoDB アプリケーション・サーバーを IBM Spectrum Protect Plus に追加した後、各アプリケーション・サーバーでインベントリーが自動的に実行され、それらのインスタンス内の関連データベースが検出されます。

データベースが追加されたことを確認するには、ジョブ・ログを調べてください。「**ジョブと操作**」に進みます。「**実行中のジョブ**」タブをクリックして、最新のアプリケーション・サーバー・インベントリー・ログ項目を見つけます。

完了したジョブは「**ジョブ・ヒストリー**」タブに表示されます。「**ソート順**」リストを使用して、開始時刻、タイプ、状況、ジョブ名、または所要時間に基づいてジョブをソートすることができます。ジョブを名前で検索するには、「**名前での検索**」フィールドを使用します。名前ではワイルドカードとしてアスタリスクを使用できます。

データベースを確実に保護できるようにするには、データベースが検出されている必要があります。手動でインベントリーを実行する手順については、MongoDB リソースの検出を参照してください。

MongoDB リソースの検出

MongoDB アプリケーション・サーバーを IBM Spectrum Protect Plus に追加した後、インベントリーが自動的に実行され、MongoDB インスタンスおよびデータベースがすべて検出されます。選択したホストのすべての MongoDB データベースの検出、リスト、および保管を行うために、任意のアプリケーション・サーバーでインベントリーを手動で実行できます。

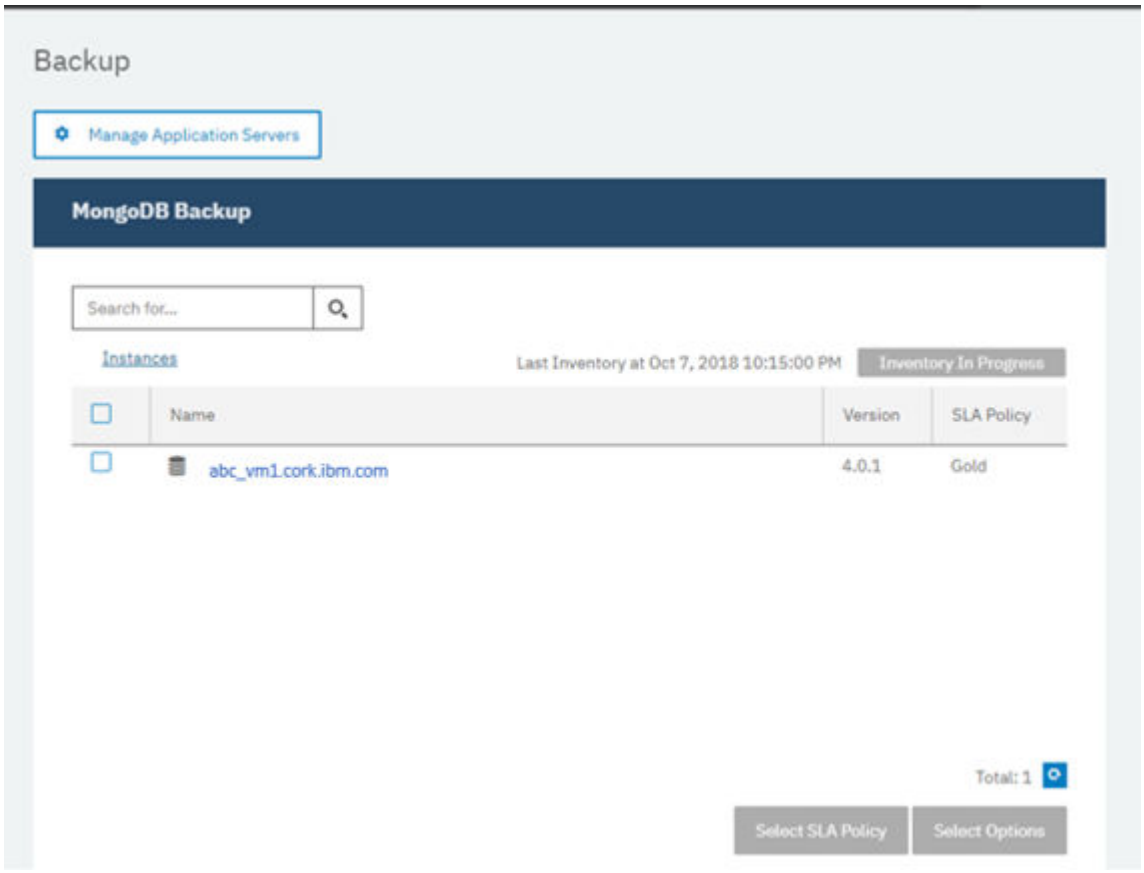
始める前に

MongoDB アプリケーション・サーバーを IBM Spectrum Protect Plus に追加したことを確認してください。手順については、MongoDB アプリケーション・サーバーの追加を参照してください。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」を展開します。

   ヒント: さらに多くの MongoDB インスタンスを「**インスタンス**」ペインに追加するには、MongoDB アプリケーション・サーバーの追加の手順に従ってください。
2. 「**インベントリーの実行**」をクリックします。



インベントリーの実行中、ボタンが「**インベントリーが進行中**」に変わります。任意の使用可能なアプリケーション・サーバーでインベントリーを実行できますが、インベントリー・プロセスは一度に 1 つしか実行できません。

インベントリー・ジョブをモニターするには、「**ジョブと操作**」に進みます。「**実行中のジョブ**」タブをクリックして、最新のアプリケーション・サーバー・インベントリー・ログ項目を見つけます。

完了したジョブは「**ジョブ・ヒストリー**」タブに表示されます。「**ソート順**」リストを使用して、開始時刻、タイプ、状況、ジョブ名、または所要時間に基づいてジョブをソートすることができます。ジョブを名前で検索するには、「**名前での検索**」フィールドを使用します。名前ではワイルドカード文字としてアスタリスクを使用できます。

3. インスタンスをクリックして、そのインスタンスで検出されたデータベースを示すビューを開きます。「**インスタンス**」リストでデータベースが欠落している場合は、MongoDB アプリケーション・サーバーを確認して、インベントリーを再実行します。場合によっては、特定のデータベースにバックアップに適格ではないというマークが付けられていることがあります。そのデータベースの上にカーソルを移動して理由を調べてください。

   ヒント : インスタンスのリストに戻るには、「**MongoDB のバックアップ**」ペインの「**インスタンス**」リンクをクリックします。

   重要 : 1 つのレプリカ・セットについて複数のアプリケーション・サーバーを登録する場合、表示されるインスタンス名は、インベントリー、バックアップ、またはリストアの操作が行われるたびに変わる可能性があります。そのレプリカ・セットに属している、最近インベントリーが実行されたアプリケーション・サーバーのホスト名がインスタンス名の一部として使用されます。インベントリー操作は、バックアップ操作およびリストア操作の一部として実行されます。

次のタスク

選択したインスタンスでカタログされている MongoDB データベースの保護を開始するには、SLA ポリシーをインスタンスに適用します。 SLA ポリシーの設定手順については、SLA バックアップ・ジョブの定義を参照してください。

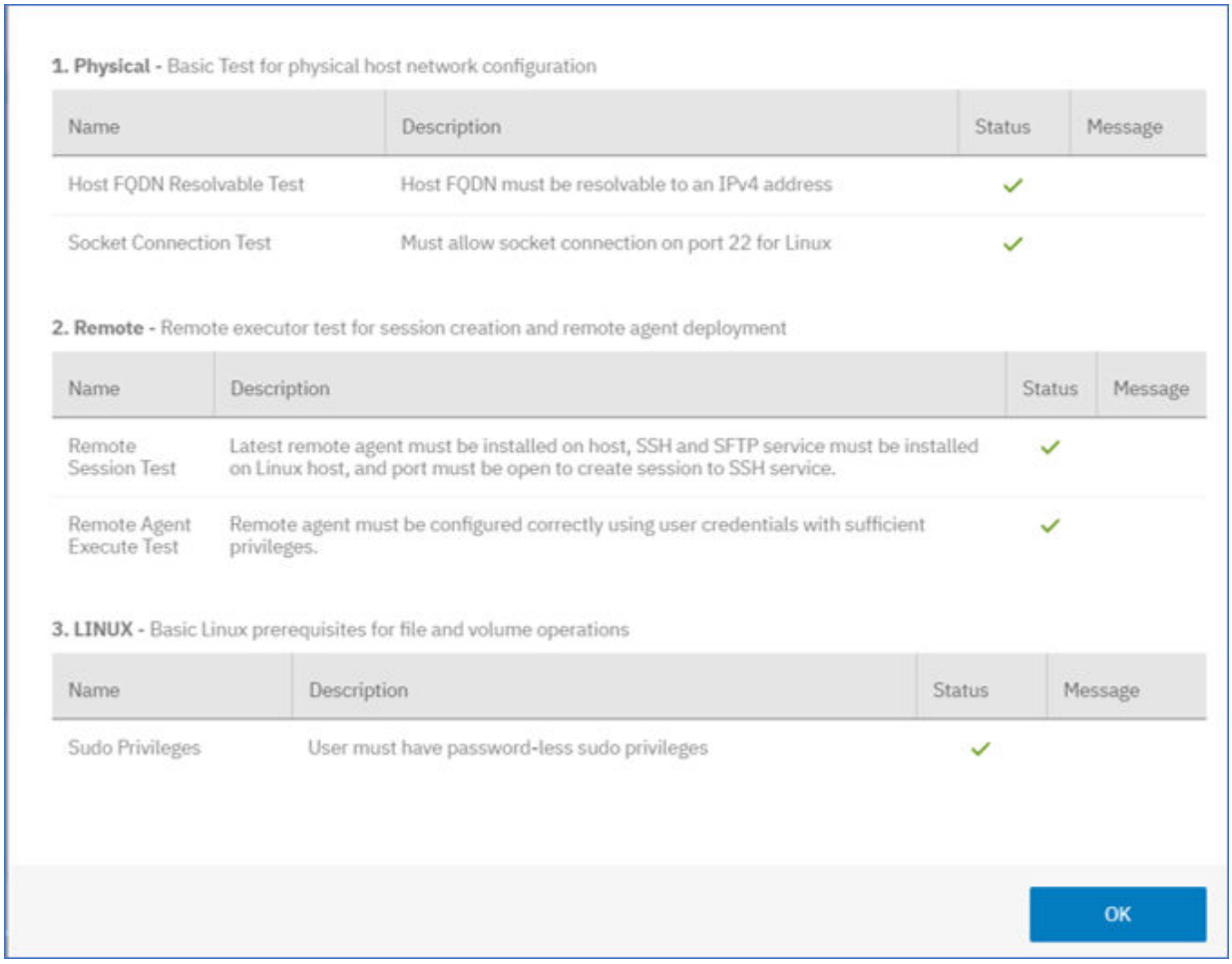
MongoDB 接続のテスト

MongoDB アプリケーション・サーバーを追加した後、接続をテストできます。このテストでは、IBM Spectrum Protect Plus と MongoDB サーバーの間の通信が検査されます。また、テストを実行するユーザーが正しい sudo 権限を使用できることも検査されます。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」をクリックします。
2. 「**MongoDB**」ウィンドウで、「**アプリケーション・サーバーの管理**」をクリックして、テストするホスト・アドレスを選択します。

   使用可能な MongoDB アプリケーション・サーバーのリストが表示されます。
3. 「**アクション**」をクリックして、「**テスト**」を選択し、物理システムとリモート・システムの接続と設定の検証テストを開始します。



テスト・レポートには、物理ホスト・ネットワーク構成のテストと、ホストのリモート・サーバー・インストールのテストが含まれるリストが表示されます。

4. 「**OK**」をクリックして、テスト・レポートを閉じます。問題が報告された場合は、問題を修正して、テストを再実行し、修正を確認してください。

MongoDB データのバックアップ

データを保護するためにバックアップ・コピーを実行して作成するオプションを指定して、定期的な MongoDB バックアップ・ジョブを定義します。データを定期的にバックアップするには、SLA ポリシーを含むバックアップ・ジョブを定義します。

始める前に

初期バックアップ操作中、IBM Spectrum Protect Plus は、新規の vSnap ボリュームおよび NFS 共有を作成します。増分バックアップ時には、以前に作成されたボリュームが再使用されます。IBM Spectrum Protect Plus MongoDB エージェントは、バックアップが実行される MongoDB サーバーに共有をマウントします。

バックアップ・ジョブ定義を作成する前に、以下の前提条件を確認してください。

- バックアップするアプリケーション・サーバーを追加します。手順については、MongoDB アプリケーション・サーバーの追加を参照してください。
- SLA ポリシーを構成します。手順については、SLA バックアップ・ジョブの定義を参照してください。
- IBM Spectrum Protect Plus ユーザーがバックアップとリストアの操作をセットアップするには、その前に、そのユーザーに役割とリソース・グループを割り当てる必要があります。「**アカウント**」ペインで、リソースおよびバックアップとリストアの 操作に対するアクセス権限をユーザーに付与します。詳細については、293 ページの『第 13 章 ユーザー・アクセスの管理』 および 195 ページの『MongoDB 用の役割』 を参照してください。

制約事項 : バックアップ・ジョブがスケジュールに入れられているのと同じ時刻にインベントリー・ジョブを実行しないでください。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」を展開します。
2. バックアップするインスタンスのチェック・ボックスを選択します。

   MongoDB インスタンスごとに、バックアップされるデータは「**すべて**」としてリストされます。「インスタンス」ペインで、各インスタンスはインスタンス名、バージョン、および適用された SLA ポリシーごとにリストされます。
3. 「**オプションの選択**」をクリックしてバックアップ操作の並列ストリーム数を指定してから、「**保存**」をクリックします。並列ストリームの適切な数を選択することで、バックアップ・ジョブに要する時間を最短に抑えることができます。

   保存されたオプションは、選択されたこのインスタンスのすべてのバックアップ・ジョブで使用されます。
4. これらのオプションを使用してバックアップ・ジョブを実行するには、該当のインスタンス名をクリックし、「**すべて**」データベース表記を選択して、「**実行**」をクリックします。

   バックアップ・ジョブが始まると、「**ジョブと操作**」 > 「**ジョブの実行**」で詳細を確認できます。

   ヒント : 「**実行**」ボタンは、SLA ポリシーがデータベースの「**すべて**」表記に適用されている場合にのみ有効になります。
5. インスタンスを再度選択し、「**SLA ポリシーの選択**」をクリックして SLA ポリシーを選択します。
6. SLA の選択内容を保存します。

   カスタムの保存率と頻度を指定して新規の SLA を定義するか、既存のポリシーを編集するには、「**保護の管理**」 > 「**ポリシーの概要**」を選択します。「**SLA ポリシー**」ペインで、「**SLA ポリシーの追加**」をクリックして、ポリシー設定を定義します。

次のタスク

SLA ポリシーが保存された後、ポリシー名の横にある「**アクション**」をクリックして「**開始**」を選択することで、いつでもポリシーを実行できます。 ログで、状況が変更され、バックアップ・ジョブが実行状態であることが示されます。

実行中のジョブをキャンセルするには、ポリシー名の横にある「**アクション**」をクリックして、「**キャンセル**」を選択します。既にバックアップされたデータを保持するかどうかを確認するメッセージが表示されます。バックアップされたデータを保持するには「**はい**」を選択して、バックアップを破棄するには「**いいえ**」を選択します。

通常の SLA ジョブの定義

MongoDB インスタンスがリストされた後、データの保護を開始するために SLA ポリシーを選択して適用します。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」を展開します。
2. MongoDB インスタンスを選択して、そのインスタンスのすべてのデータをバックアップします。

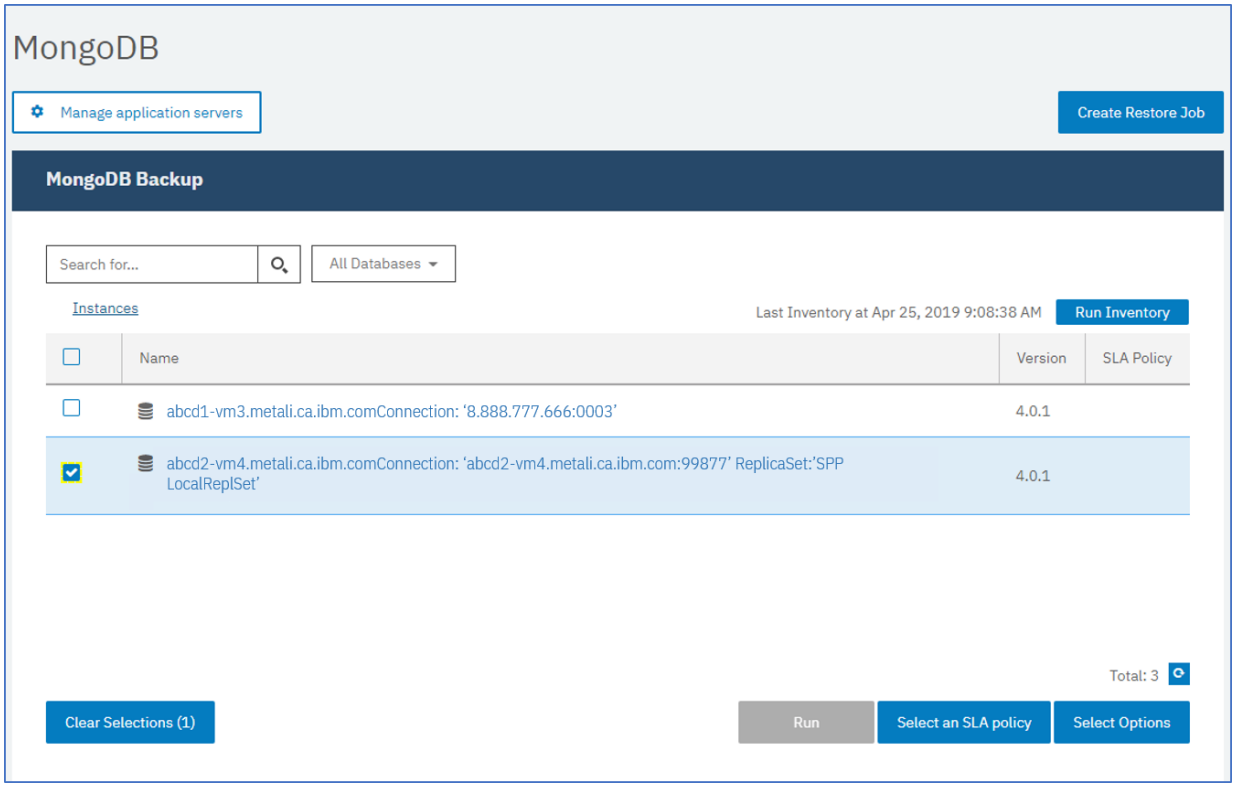


図 *26.* インスタンスを示す「*MongoDB* バックアップ」ペイン

3. 「**SLA ポリシーの選択**」をクリックして、SLA ポリシーを選択します。選択内容を保存します。

   事前定義の選択項目は、それぞれ頻度と保存率が異なる「ゴールド」、「シルバー」、および「ブロンズ」です。「**ポリシーの概要**」 > 「**SLA ポリシーの追加**」にナビゲートして、カスタム SLA ポリシーを作成することもできます。

4. オプション: 大容量データベースのバックアップにかかる時間を短縮するために複数のバックアップ・ストリームを有効にするには、「**オプションの選択**」をクリックして、並列ストリームの数を入力します。変更内容を保存します。

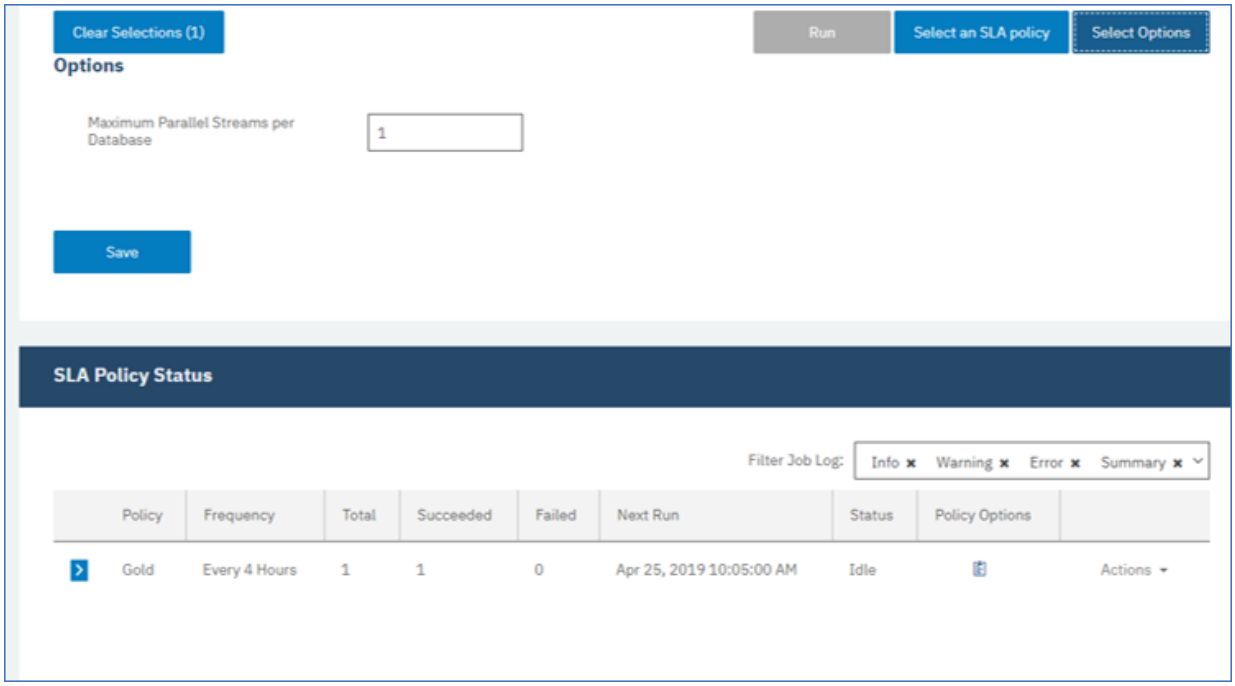


図 27. バックアップ・オプションおよび *SLA* ポリシーのステータス

5. 「**SLA ポリシーのステータス**」テーブルの「**ポリシー・オプション**」列のアイコンをクリックして、SLA ポリシーを構成します。

   SLA 構成について詳しくは、204 ページの『バックアップ用の SLA 構成オプションの設定』を参照してください。
6. スケジュールに入れられたジョブの外部でポリシーを実行する場合は、インスタンスを選択します。「**アクション**」ボタンをクリックして、「**開始**」を選択します。選択した SLA の状況が「**実行**」に代わります。表示されるログでジョブの進行状況を確認できます。

次のタスク

SLA ポリシーが保存された後、ポリシー名の横にある「**アクション**」をクリックして「**開始**」を選択することで、いつでもポリシーを実行できます。 ログで、状況が変更され、バックアップ・ジョブが実行状態であることが示されます。

実行中のジョブをキャンセルするには、ポリシー名の横にある「**アクション**」をクリックして、「**キャンセル**」を選択します。既にバックアップされたデータを保持するかどうかを確認するメッセージが表示されます。バックアップされたデータを保持するには「**はい**」を選択して、バックアップを破棄するには「**いいえ**」を選択します。

バックアップ用の SLA 構成オプションの設定

バックアップ・ジョブ用の SLA ポリシーをセットアップした後、そのジョブに対してさらに多くのオプションを構成できます。追加の SLA オプションには、スクリプトの実行やフル基本バックアップの強制実行があります。

手順

1. 構成するジョブの「**SLA ポリシーのステータス**」テーブルの「**ポリシー・オプション**」列で、クリップボード・アイコン をクリックして、追加の構成オプションを指定します。
   ジョブが既に構成されている場合は、構成を編集するためのアイコンをクリックします。

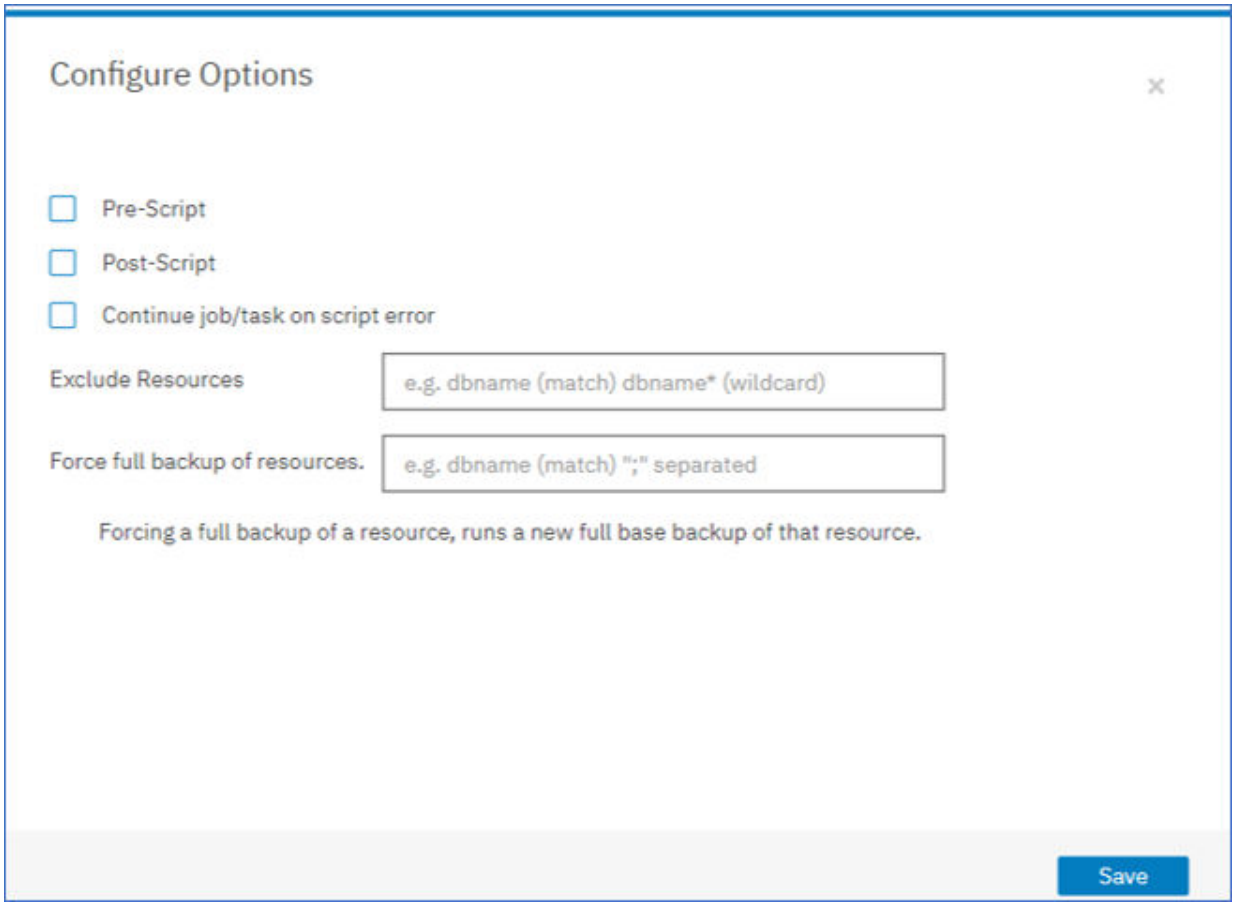


図 *28.* 追加の *SLA* 構成オプションの指定

2. 「**事前スクリプト**」をクリックして、以下のいずれかのオプションを選択し、事前スクリプト構成を定義します。
   - 「**スクリプト・サーバーの使用**」をクリックして、アップロード済みのスクリプトをメニューから選択します。
   - 「**スクリプト・サーバーの使用**」をクリックしないでください。アプリケーション・サーバーをリストから選択して、その場所でスクリプトを実行します。
3. 「**事後スクリプト**」をクリックして、以下のいずれかのオプションを選択し、事後スクリプト構成を定義します。
   - 「**スクリプト・サーバーの使用**」をクリックして、アップロード済みのスクリプトをメニューから選択します。
   - 「**スクリプト・サーバーの使用**」をクリックしないでください。アプリケーション・サーバーをリストから選択して、その場所でスクリプトを実行します。

   スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成されます。スクリプトの処理について詳しくは、**スクリプトの構成**を参照してください。
4. ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。

   このオプションが選択される場合、スクリプトの処理がゼロ以外の戻りコードで完了すると、バックアップまたはリストアの操作は最初に失敗した後で再試行され、スクリプト・タスクの状況は「完了」として報告されます。このオプションが選択されない場合は、バックアップまたはリストアは再試行されず、スクリプト・タスクの状況は「失敗」として報告されます。
5. MongoDB の SLA オプションの「**リソースの除外**」をスキップします。除外するリソースは指定できないためです。個々のデータベースではなく、インスタンスがバックアップされます。
6. MongoDB インスタンスの新規のフルバックアップを 作成するには、「**リソースのフルバックアップを 強制します**」を選択します。

そのリソースの新規のフルバックアップが作成され、1 つのオカレンスでのみ、そのリソースの既存のバックアップが置き換えられます。その後、そのリソースは以前と同様に増分バックアップされます。

MongoDB データのリストア

データをリストアするには、データを最新のバックアップにリストアするか、それ以前のバックアップ・コピーを選択するジョブを定義します。データをオリジナル・インスタンスにリストアするか、別のマシン上の代替インスタンスにリストアして複製コピーを作成するかを選択します。臨時の操作として実行されるか、スケジュール・ジョブとして定期的に実行されるように、ジョブを定義して保存します。

始める前に

MongoDB のリストア・ジョブを作成する前に、以下の要件が満たされていることを確認します。

- 少なくとも 1 つの MongoDB バックアップ・ジョブがセットアップされていて正常に実行されている。バックアップ・ジョブのセットアップについての説明は、201 ページの『MongoDB データのバックアップ』を参照してください。
- リストア・ジョブをセットアップしているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当ての手順については、293 ページの『第 13 章 ユーザー・アクセスの管理』および 195 ページの『MongoDB 用の役割』を参照してください。
- リストア操作のために十分なディスク・スペースがターゲット・サーバーに割り振られています。
- 専用ボリュームは、ファイルのコピー用に割り振られます。
- ターゲットとソースの両方のサーバーで、同じディレクトリー構造とレイアウトが使用可能です。
- IBM Spectrum Protect アーカイブからリストアする場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

代替インスタンスへのリストア操作の場合は、MongoDB がターゲットとホストのマシンで同じバージョン・レベルでなければなりません。

スペース所要量について詳しくは、MongoDB 保護のためのスペース前提条件を参照してください。前提条件およびセットアップについて詳しくは、MongoDB の前提条件を参照してください。

手順

MongoDB リストア・ジョブを定義するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**MongoDB**」をクリックして開始することもできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、  アイコンにカーソルを移動します。
   - ウィザードでオプションのページをバイパスする場合は、「**オプションのステップをスキップ (Skip optional steps)**」を選択します。

2. 「**ソースの選択**」ページで、以下のステップを実行します。

   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。

   b) リストア操作のソースとして使用するデータベースの横にある「リストア・リストに追加」アイコン  をクリックします。複数のデータベースをリストから選択できます。

   選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストのソースから項目を削除するには、その項目の横にある「リストア・リストから削除」アイコン  をクリックします。

c)「**次へ**」をクリックして先に進みます。

3.「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを 指定します。以下のフィールドに入力し、「**次へ**」をクリックして続行します。

オプション	説明
リストアのタイプ	実行するリストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** スナップショット・バックアップからの 1 回限りのリストア操作を実行します。 **オンデマンド: 特定時点** 特定時点バックアップからの 1 回限りのリストア操作を実行します。 **繰り返し** 最新のリストア・ポイントからデータの定期リストア操作を実行します。
リストア・ロケーションのタイプ	リストア元にするロケーションのタイプを以下から選択します。 **サイト** バックアップ・ストレージ・サーバーに関連付けられたサイトからデータをリストアします。 **クラウド・オフロード** クラウド・ストレージに保管されているデータをリストアします。 **リポジトリー・オフロード** リポジトリー・サーバーに保管されているデータをリストアします。 **クラウド・アーカイブ** クラウド・ストレージにアーカイブされているデータをリストアします。 **リポジトリー・アーカイブ** リポジトリー・サーバーにアーカイブされているデータをリストアします。
ロケーションの選択 (Select a location)	サイトからデータをリストアする 場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** テスト用にセットアップされているデモンストレーション vSnap サーバーからデータをリストアします。 **1 次** 1 次バックアップ宛先である vSnap サーバーからデータをリストアします。 **2 次** 2 次バックアップ宛先である vSnap サーバーからデータをリストアします。 クラウド・サーバーまたはリポジトリー・サーバーからデータをリストアする場合、ロケーションは既に選択されているため、ユーザーが選択する必要はありません。
日付セレクター	オンデマンド・リストア操作の場合は、日付の範囲を指定すると、その日付範囲内で使用可能なスナップショットが表示されます。
リストア・ポイント	オンデマンド・リストア操作の場合は、選択した日付範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーから特定のリストア・ポイントをリストアする場合に、代替 vSnap サーバーを指定するには、このボックスを選択して、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーにオフロードされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽

オプション	説明
	減するために、リストア操作のゲートウェイとして使用する代替 vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、オリジナル・サーバーにリストアする場合は「**オリジナル・インスタンスにリストアする**」を選択して、リスト内のロケーションから選択できる別のロケーションにリストアする場合は「**代替インスタンスにリストアする**」を選択します。

   オリジナル・インスタンスへのデータのリストアについて詳しくは、オリジナル・インスタンスへのリストアを参照してください。代替インスタンスへのデータのリストアについて詳しくは、代替インスタンスへのリストアを参照してください。

5. 「**リストア方式**」ページで、リストア操作のタイプを選択し、「**次へ**」をクリックして先に進みます。

   - **テスト**: このモードでは、エージェントは、vSnap リポジトリーから直接データ・ファイルを使用してデータベースを作成します。このオプションは、代替インスタンスにデータをリストアする場合にのみ使用できます。MongoDB サーバーが始動された後、レプリカ・セットのメンバーが再構成されることはありません。サーバーは、単一ノードのレプリカ・セットとして始動されます。
   - **実動**: このモードでは、MongoDB アプリケーション・サーバーは、最初に vSnap リポジトリーからターゲット・ホストにファイルをコピーします。コピーされたデータは、データベースの開始に使用されます。実動リストア操作中、レプリカ・セットのメンバーである MongoDB インスタンスは始動されません。このアクションにより、レプリカ・セットへの接続時にデータは上書きされなくなります。
   - **インスタント・アクセス**: このモードでは、IBM Spectrum Protect Plus が共有をマウントした後、それ以上のアクションは実行されません。vSnap リポジトリー内のファイルからのカスタム・リカバリーにデータを使用します。

   テスト・モードまたは実動モードの場合、オプションで、リストアされるデータベースの新規名を入力できます。

   実動モードの場合は、データベースを展開して新規フォルダー名を入力することで、リストアされるデータベース用に新規フォルダーを指定できます。

6. オプション: 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   「**リカバリー・オプション**」セクションでは、MongoDB に対して「**バックアップの最後までリカバリーする**」がデフォルトで選択されています。このオプションにより、バックアップが作成された時点における状態に、選択したデータがリカバリーされます。リカバリー操作では、MongoDB バックアップに含まれているログ・ファイルが使用されます。

   アプリケーション・オプション
   以下のアプリケーション・オプションを設定します。

   既存のデータベースを上書きする
   選択済みデータベースをリストア・ジョブが上書きすることを許可するには、このオプションを有効にします。このオプションが選択されない場合、リストア・プロセス中に名前が同じデータが検出されると、リストア・ジョブは失敗します。

   重要: 他のデータが元のデータと同じローカル・データベース・ディレクトリーを共有していないことを確認してください。そうしないと、元のデータが上書きされます。

   データベースごとの最大並列ストリーム数
   バックアップ・ストレージからのデータベースごとの並列データ・ストリームの最大数を設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を 1 に設定すると、複数のデータベースのリストアを並列に実行できます。複数の並列ストリームでリストア操作の速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

   このオプションは、MongoDB データベースを元のデータベース名を使用してオリジナル・ロケーションにリストアする場合にのみ適用可能です。

   高度なオプション
   以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
このオプションはデフォルトで選択されており、リカバリーが失敗した場合にリストア操作の一部として割り振り済みのリソースを自動的にクリーンアップします。

セッションの上書きを許可する
リストア操作時に名前が同じ既存のデータベースを置き換える場合は、このオプションを選択します。インスタント・ディスク・リストア操作時に、既存のデータベースはシャットダウンされて上書きされ、リカバリーされたデータベースが再始動されます。このオプションが選択されていない場合、同じ名前のデータベースが検出されると、リストア操作はエラーで失敗します。

いずれかが失敗しても、他の選択されたデータベースのリストアを続行する
インスタンスの 1 つのデータベースが正常にリストアされない場合でも、リストアの対象になっているその他のすべてのデータに対するリストア操作は続行されます。このオプションが選択されていない場合、リソースのリカバリーが失敗すると、リストア・ジョブは停止します。

マウント・ポイント接頭部
「**インスタント・アクセス**」リストア操作の場合、マウントの送信先のパスのマウント・ポイント接頭部を指定します。

7. オプション:「**スクリプトの適用**」ページで、ジョブの実行前または実行後に実行可能なスクリプトを指定します。Windows オペレーティング・システムはバッチ・スクリプトと PowerShell スクリプトをサポートし、Linux オペレーティング・システムはシェル・スクリプトをサポートしています。

   事前スクリプト
   アップロードされたスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このチェック・ボックスを選択します。アプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーを構成する場合は、「**システム構成**」 > 「**スクリプト**」をクリックします。

   事後スクリプト
   アップロードされたスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このオプションを選択します。アプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーを構成する場合は、「**システム構成**」 > 「**スクリプト**」ページをクリックします。

   スクリプト・エラー時にジョブ/タスクを続行
   ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、このオプションを選択します。このオプションが有効になっている場合、スクリプトがゼロ以外の戻りコードで処理を完了すると、バックアップまたはリストアのジョブの 実行は続行され、事前スクリプト・タスクの状況は「完了」と報告されます。事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、事後スクリプト・タスク状況は「完了」と報告されます。このオプションが選択されない場合は、バックアップまたはリストアのジョブは実行されず、事前スクリプトまたは事後スクリプトのタスク状況は「失敗」と報告されます。

   「**次へ**」をクリックして先に進みます。
8. 「**スケジュール**」ページで、「**次へ**」をクリックして、「スナップショットのリストア」ウィザードを完了後にオンデマンド・ジョブを開始します。反復ジョブの場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。
9. 「**確認**」ページで、リストア・ジョブの設定を確認します。

   重要 : 「**実行**」に進む前に、選択したオプションを確認します。「**既存のデータベースを上書きする**」アプリケーション・オプションが選択された場合はデータが上書きされるためです。進行中のリストア・ジョブをキャンセルできますが、「**既存のデータベースを上書きします**」オプションが選択されている場合は、ジョブをキャンセルしてもデータは上書きされます。

10. ジョブを続行するには、「**実行**」をクリックします。ジョブをキャンセルするには、「**ジョブと操作**」にナビゲートして、「**スケジュール**」タブをクリックします。キャンセルするリストア・ジョブを見つけます。「**アクション**」をクリックして、「**キャンセル**」を選択します。

タスクの結果

「**リストア**」を選択してしばらくすると、「**onDemandRestore**」ジョブが「**ジョブと操作**」 > 「**実行中のジョブ**」ペインに追加されます。このレコードをクリックして、操作のステップごとの詳細を表示します。「**ダウンロード (.zip)**」をクリックして、ログ・ファイル (zip) をダウンロードすることもできます。その他のジョブについては、「**実行中のジョブ**」タブまたは「**ジョブ・ヒストリー**」タブをクリックし、ジョブをクリックしてその詳細を表示します。

リストアされるサーバーの IP アドレスとポートは、リストア操作のログ・ファイルで見つかります。「**ジョブと操作**」 > 「**実行中のジョブ**」にナビゲートして、リストア操作のログを見つけます。

オリジナル・インスタンスへのデータのリストアについては、オリジナル・インスタンスへのリストアを参照してください。代替インスタンスへのデータのリストアについては、代替インスタンスへのリストアを参照してください。

オリジナル・インスタンスへの MongoDB データのリストア

MongoDB インスタンスを元のホストにリストアすることが可能で、最新バックアップへのリストアか、それより前の MongoDB データベース・バックアップ・バージョンへのリストアかを選択できます。オリジナル・インスタンスにデータをバックアップする 場合は、データを名前変更することはできません。このリストア操作では、データの完全な実動リストアが実行され、「**既存のデータベースを上書きします**」アプリケーション・オプションが選択されている場合にはターゲット・サイトで既存のデータが上書きされます。

始める前に

MongoDB のリストア・ジョブを作成する前に、以下の要件が満たされていることを確認します。

- 少なくとも 1 つの MongoDB バックアップ・ジョブがセットアップされていて正常に実行されている。バックアップ・ジョブのセットアップについての説明は、201 ページの『MongoDB データのバックアップ』を参照してください。
- リストア・ジョブをセットアップしているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当ての手順については、293 ページの『第 13 章 ユーザー・アクセスの管理』および 195 ページの『MongoDB 用の役割』を参照してください。
- リストア操作のために十分なディスク・スペースがターゲット・サーバーに割り振られています。
- 専用ボリュームは、ファイルのコピー用に割り振られます。
- ターゲットとソースの両方のサーバーで、同じディレクトリー構造とレイアウトが使用可能です。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

スペース所要量について詳しくは、MongoDB 保護のためのスペース前提条件を参照してください。前提条件およびセットアップについて詳しくは、MongoDB の前提条件を参照してください。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント:

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**MongoDB**」をクリックして開始することもできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、  アイコンにカーソルを移動します。
   - ウィザードでオプションのページをバイパスする 場合は、「**オプションのステップをスキップ (Skip optional steps)**」を選択します。
2. 「**ソースの選択**」ページで、以下のステップを実行します。

a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。

b) リストア操作のソースとして使用するデータベースの横にある「リストア・リストに追加」アイコン をクリックします。複数のデータベースをリストから選択できます。

選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストのソースから項目を削除するには、その項目の横にある「リストア・リストから削除」アイコン をクリックします。

c)「**次へ**」をクリックして先に進みます。

3.「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして続行します。

オプション	説明
リストアのタイプ	実行するリストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** スナップショット・バックアップからの 1 回限りのリストア操作を実行します。 **オンデマンド: 特定時点** 特定時点バックアップからの 1 回限りのリストア操作を実行します。 **繰り返し** 最新のリストア・ポイントからデータの定期リストア操作を実行します。
リストア・ロケーションのタイプ	リストア元にするロケーションのタイプを以下から選択します。 **サイト** バックアップ・ストレージ・サーバーに関連付けられたサイトからデータをリストアします。 **クラウド・オフロード** クラウド・ストレージに保管されているデータをリストアします。 **リポジトリー・オフロード** リポジトリー・サーバーに保管されているデータをリストアします。 **クラウド・アーカイブ** クラウド・ストレージにアーカイブされているデータをリストアします。 **リポジトリー・アーカイブ** リポジトリー・サーバーにアーカイブされているデータをリストアします。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** テスト用にセットアップされているデモンストレーション vSnap サーバーからデータをリストアします。 **1 次** 1 次バックアップ宛先である vSnap サーバーからデータをリストアします。 **2 次** 2 次バックアップ宛先である vSnap サーバーからデータをリストアします。 クラウド・サーバーまたはリポジトリー・サーバーからデータをリストアする場合、ロケーションは既に選択されているため、ユーザーが選択する必要はありません。
日付セレクター	オンデマンド・リストア操作の場合は、日付の範囲を指定すると、その日付範囲内で使用可能なスナップショットが表示されます。

オプション	説明
リストア・ポイント	オンデマンド・リストア操作の場合は、選択した日付範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーから特定のリストア・ポイントをリストアする場合に、代替 vSnap サーバーを指定するには、このボックスを選択して、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーにオフロードされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、リストア操作のゲートウェイとして使用する代替 vSnap サーバーを選択できます。

4. 「宛先の設定」ページで、「**オリジナル・インスタンスにリストアする**」を選択して、「**次へ**」をクリックします。
5. 「**リストア方式**」ページで、リストア操作のタイプを選択し、「**次へ**」をクリックして先に進みます。
   - **実動**

     インスタンス全体をオリジナル・インスタンスへリカバリーするには、上書きのアプリケーション・オプションを選択して、このオプションを選択することをお勧めします。実動リストア操作中、レプリカ・セットのメンバーである MongoDB インスタンスは始動されません。このアクションにより、レプリカ・セットへの接続時にデータは上書きされなくなります。
   - **テスト**

     データを同じサーバーにリストアするには、このオプションを選択します。ただし、ポートは別のポートを使用します。
   - **インスタント・アクセス**

     このオプションは、データをリストアしたり上書きしたりすることなく、バックアップをアプリケーション・サーバーにマウントする場合に選択します。

     「**次へ**」をクリックして先に進みます。

   テスト・モードまたは実動モードの場合、オプションで、リストアされるデータベースの新規名を入力できます。

   実動モードの場合は、データベースを展開して新規フォルダー名を入力することで、リストアされるデータベース用に新規フォルダーを指定できます。
6. オプション: 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   「**リカバリー・オプション**」セクションでは、MongoDB に対して「**バックアップの最後までリカバリーする**」がデフォルトで選択されています。このオプションにより、バックアップが作成された時点における状態に、選択したデータがリカバリーされます。リカバリー操作では、MongoDB バックアップに含まれているログ・ファイルが使用されます。

   アプリケーション・オプション

   以下のアプリケーション・オプションを設定します。

   既存のデータベースを上書きする

   選択済みデータベースをリストア・ジョブが上書きすることを許可するには、このオプションを有効にします。このオプションが選択されない場合、リストア・プロセス中に名前が同じデータが検出されると、リストア・ジョブは失敗します。

   重要: 他のデータが元のデータと同じローカル・データベース・ディレクトリーを共有していないことを確認してください。そうしないと、元のデータが上書きされます。

データベースごとの最大並列ストリーム数
バックアップ・ストレージからのデータベースごとの並列データ・ストリームの最大数を設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を 1 に設定すると、複数のデータベースのリストアを並列に実行できます。複数の並列ストリームでリストア操作の速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

このオプションは、MongoDB データベースを元のデータベース名を使用してオリジナル・ロケーションにリストアする場合にのみ適用可能です。

高度なオプション
以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
このオプションはデフォルトで 選択されており、リカバリーが失敗した場合にリストア操作の一部として割り振り済みのリソースを自動的にクリーンアップします。

セッションの上書きを許可する
リストア操作時に名前が同じ既存のデータベースを置き換える場合は、このオプションを選択します。 インスタント・ディスク・リストア操作時に、既存のデータベースはシャットダウンされて上書きされ、リカバリーされたデータベースが再始動されます。このオプションが選択されていない場合、同じ名前のデータベースが検出されると、リストア操作はエラーで失敗します。

いずれかが失敗しても、他の選択されたデータベースのリストアを続行する
インスタンスの 1 つのデータベースが正常にリストアされない場合でも、リストアの対象になっているその他のすべてのデータに対するリストア操作は続行されます。このオプションが選択されていない場合、リソースのリカバリーが失敗すると、リストア・ジョブは停止します。

マウント・ポイント接頭部
「**インスタント・アクセス**」リストア操作の場合、マウントの送信先のパスのマウント・ポイント接頭部を指定します。

7. オプション:「**スクリプトの適用**」ページで、ジョブの実行前または実行後に実行可能なスクリプトを指定します。Windows オペレーティング・システムはバッチ・スクリプトと PowerShell スクリプトをサポートし、Linux オペレーティング・システムはシェル・スクリプトをサポートしています。

事前スクリプト
アップロードされたスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このチェック・ボックスを選択します。アプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーを構成する場合は、「**システム構成**」 > 「**スクリプト**」をクリックします。

事後スクリプト
アップロードされたスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このオプションを選択します。アプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーを構成する場合は、「**システム構成**」 > 「**スクリプト**」ページをクリックします。

スクリプト・エラー時にジョブ/タスクを続行
ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、このオプションを選択します。このオプションが有効になっている場合、スクリプトがゼロ以外の戻りコードで処理を完了すると、バックアップまたはリストアのジョブの 実行は続行され、事前スクリプト・タスクの状況は「完了」と報告されます。事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、事後スクリプト・タスク状況は「完了」と報告されます。このオプションが選択されない場合は、バックアップまたはリストアのジョブは実行されず、事前スクリプトまたは事後スクリプトのタスク状況は「失敗」と報告されます。

「**次へ**」をクリックして先に進みます。

8. 「**スケジュール**」ページで、「**次へ**」をクリックして、「スナップショットのリストア」ウィザードを完了後にオンデマンド・ジョブを開始します。反復ジョブの場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。

9. 「**確認**」ページで、リストア・ジョブの設定を確認します。

   重要：「**実行**」に進む前に、選択したオプションを確認します。「**既存のデータベースを上書きする**」アプリケーション・オプションが選択された場合はデータが上書きされるためです。進行中のリストア・ジョブをキャンセルできますが、「**既存のデータベースを上書きします**」オプションが選択されている場合は、ジョブをキャンセルしてもデータは上書きされます。

10. ジョブを続行するには、「**実行**」をクリックします。ジョブをキャンセルするには、「**ジョブと操作**」にナビゲートして、「**スケジュール**」タブをクリックします。キャンセルするリストア・ジョブを見つけます。「**アクション**」をクリックして、「**キャンセル**」を選択します。

代替インスタンスへの MongoDB データのリストア

MongoDB データベース・バックアップを選択して、代替ホスト上にリストアすることができます。データベースを別の vSnap リポジトリーにリストアしたり、データベースを名前変更したりすることもできます。このプロセスにより、別のホスト上にインスタンスの正確なコピーが作成されます。

始める前に

MongoDB のリストア・ジョブを作成する前に、以下の要件が満たされていることを確認します。

- 少なくとも 1 つの MongoDB バックアップ・ジョブがセットアップされていて正常に実行されている。バックアップ・ジョブのセットアップについての説明は、201 ページの『MongoDB データのバックアップ』を参照してください。
- リストア・ジョブをセットアップしているユーザーに IBM Spectrum Protect Plus の役割とリソース・グループが割り当てられている。役割の割り当ての手順については、293 ページの『第 13 章 ユーザー・アクセスの管理』および 195 ページの『MongoDB 用の役割』を参照してください。
- リストア操作のために十分なディスク・スペースがターゲット・サーバーに割り振られています。
- 専用ボリュームは、ファイルのコピー用に割り振られます。
- ターゲットとソースの両方のサーバーで、同じディレクトリー構造とレイアウトが使用可能です。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

代替インスタンスへのリストア操作の場合は、MongoDB がターゲットとホストのマシンで同じバージョン・レベルでなければなりません。

スペース所要量について詳しくは、MongoDB 保護のためのスペース前提条件を参照してください。前提条件およびセットアップについて詳しくは、MongoDB の前提条件を参照してください。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント：

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**MongoDB**」をクリックして開始することもできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、アイコンにカーソルを移動します。
   - ウィザードでオプションのページをバイパスする 場合は、「**オプションのステップをスキップ (Skip optional steps)**」を選択します。

2. 「**ソースの選択**」ページで、以下のステップを実行します。

   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。

b) リストア操作のソースとして使用するデータベースの横にある「リストア・リストに追加」アイコン をクリックします。複数のデータベースをリストから選択できます。

選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストのソースから項目を削除するには、その項目の横にある「リストア・リストから削除」アイコン をクリックします。

c)「**次へ**」をクリックして先に進みます。

3.「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして続行します。

オプション	説明
リストアのタイプ	実行するリストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** スナップショット・バックアップからの 1 回限りのリストア操作を実行します。 **オンデマンド: 特定時点** 特定時点バックアップからの 1 回限りのリストア操作を実行します。 **繰り返し** 最新のリストア・ポイントからデータの定期リストア操作を実行します。
リストア・ロケーションのタイプ	リストア元にするロケーションのタイプを以下から選択します。 **サイト** バックアップ・ストレージ・サーバーに関連付けられたサイトからデータをリストアします。 **クラウド・オフロード** クラウド・ストレージに保管されているデータをリストアします。 **リポジトリー・オフロード** リポジトリー・サーバーに保管されているデータをリストアします。 **クラウド・アーカイブ** クラウド・ストレージにアーカイブされているデータをリストアします。 **リポジトリー・アーカイブ** リポジトリー・サーバーにアーカイブされているデータをリストアします。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** テスト用にセットアップされているデモンストレーション vSnap サーバーからデータをリストアします。 **1 次** 1 次バックアップ宛先である vSnap サーバーからデータをリストアします。 **2 次** 2 次バックアップ宛先である vSnap サーバーからデータをリストアします。 クラウド・サーバーまたはリポジトリー・サーバーからデータをリストアする場合、ロケーションは既に選択されているため、ユーザーが選択する必要はありません。
日付セレクター	オンデマンド・リストア操作の場合は、日付の範囲を指定すると、その日付範囲内で使用可能なスナップショットが表示されます。
リストア・ポイント	オンデマンド・リストア操作の場合は、選択した日付範囲内で使用可能なスナップショットのリストからスナップショットを選択します。

オプション	説明
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーから特定のリストア・ポイントをリストアする場合に、代替 vSnap サーバーを指定するには、このボックスを選択して、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーにオフロードされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、リストア操作のゲートウェイとして使用する代替 vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、「**代替インスタンスにリストアする**」を選択して、データのリストア先のターゲット・インスタンスを選択します。

   「**代替インスタンスにリストアします**」を選択する場合は元のデータを上書きできないため、オリジナル・インスタンスを選択することはできません。また、別のバージョン・レベルのインスタンスや、オリジナル・インスタンスと同じホスト上のインスタンスを選択することもできません。

   「**次へ**」をクリックして先に進みます。
5. 「**リストア方式**」ページで、リストア操作のタイプを選択し、「**次へ**」をクリックして先に進みます。
   - **テスト**: このモードでは、エージェントは、vSnap リポジトリーから直接データ・ファイルを使用してデータベースを作成します。このオプションは、代替インスタンスにデータをリストアする場合にのみ使用できます。MongoDB サーバーが始動された後、レプリカ・セットのメンバーが再構成されることはありません。サーバーは、単一ノードのレプリカ・セットとして始動されます。
   - **実動**: このモードでは、MongoDB アプリケーション・サーバーは、最初に vSnap リポジトリーからターゲット・ホストにファイルをコピーします。コピーされたデータは、データベースの開始に使用されます。実動リストア操作中、レプリカ・セットのメンバーである MongoDB インスタンスは始動されません。このアクションにより、レプリカ・セットへの接続時にデータは上書きされなくなります。
   - **インスタント・アクセス**: このモードでは、IBM Spectrum Protect Plus が共有をマウントした後、それ以上のアクションは実行されません。vSnap リポジトリー内のファイルからのカスタム・リカバリーにデータを使用します。

   テスト・モードまたは実動モードの場合、オプションで、リストアされるデータベースの新規名を入力できます。

   実動モードの場合は、データベースを展開して新規フォルダー名を入力することで、リストアされるデータベース用に新規フォルダーを指定できます。
6. オプション: 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   「**リカバリー・オプション**」セクションでは、MongoDB に対して「**バックアップの最後までリカバリーする**」がデフォルトで選択されています。このオプションにより、バックアップが作成された時点における状態に、選択したデータがリカバリーされます。リカバリー操作では、MongoDB バックアップに含まれているログ・ファイルが使用されます。

   アプリケーション・オプション

   以下のアプリケーション・オプションを設定します。

   既存のデータベースを上書きする

   選択済みデータベースをリストア・ジョブが上書きすることを許可するには、このオプションを有効にします。このオプションが選択されない場合、リストア・プロセス中に名前が同じデータが検出されると、リストア・ジョブは失敗します。

   重要 : 他のデータが元のデータと同じローカル・データベース・ディレクトリーを共有していないことを確認してください。そうしないと、元のデータが上書きされます。

データベースごとの最大並列ストリーム数
バックアップ・ストレージからのデータベースごとの並列データ・ストリームの最大数を設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を 1 に設定すると、複数のデータベースのリストアを並列に実行できます。複数の並列ストリームでリストア操作の速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

このオプションは、MongoDB データベースを元のデータベース名を使用してオリジナル・ロケーションにリストアする場合にのみ適用可能です。

高度なオプション
以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
このオプションはデフォルトで 選択されており、リカバリーが失敗した場合にリストア操作の一部として割り振り済みのリソースを自動的にクリーンアップします。

セッションの上書きを許可する
リストア操作時に名前が同じ既存のデータベースを置き換える場合は、このオプションを選択します。 インスタント・ディスク・リストア操作時に、既存のデータベースはシャットダウンされて上書きされ、リカバリーされたデータベースが再始動されます。このオプションが選択されていない場合、同じ名前のデータベースが検出されると、リストア操作はエラーで失敗します。

いずれかが失敗しても、他の選択されたデータベースのリストアを続行する
インスタンスの 1 つのデータベースが正常にリストアされない場合でも、リストアの対象になっているその他のすべてのデータに対するリストア操作は続行されます。このオプションが選択されていない場合、リソースのリカバリーが失敗すると、リストア・ジョブは停止します。

マウント・ポイント接頭部
「**インスタント・アクセス**」リストア操作の場合、マウントの送信先のパスのマウント・ポイント接頭部を指定します。

7. オプション:「**スクリプトの適用**」ページで、ジョブの実行前または実行後に実行可能なスクリプトを指定します。Windows オペレーティング・システムはバッチ・スクリプトと PowerShell スクリプトをサポートし、Linux オペレーティング・システムはシェル・スクリプトをサポートしています。

事前スクリプト
アップロードされたスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このチェック・ボックスを選択します。アプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーを構成する場合は、「**システム構成**」 > 「**スクリプト**」をクリックします。

事後スクリプト
アップロードされたスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このオプションを選択します。アプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーを構成する場合は、「**システム構成**」 > 「**スクリプト**」ページをクリックします。

スクリプト・エラー時にジョブ/タスクを続行
ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、このオプションを選択します。このオプションが有効になっている場合、スクリプトがゼロ以外の戻りコードで処理を完了すると、バックアップまたはリストアのジョブの 実行は続行され、事前スクリプト・タスクの状況は「完了」と報告されます。事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、事後スクリプト・タスク状況は「完了」と報告されます。このオプションが選択されない場合は、バックアップまたはリストアのジョブは実行されず、事前スクリプトまたは事後スクリプトのタスク状況は「失敗」と報告されます。

「**次へ**」をクリックして先に進みます。

8. 「**スケジュール**」ページで、「**次へ**」をクリックして、「スナップショットのリストア」ウィザードを完了後にオンデマンド・ジョブを開始します。反復ジョブの場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。

9. 「**確認**」ページで、リストア・ジョブの設定を確認します。

   重要：「**実行**」に進む前に、選択したオプションを確認します。「**既存のデータベースを上書きする**」アプリケーション・オプションが選択された場合はデータが上書きされるためです。進行中のリストア・ジョブをキャンセルできますが、「**既存のデータベースを上書きします**」オプションが選択されている場合は、ジョブをキャンセルしてもデータは上書きされます。

10. ジョブを続行するには、「**実行**」をクリックします。ジョブをキャンセルするには、「**ジョブと操作**」にナビゲートして、「**スケジュール**」タブをクリックします。キャンセルするリストア・ジョブを見つけます。「**アクション**」をクリックして、「**キャンセル**」を選択します。

MongoDB の高細分度リストア操作の使用

高細分度リストア操作を使用して、特定の MongoDB のデータベースまたはコレクションをリストアできます。高細分度リストア操作では、最初に、テストのリストア・ジョブを実行してから、適切な MongoDB コマンドを実行します。

始める前に

認証が有効になっている場合、ユーザーがテスト・リストア操作でインスタンスに対する許可を修正できるようにユーザーの資格情報を指定する必要があります。

このタスクについて

MongoDB の高細分度リストア操作は、テスト・モードのリストア・ジョブに基づいています。テストのリストア・ジョブを IBM Spectrum Protect Plus で実行し、**mongodump** コマンドと **mongorestore** コマンドを MongoDB サーバーで実行すると、リカバリー・ソースから個々のデータベースまたはコレクションにアクセスできます。

この手順を使用して以下のいずれかのタスクを実行します。

- 必要なデータベースに対して **mongodump** コマンドと **mongorestore** コマンドを使用して、任意の数のデータベースをリストアする。
- 必要なコレクションに対して **mongodump** コマンドと **mongorestore** コマンドを使用して、任意の数のコレクションをリストアする。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**MongoDB**」をクリックします。
2. 「**リストア・ジョブの作成**」をクリックして、リストア・ウィザードを開きます。MongoDB が自動的に選択されます。
3. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。
   b) リストア操作のソースとして使用するデータベースの横にある「リストア・リストに追加」アイコン をクリックします。複数のデータベースをリストから選択できます。

      選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストのソースから項目を削除するには、その項目の横にある「リストア・リストから削除」アイコン をクリックします。
   c) 「**次へ**」をクリックして先に進みます。
4. 「**宛先の設定**」ページで、「**代替インスタンスにリストアする**」を選択し、データのリストア先にするターゲット・インスタンスを選択します。

   「**代替インスタンスにリストアする**」を選択した場合は元のデータを上書きできないため、オリジナル・インスタンスを選択することはできません。別のバージョン・レベルのインスタンスは選択できません。オリジナル・インスタンスと同じホスト上の他のインスタンスも選択できません。

「**次へ**」をクリックして先に進みます。

5. 「**リストア方式**」ページで、「**テスト**」を選択し、「**次へ**」をクリックして、テスト・リストア・プロセスに進みます。
6. 「リストア」ウィザードの各ページを進み、必要なオプションを選択します。
7. 「**確認**」ページで、リストア・ジョブの設定を確認します。

   重要：「**実行**」に進む前に、選択したオプションを確認します。「**既存のデータベースを上書きする**」アプリケーション・オプションが選択された場合はデータが上書きされるためです。進行中のリストア・ジョブをキャンセルできますが、「**既存のデータベースを上書きします**」オプションが選択されている場合は、ジョブをキャンセルしてもデータは上書きされます。

8. テストのリストア・ジョブが向けられている MongoDB サーバーにログオンします。
9. MongoDB システム・コマンド `ps -ef | grep mongod` を実行して、一時的なリカバリー MongoDB インスタンスのロケーションを見つけます。
10. MongoDB mongodump コマンドを実行して、特定のデータベースまたはコレクションのダンプ・ファイルを作成します。

    適切なコマンドを使用してください。最初のコマンドはデータベース向けのものであり、2 番目のコマンドはコレクション向けです。

    ```
    mongodump --host <hostname> --port <port> --db <dbname> <dumpfolder>
    ```

    または

    ```
    mongodump --host <hostname> --port <port> --collection <collectionname> <dumpfolder>
    ```

11. **mongorestore** コマンドを実行して、任意の MongoDB インスタンスにダンプ・ファイルをリストアします。バックアップが作成されたオリジナルの MongoDB インスタンス、または任意の代替インスタンスを選択します。

    適切なコマンドを使用してください。最初のコマンドはデータベース向けのものであり、2 番目のコマンドはコレクション向けです。

    ```
    mongorestore --host <hostname> --port <port> --db <dbname> <dumpfolder>¥<dbname>
    ```

    または

    ```
    mongorestore --host <hostname> --port <port> --collection <collectionname> <dumpfolder>
    ¥<dbname>
    ```

12. データベースまたはコレクションのリストア操作が完了したら、「**ジョブと操作**」 > 「**アクティブ・リソース**」に移動します。
13. 「**アクション**」 > 「**リストアのキャンセル**」をクリックして、高細分度リストア手順を終了します。

SQL Server データのバックアップとリストア

SQL Server サーバーのコンテンツを保護するには、IBM Spectrum Protect Plus が SQL Server を認識するように SQL Server インスタンスを最初に登録します。次に、バックアップ操作およびリストア操作用のジョブを作成します。

システム要件

ご使用の SQL Server 環境が 39 ページの『Microsoft SQL Server の要件』 のシステム要件を満たしていることを確認してください。

登録および認証

IBM Spectrum Protect Plus で各 SQL Server サーバーを名前または IP アドレスで登録します。SQL Server Cluster (AlwaysOn) ノードを登録する場合、各ノードを名前または IP アドレスで登録します。IP アドレス

は公開であり、ポート 5985 で listen する必要があることに注意してください。完全修飾ドメイン名と仮想マシンのノード DNS 名は解決可能であり、IBM Spectrum Protect Plus アプライアンスからルーティング可能でなければなりません。

ユーザー ID には、「**サービスとしてログオン**」権限を含めて、ノード上で IBM Spectrum Protect Plus Tools Service をインストールして開始できる十分な権限が必要です。 この権限について詳しくは、Add the Log on as a service Right to an Account を参照してください。

デフォルトのセキュリティー・ポリシーでは Windows NTLM プロトコルを使用し、ユーザー ID の形式はデフォルトの *domain*¥*name* 形式に従います。

グループ・ポリシー・オブジェクトの設定として Windows Group Policy Object (GPO) を使用する場合、**Network security: LAN Manager** 認証レベルが正しく設定されなければなりません。以下のいずれかのオプションを使用して設定してください。

- 未定義
- NTLMv2 応答のみ送信する
- NTLMv2 応答のみ送信する (LM を拒否する)
- NTLMv2 応答のみ送信する (LM と NTLM を拒否する)

Kerberos 要件

Kerberos ベースの認証は、IBM Spectrum Protect Plus アプライアンスの構成ファイルを使用して有効にすることができます。これにより、デフォルトの Windows NTLM プロトコルが指定変更されます。

Kerberos ベースの認証の場合のみ、ユーザー ID は username@FQDN 形式で指定されなければなりません。完全修飾ドメイン名で指定されたドメイン上の鍵配布センター (KDC) から発券許可証 (TGT) を取得するには、ユーザー名は、登録済みのパスワードを使用して認証できなければなりません。

Kerberos 認証には、ドメイン・コントローラーと IBM Spectrum Protect Plus アプライアンスとの間のクロック・スキューが 5 分未満であることも必要です。

デフォルトの Windows NTLM プロトコルは、時間に依存しません。

特権

SQL Server サーバーのシステム・ログイン資格情報には、パブリック許可と sysadmin 許可に加えて、SQL Server AlwaysOn 環境でクラスター・リソースにアクセスする許可も有効になっている必要があります。すべての SQL Server 機能に 1 つのユーザー・アカウントを使用する場合、SQL Server サーバーに対する Windows ログインが有効であり、パブリック許可と sysadmin 許可が有効でなければなりません。

各 SQL Server インスタンスで、その特定のインスタンスのリソースにアクセスするために特定のユーザー・アカウントを使用できます。

ログ・バックアップ操作を実行するには、IBM Spectrum Protect Plus に登録された SQL Server ユーザーには、SQL Server エージェント・ジョブを管理するための sysadmin 許可が有効になっている必要があります。

Windows タスク・スケジューラーはログ・バックアップをスケジュールするために使用されます。環境によっては、ユーザーに次のエラーが表示されることがあります: 指定されたログオン・セッションは存在しません。すでに終了している可能性があります。これは、ネットワーク・アクセス・グループ・ポリシー設定を無効にする必要があることが原因で発生します。この GPO を無効にする方法について詳しくは、以下の Microsoft サポートの記事を参照してください: https://support.microsoft.com/en-us/help/968264/error-message-when-you-try-to-map-to-a-network-drive-of-a-dfs-share-by

SQL Server アプリケーション・サーバーの追加

SQL Server アプリケーション・サーバーが追加されると、そのアプリケーション・サーバーに関連付けられているインスタンスおよびデータベースのインベントリーがキャプチャーされ、IBM Spectrum Protect Plus に追加されます。このプロセスにより、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

手順

SQL Server ホストを追加するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**SQL**」 > 「**バックアップ**」をクリックします。
2. 「**アプリケーション・サーバーの管理**」をクリックします。
3. 「**アプリケーション・サーバーの追加**」をクリックします。
4. 「**アプリケーション・プロパティー**」ペインのフィールドにデータを設定します。

   ホスト・アドレス

   解決可能な IP アドレスまたは解決可能なパスとマシン名を入力します。

   既存のユーザーの使用

   プロバイダーについて以前に入力済みのユーザー名とパスワードを選択できます。

   ユーザー ID

   プロバイダーのユーザー名を入力します。仮想マシンがドメインに接続されている場合、ユーザー ID の形式はデフォルトの *domain¥name* です。ユーザーがローカル管理者である場合は、*local _administrator* 形式が使用されます。

   Kerberos ベースの認証の場合に限り、ユーザー ID は username@FQDN 形式で指定する必要があります。完全修飾ドメイン名で指定されたドメイン上の鍵配布センター (KDC) からチケット許可チケット (TGT) を取得するには、登録されたパスワードを使用してユーザー名を認証できる必要があります。

   パスワード

   プロバイダーのパスワードを入力します。

   最大同時データベース数

   サーバーで同時にバックアップするデータベースの最大数を設定します。多数のデータベースを同時にバックアップすると、データのコピー時に各データベースで複数のスレッドが使用され、帯域幅が消費されるため、サーバーのパフォーマンスに影響が及びます。サーバー・リソースに対する影響を制御して、実動操作に対する影響を最小限に抑えるには、このオプションを使用してください。
5. 「**保存**」をクリックします。IBM Spectrum Protect Plus により、ネットワーク接続が確認され、アプリケーション・サーバーが IBM Spectrum Protect Plus データベースに追加され、インスタンスがカタログされます。

   接続が失敗したことを示すメッセージが表示される場合は、項目を確認してください。項目が正確であっても接続が失敗する場合は、システム管理者に連絡して接続を確認してください。

次のタスク

SQL Server アプリケーション・サーバーを追加した後、以下のアクションを実行します。

アクション	方法
アプリケーション・サーバーにユーザー許可を割り当てます。	298 ページの『役割の作成』を参照してください。

関連概念

293 ページの『ユーザー・アクセスの管理』
役割ベースのアクセス制御を使用すると、IBM Spectrum Protect Plus ユーザー・アカウントから使用可能なリソースや許可を設定できます。

関連タスク

222 ページの『SQL Server データのバックアップ』
スナップショットを使用して SQL Server 環境をバックアップするには、バックアップ・ジョブを使用します。

225 ページの『SQL Server データのリストア』

Microsoft SQL Server 環境をスナップショットからリストアするには、リストア・ジョブを使用します。IBM Spectrum Protect Plus インスタント・ディスク・リストア・ジョブを実行した後、SQL Server クローンを即時に使用できます。IBM Spectrum Protect Plus は、すべてのクローン・インスタンスをカタログして追跡します。

SQL Server リソースの検出
SQL Server リソースは、アプリケーション・サーバーが IBM Spectrum Protect Plus に追加されると、自動的に検出されます。 しかし、インベントリー・ジョブを実行すると、アプリケーション・サーバーの追加以降に行われた変更を検出できます。

手順

インベントリー・ジョブを実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**SQL**」 > 「**バックアップ**」をクリックします。
2. SQL Server インスタンスのリストで、インスタンスを選択するか、必要なリソースにナビゲートできるインスタンスのリンクをクリックします。例えば、インスタンス内の個別のデータベースについてインベントリー・ジョブを実行したい場合は、インスタンス・リンクをクリックしてから、仮想マシンを選択してください。
3. 「**インベントリーの実行**」をクリックします。

SQL Server アプリケーション・サーバーへの接続のテスト
SQL Server ホストへの接続をテストすることができます。テスト機能は、ホストとの通信を検証し、IBM Spectrum Protect 仮想アプライアンスとホストとの間で DNS 設定をテストします。

手順

接続をテストするには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**SQL**」 > 「**バックアップ**」をクリックします。
2. 「**アプリケーション・サーバーの管理**」をクリックします。
3. ホストのリストで、そのホスト用の「**アクション**」メニューの「**テスト**」をクリックします。

SQL Server データのバックアップ

スナップショットを使用して SQL Server 環境をバックアップするには、バックアップ・ジョブを使用します。

始める前に

最初の基本バックアップ時に、IBM Spectrum Protect Plus は新規 vSnap ボリュームを作成し、NFS 共有を作成します。増分バックアップ時には、以前に作成したボリュームが再使用されます。 IBM Spectrum Protect Plus エージェントは、バックアップを完了する SQL Server にその共有をマウントします。

バックアップが完了すると、IBM Spectrum Protect Plus エージェントは SQL Server から共有をアンマウントして、バックアップ・ボリュームの vSnap スナップショットを作成します。

以下の情報を確認します。

- IBM Spectrum Protect Plus ユーザーがバックアップおよびリストアの操作を実装できるようにするには、その前に役割グループとリソース・グループをそのユーザーに割り当てる必要があります。「**アカウント**」ペインで、リソースおよびバックアップ/リストア操作へのアクセス権限をユーザーに付与してください。詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。
- Microsoft iSCSI イニシエーターを有効にして、Windows サーバーで実行する必要があります。SQL システムと vSnap サーバーとの間の iSCSI 経路が有効になっている必要があります。詳しくは、を参照してください。Microsoft iSCSI Initiator Step-by-Step Guide.
- 1 つの SQL データベースに対して複数のバックアップ・ジョブでログ・バックアップを構成しないでください。ログは、ログ・バックアップ操作中に切り捨てられます。ログ・バックアップが有効な状態で単一の SQL データベースが複数のジョブ定義に追加されると、あるジョブからのログ・バックアップによ

って、次のジョブでバックアップされる前にログが切り捨てられてしまいます。このため、特定時点リストア・ジョブが失敗する可能性があります。

- IBM Spectrum Protect Plus は、単純リカバリー・モデルのログ・バックアップをサポートしません。
- ログを vSnap にコピーする前に、SPP は SQL サーバー・インスタンス用に構成されたバックアップ・フォルダーをステージング域として使用して、ログを収集します。このフォルダーが配置されるボリュームには、バックアップ・ジョブ間のすべてのトランザクション・ログを保持できるだけの十分なスペースがなければなりません。ステージング域は、SQL Server Management Studio (SSMS) を使用してバックアップ・フォルダー構成を変更することによって変更できます。
- バックアップ時の SQL クラスター・インスタンスのフェイルオーバーはサポートされていません。
- 多数のデータベースのバックアップを予定している場合、バックアップ・ジョブを確実に正常に完了させるには、関連の各 SQL Server インスタンスの最大ワーカー・スレッド数を増やさなければならない場合があります。最大ワーカー・スレッド数のデフォルト値は 0 です。サーバーは、サーバーで使用可能なプロセッサーの数に基づいて、最大ワーカー・スレッド数の値を自動的に決定します。SQL Server は、このプールからのスレッドをネットワーク接続、データベース・チェックポイント、および照会に使用します。さらに、各データベースのバックアップに、このプールからのスレッドが 1 つ追加で必要です。1 つのバックアップ・ジョブに多数のデータベースが含まれている場合、デフォルトの最大ワーカー・スレッド数ではデータベースのすべてをバックアップするには不十分で、ジョブが失敗する可能性があります。最大ワーカー・スレッド数オプションの増加について詳しくは、max worker threads サーバー構成オプションの構成を参照してください。
- 2 次の SQL Always On データベースのログ・バックアップが以下のエラーで失敗した場合は、可用性グループのバックアップ・プリファレンスを「1 次」に変更する必要があります。

```
Log backup for database 'DatabaseName' on a secondary replica failed because a
synchronization point could not be established on the primary database.
```

  プリファレンスを「1 次」に変更すると、1 次レプリカからログがバックアップされます。1 次レプリカのログ・バックアップが正常に完了したら、バックアップ・プリファレンスを変更できます。

次のアクションを実行してください。

- バックアップするプロバイダーを登録します。詳しくは、220 ページの『SQL Server アプリケーション・サーバーの追加』を参照してください。
- SLA ポリシーを構成します。詳しくは、73 ページの『バックアップ・ポリシーの作成』を参照してください。
- SQL バックアップ・ジョブを設定して実行する前に、SQL データベースが配置されているボリュームについてシャドー・コピー・ストレージ設定を構成する必要があります。この設定はボリュームごとに 1 回構成します。ジョブに新規データベースを追加する場合、SQL データベースが含まれているすべての新規ボリュームについて、この設定を構成する必要があります。Windows Explorer で、ソース・ボリュームを右クリックして「**シャドー・コピー**」タブを選択します。ソース・ボリューム・サイズと入出力アクティビティーに応じて、「**最大サイズ**」を「**無制限**」 または妥当なサイズに設定し、「**OK**」をクリックします。シャドー・コピー・ストレージ域は、同じボリューム上にあるか、またはバックアップ時に使用可能な別のボリューム上になければなりません。

手順

SQL バックアップ・ジョブを定義するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**SQL**」をクリックします。
2. バックアップする SQL Server インスタンスを選択します。

   検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えます。使用可能なオプションは、「**スタンドアロン/フェイルオーバー・クラスター**」と「**Always On**」です。
3. 「**SLA ポリシーの選択**」をクリックして、バックアップ・データ基準に適合する 1 つ以上の SLA ポリシーをジョブ定義に追加します。
4. デフォルト・オプションを使用してジョブ定義を作成するには、「**保存**」をクリックします。

ジョブは、選択した SLA ポリシーで定義されたとおりに実行されます。ジョブを手動で実行するには、「**ジョブと操作**」 > 「**スケジュール**」をクリックします。ジョブを選択して、「**アクション**」 > 「**開始**」をクリックします。

ヒント:「**実行**」ボタンは単一のデータベース・バックアップについてのみ有効であり、該当のデータベースに SLA ポリシーが適用されている必要があります。

5. ジョブ定義を作成する前にオプションを編集するには、「**オプションの選択**」をクリックします。ジョブ定義オプションを設定してください。

   ログ・バックアップの有効化

   IBM Spectrum Protect Plus を有効にしてトランザクション・ログをバックアップし、基礎となるディスクを保護する場合に選択します。

   IBM Spectrum Protect Plus は、バックアップ対象のデータベースのポスト・ログ・バックアップを自動的に切り捨てます。データベース・ログのバックアップを IBM Spectrum Protect Plus で行っていない場合は、ログは IBM Spectrum Protect Plus では切り捨てられないため、別個に管理する必要があります。

   ログ・バックアップが有効になっていて SQL バックアップ・ジョブが完了すると、ジョブ完了時点までのすべてのトランザクション・ログは SQL Server サーバーからパージされます。ログ・パージは、SQL バックアップ・ジョブが正常に完了した場合にのみ発生します。ジョブの再実行時にログ・バックアップが無効になっていると、ログ・パージは発生しません。

   ソース・データベースが上書きされると、そのポイントまでの古いトランザクション・ログはすべて、オリジナル・データベースの回復が完了すると同時に「圧縮」ディレクトリーに置かれます。SQL バックアップ・ジョブの次回の実行が完了すると、圧縮フォルダーの内容は削除されます。

   ログ・バックアップを完了するには、SQL Server エージェント・サービス・ユーザーはローカル Windows 管理者でなければならず、SQL Server のエージェント・ジョブを管理するために有効化された sysadmin 許可を持っている必要があります。エージェントは、その管理者アカウントを使用してログ・バックアップ・ジョブを有効にしてそれにアクセスします。IBM Spectrum Protect Plus SQL Server エージェント・サービス・ユーザーは、保護対象のすべての SQL Server インスタンスの SQL Server サービスおよび SQL Server エージェント・サービスのアカウントと同じユーザーである必要があります。

   SQL ログ・ファイルは、CIFS 共有にコピーされる前に、ローカル・ステージング域に一時的に保管されます。SQL サーバーのデフォルトのバックアップ宛先はステージング域としての機能を果たします。そのため、トランザクション・ログ・ファイルを CIFS 共有にコピーする前にそれらのファイルを保管するための十分なフリー・スペースを備えている必要があります。

   同じ SQL Server インスタンスに複数のデータベース用のログ・バックアップ・スケジュールを作成できるようにするには、すべてのデータベースを必ず同じ SLA ポリシーに追加してください。

   このオプションを選択した場合、SQL リストア操作に特定時点リストア・オプションを使用できます。

   データベースごとの最大並列ストリーム数

   バックアップ・ストレージへのデータベースごとの最大データ・ストリームを設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を「**1**」 に設定すると、複数のデータベースのバックアップを並列に実行できます。複数の並列ストリームでバックアップ速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体のシステム・パフォーマンスに影響を与えることがあります。

6. ジョブ固有の情報が正しいことを確認したら、「**保存**」をクリックします。

   ジョブは、SLA ポリシーで定義されたとおりに実行されます。あるいは、ジョブ・モニター・ペインから手動で実行することもできます。

7. 追加オプションを構成するには、「**SLA ポリシー状況**」セクションでジョブと関連付けられている「**ポリシー・オプション**」をクリックします。以下の追加のポリシー・オプションを設定します。

   事前スクリプトと事後スクリプト

   事前スクリプトまたは事後スクリプトを実行します。事前スクリプトと事後スクリプトは、ジョブの実行の前または後に実行できるスクリプトです。バッチ・スクリプトと PowerShell スクリプトがサポートされます。

「**事前スクリプト**」セクションまたは「**事後スクリプト**」セクションで、アップロード済みのスクリプトと、そのスクリプトを実行するアプリケーション・サーバーまたはスクリプト・サーバーを選択してください。スクリプトを実行するアプリケーション・サーバーを選択するには、「**スクリプト・サーバーを使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成します。

ジョブに関連付けられたスクリプトが失敗した場合でもジョブを続行するには、「**スクリプト・エラーの場合もジョブ/タスクを続行**」を選択します。

このオプションを有効にすると、事前スクリプトまたは事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、バックアップ操作またはリストア操作が試行され、事前スクリプト・タスク状況は「完了」と報告されます。事後スクリプトがゼロ以外の戻りコードで完了した場合、事後スクリプト・タスク状況は「完了」と報告されます。

このオプションを無効にすると、バックアップまたはリストアは試行されず、事前スクリプトまたは事後スクリプトのタスク状況は「失敗」と報告されます。

リソースの除外

単一または複数の除外パターンを使用して、バックアップ・ジョブから特定のリソースを除外します。リソースを除外するには、完全一致を使用するか、あるいは、パターンの前 (*test) またはパターンの後 (test*) ワイルドカード・アスタリスクを指定します。

単一パターン内で複数のアスタリスク・ワイルドカードを指定することもできます。パターンでは、標準の英数字のほか、特殊文字 -、_、および * を使用できます。

複数のフィルターはセミコロンで区切ります。

リソースのフルバックアップを 強制します

バックアップ・ジョブ定義内にある特定の仮想マシンまたはデータベースへの基本バックアップ操作を強制的に実行します。複数のリソースはセミコロンで区切ります。

8. 構成した追加オプションを保存するには、「**保存**」をクリックします。

次のタスク

バックアップ・ジョブ定義を作成した後、以下のアクションを実行してください。

アクション	ハウツー
SQL リストア・ジョブ定義を作成する。	225 ページの『SQL Server データのリストア』を参照してください。

関連概念

250 ページの『バックアップ操作とリストア操作のスクリプトの構成』
事前スクリプトと事後スクリプトは、バックアップ・ジョブとリストア・ジョブがジョブ・レベルで実行される前または後に実行できるスクリプトです。サポートされるスクリプトには、Linux ベースのマシン用のシェル・スクリプトや、Windows ベースのマシン用の Batch および PowerShell スクリプトがあります。スクリプトはローカル側で作成され、「**スクリプト**」ページを使用して環境にアップロードされてから、ジョブ定義に適用されます。

関連タスク

248 ページの『ジョブの開始』
いずれのジョブも、スケジュールで実行するよう設定されている場合でも、オンデマンドで実行できます。

SQL Server データのリストア

Microsoft SQL Server 環境をスナップショットからリストアするには、リストア・ジョブを使用します。IBM Spectrum Protect Plus インスタント・ディスク・リストア・ジョブを実行した後、SQL Server クローンを即時に使用できます。IBM Spectrum Protect Plus は、すべてのクローン・インスタンスをカタログして追跡します。

始める前に

以下の前提条件をすべて満たしてください。

- SQL バックアップ・ジョブを作成して実行します。手順については、222 ページの『SQL Server データのバックアップ』を参照してください。
- IBM Spectrum Protect Plus ユーザーがデータをリストアできるようにするには、その前に、そのユーザーに適切な役割とリソース・グループを割り当てる必要があります。「**アカウント**」ペインを使用して、リソースおよびバックアップ/リストア操作へのアクセス権限をユーザーに付与してください。手順については、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。
- 特定時点リカバリーを実行する予定の場合は、リストア・ターゲットの SQL インスタンス・サービスと IBM Spectrum Protect Plus SQL Server サービスの両方で、必ず同じユーザー・アカウントを使用してください。

以下の制約事項と考慮事項を確認してください。

- SQL Server フェイルオーバー・クラスターへの実動リストア操作を実行する予定の場合は、代替ファイル・パスのルート・ボリュームをホスト・データベースとログ・ファイルで使用できる必要があります。このボリュームは、宛先 SQL Server のクラスター・サーバー・リソース・グループに属していて、SQL Server クラスター・サーバーに従属している必要があります。
- SQL Server データベースの制約事項により、NTFS または FAT の圧縮ボリュームにデータをリストアすることはできません。詳しくは、Description of support for SQL Server databases on compressed volumes を参照してください。
- 代替ロケーションにデータをリストアする 予定の場合は、SQL Server 宛先で SQL Server の同じバージョンまたはそれ以降のバージョンを実行している必要があります。詳しくは、Compatibility Support を参照してください。
- SQL Always On 可用性グループ環境で 1 次インスタンスをデータをリストアすると、データベースはターゲットの Always On データベース・グループに追加されます。自動シードがサポートされる環境 (Microsoft SQL Server 2016 以降) では、1 次リストア操作の後で SQL Server によって 2 次データベースがシードされます。その後、このデータベースは宛先可用性グループで有効になります。同期時間は、転送されるデータの量と 1 次レプリカと 2 次レプリカの間の接続に応じて異なります。

  自動シードがサポートされていないか有効になっていない場合は、1 次インスタンスのログ・シーケンス番号 (LSN) のギャップが最も短いリストア・ポイントからの 2 次リストアを実行する必要があります。1 次インスタンスでログ・バックアップが有効になっていた場合は、IBM Spectrum Protect Plus によって作成された最新の特定時点リストア・ポイントを使用してログ・バックアップをリストアする 必要があります。2 次データベースのリストア操作は「リストア」状態で完了します。ユーザーは、**T-SQL** コマンドを使用してデータベースをターゲット・グループに追加する必要があります。詳しくは、Transact-SQL リファレンス (データベース・エンジン)を参照してください。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

このタスクについて

インスタント・ディスク・リストアでは、iSCSI プロトコルを使用して、データを転送せずに LUN を即時にマウントします。 スナップショットが作成されたデータベースがカタログされ、即時にリカバリー可能になります。データの物理的転送は行われません。

以下のリストア・モードがサポートされています。

インスタント・アクセス・モード
インスタント・アクセス・モードでは、共有をマウントした後、それ以上のアクションは実行されません。ユーザーは、vSnap ボリューム内のファイルを使用して任意のカスタム・リカバリーを実行できます。Always On データベースのインスタント・アクセス・リストアでは、ローカル宛先インスタンスにリストアされます。

テスト・モード
テスト・モードでは、エージェントは vSnap ボリュームからデータ・ファイルを直接使用して新規データベースを作成します。

実動モード

実動モードでは、エージェントはまず vSnap ボリュームから 1 次ストレージにファイルをリストアし、次にそのリストアされたファイルを使用して新規データベースを作成します。

手順

SQL リストア・ジョブを定義するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**SQL**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント：

   - 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**SQL**」をクリックして開くこともできます。
   - 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
   - ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。

2. 「**ソースの選択**」ページで、以下のアクションを実行します。

   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。「**表示**」フィルターを使用して、表示されるソースを切り替え、スタンドアロン環境またはクラスター環境、あるいは Always On 可用性グループのいずれかの SQL Server インスタンスを表示することができます。

   検索機能を使用して、インスタンスまたは可用性グループ内のデータベースを検索することもできます。

   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。複数のデータベースをリストから選択できます。

   選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リスト・ソースから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。

   c) 「**次へ**」をクリックして先に進みます。

3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。いくつかのフィールドは、関連フィールドを選択するまで表示されません。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。

オプション	説明
	クラウド・オフロード スナップショットがオフロードされたクラウド・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・リストア操作の場合は、日付の範囲を指定すると、その日付範囲内で使用可能なスナップショットが表示されます。
リストア・ポイント	オンデマンド・リストア操作の場合は、選択した日付範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、データベースをリストアする場所を指定して、「**次へ**」をクリックします。

   オリジナル・インスタンスにリストアします
   元のインスタンスにデータベースをリストアするには、このオプションを選択します。

   1 次インスタンスにリストアします
   SQL Always On 環境でリストア操作を実行する場合に、Always On 可用性グループの 1 次インスタンスにデータベースをリストアするには、このオプションを選択します。データベースは元のグループに追加されます。

代替インスタンスにリストアします
オリジナル・インスタンスとは異なるローカル宛先にデータベースをリストアするには、このオプションを選択します。その後、使用可能なサーバーのリストから代替ロケーションを選択します。

テスト・モードの SQL Always On 環境でのリストア操作の場合、選択されたターゲット・インスタンスにソースの可用性データベースがリストアされます。

実動モードの SQL Always On 環境でのリストア操作では、宛先インスタンスが 1 次レプリカである場合、リストアされたデータベースはターゲットの 可用性グループに追加されます。宛先インスタンスがターゲット可用性グループの 2 次レプリカである場合、データベースは 2 次レプリカにリストアされ、リストア中の状態のままになります。

宛先可用性グループで自動シード・オプションが有効になっている場合は、2 次データベース・ファイル・パスが 1 次データベースと同期されます。1 次データベース・ログが切り捨てられなければ、2 次データベースが SQL によって可用性グループに追加される場合があります。

5. 「**リストア方式**」ページで、テスト・モード、実動モード、またはインスタント・アクセス・モードでリストア・ジョブをデフォルトで実行するように設定します。

   テスト・モードまたは実動モードの場合、オプションで、リストアされるデータベースの新規名を入力できます。

   実動モードの場合は、データベースを展開して新規フォルダー名を入力することで、リストアされるデータベース用に新規フォルダーを指定できます。

   「**次へ**」をクリックして先に進みます。

   ジョブが作成された後、「**ジョブ・セッション**」ペインで、そのジョブをテスト・モード、実動モード、またはインスタント・アクセス・モードで実行できます。

6. 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   リカバリー・オプション
   以下の特定時点リカバリー・オプションを設定します。

   リカバリーなし
   選択済みのデータベースを「リストア中」の状態にします。IBM Spectrum Protect Plus を使用せずにトランザクション・ログ・バックアップを管理している場合、2 次と 1 次のデータベース・コピーの LSN が基準を満たしていれば、手動でログ・ファイルをリストアし、データベースを可用性グループに追加することができます。

   制約事項 : 「**リカバリーなし**」オプションでは、SQL Always On グループへの実動モードのリストア操作はサポートされません。

   バックアップの最後までリカバリーします
   選択されたデータベースをバックアップの 作成時の状態にリストアします。

   特定時点までリカバリーします
   SQL バックアップ・ジョブ定義を使用してログ・バックアップを有効にしている場合、SQL リストア・ジョブ定義の作成時に特定時点リストア・オプションを選択できます。以下のオプションのいずれかを選択してください。

   - **時刻別**。特定の日時からの特定時点リカバリーを構成するには、このオプションを選択します。
   - **トランザクション ID 別**。トランザクション ID 別に特定時点リカバリーを構成するには、このオプションを選択します。

   スタンドアロン・リストア操作では、IBM Spectrum Protect Plus は、選択された特定時点の直前および直後のリストア・ポイントを検出します。リカバリーの実行中は、古いデータ・バックアップ・ボリュームと新しいログ・バックアップ・ボリュームがマウントされています。特定時点が最後のバックアップ操作より後である場合は、一時的なリストア・ポイントが作成されます。

   テスト・モードの SQL Always On 環境でリストア操作を実行する場合、リストアされるデータベースは、可用性グループが常駐しているインスタンスに結合されます。

実動モードの SQL Always On 環境でリストア操作を実行する場合、リストアされる 1 次データベースは可用性グループに結合されます。宛先可用性グループで自動シード・オプションが有効になっている場合は、2 次データベース・ファイル・パスが 1 次データベースと同期されます。1 次データベース・ログが切り捨てられなければ、2 次データベースが SQL によって可用性グループに追加される場合があります。

アプリケーション・オプション
以下のアプリケーション・オプションを設定します。

既存のデータベースを上書きします
選択済みデータベースをリストア・ジョブが上書きできるようにします。デフォルトでは、このオプションは有効ではありません。

ヒント : 実動モードで「**既存のデータベースを上書きする**」オプションを指定して SQL Always On 環境でリストア操作を実行する前に、該当のデータベースがターゲット可用性グループのレプリカに含まれていないことを使用可能 environment by using the production mode with the option, 確認してください。この操作をする場合は、ターゲット可用性グループのすべてのレプリカから、手動でオリジナル・データベース (上書き対象) をクリーンアップする必要があります。

データベースごとの最大並列ストリーム数
バックアップ・ストレージからのデータベースごとの並列データ・ストリームの最大数を設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値が 1 に設定される場合でも、複数のデータベースを並列にリストアできます。複数の並列ストリームによってリストア速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

このオプションは、SQL Server データベースを元のデータベース名を使用してオリジナル・ロケーションにリストアする場合にのみ適用可能です。

高度なオプション
以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
リカバリーが失敗した場合、リストア操作の一部として、割り振り済みのリソースを自動的にクリーンアップします。

セッションの上書きを許可します
リカバリー時に既存のデータベースを同じ名前のデータベースで置き換える場合は、このオプションを選択します。インスタント・ディスク・リストアをデータベースに対して実行したときに、同じ名前のデータベースが宛先のホストまたはクラスターで既に実行中になっていた場合、IBM Spectrum Protect Plus は、既存のデータベースをシャットダウンしてからリカバリー済みデータベースを始動します。このオプションを選択していない場合、IBM Spectrum Protect Plus が同じ名前で実行中のデータベースを検出すると、リストア・ジョブは失敗します。

いずれかが失敗しても、ほかのデータベースのリストアを続行します
直前のリソース・リカバリーが失敗した場合、シリーズ内のリソースのリカバリーを切り替えます。このオプションが有効になっていない場合、リソースのリカバリーが失敗すると、リストア・ジョブは停止します。

「**プロトコルの優先度**」**(インスタント・アクセスの場合のみ)**
複数のストレージ・プロトコルが使用可能な場合、ジョブで優先するプロトコルを選択します。選択可能なプロトコルは、「**iSCSI**」および「**ファイバー・チャネル**」です。

マウント・ポイント接頭部
インスタント・アクセス・リストア操作の場合に、マウント・ポイントの送信先パスの接頭部を指定します。

7. オプション: 「**スクリプトの適用**」ページで、操作の実行前または実行後にジョブ・レベルで実行できるスクリプトを指定します。バッチ・スクリプトと PowerShell スクリプトがサポートされます。

事前スクリプト
アップロードされたスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このチェック・ボックスを選択します。事前スクリプトが実行されるアプリケーション・サーバーを選択するには、「**スクリプト・サーバーの使用**」チ

ェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成します。

事後スクリプト
アップロードされたスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このオプションを選択します。事後スクリプトが実行されるアプリケーション・サーバーを選択するには、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成します。

スクリプト・エラー時にジョブ/タスクを続行
ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、このチェック・ボックスを選択します。

このチェック・ボックスを選択すると、事前スクリプトまたは事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、バックアップ操作またはリストア操作が試行され、事前スクリプト・タスク状況は「完了」と報告されます。事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、事後スクリプト・タスク状況は「完了」と報告されます。

このチェック・ボックスをクリアすると、バックアップ操作またはリストア操作は試行されず、事前スクリプトまたは事後スクリプトのタスク状況は「失敗」と報告されます。

8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。

タスクの結果

「**実行**」をクリックした後でオンデマンド・ジョブが始まるとまもなく、「**onDemandRestore**」レコードが「**ジョブ・セッション**」ペインに追加されます。リストア操作の進行状況を表示するには、ジョブを展開します。ダウンロード・アイコン  をクリックして、ログ・ファイルをダウンロードすることもできます。

「**ジョブと操作**」 > 「**スケジュール**」ページでスケジュールを開始すると、スケジュールされた開始時刻に反復ジョブが始まります。

実行中のジョブはすべて、「**ジョブと操作**」 > 「**実行中のジョブ**」ページで表示できます。

関連概念

250 ページの『バックアップ操作とリストア操作のスクリプトの構成』
事前スクリプトと事後スクリプトは、バックアップ・ジョブとリストア・ジョブがジョブ・レベルで実行される前または後に実行できるスクリプトです。サポートされるスクリプトには、Linux ベースのマシン用のシェル・スクリプトや、Windows ベースのマシン用の Batch および PowerShell スクリプトがあります。スクリプトはローカル側で作成され、「**スクリプト**」ページを使用して環境にアップロードされてから、ジョブ定義に適用されます。

関連タスク

220 ページの『SQL Server アプリケーション・サーバーの追加』
SQL Server アプリケーション・サーバーが追加されると、そのアプリケーション・サーバーに関連付けられているインスタンスおよびデータベースのインベントリーがキャプチャーされ、IBM Spectrum Protect Plus に追加されます。このプロセスにより、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

222 ページの『SQL Server データのバックアップ』

スナップショットを使用して SQL Server 環境をバックアップするには、バックアップ・ジョブを使用します。

Oracle データのバックアップとリストア

Oracle のコンテンツを保護するために、IBM Spectrum Protect Plus が Oracle インスタンスを認識するように最初にそのインスタンスを登録します。次に、バックアップ操作およびリストア操作用のジョブを作成します。

ご使用の Oracle 環境が 35 ページの『Oracle 要件』 のシステム要件を満たしていることを確認してください。

Oracle アプリケーション・サーバーの追加

Oracle アプリケーション・サーバーが追加されると、そのアプリケーション・サーバーに関連付けられているインスタンスおよびデータベースのインベントリーがキャプチャーされ、IBM Spectrum Protect Plus に追加されます。このプロセスにより、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

手順

Oracle アプリケーション・サーバーを登録するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Oracle**」 > 「**バックアップ**」をクリックします。
2. 「**アプリケーション・サーバーの管理**」をクリックします。
3. 「**アプリケーション・サーバーの追加**」をクリックして、ホスト・マシンを追加します。
4. 「**アプリケーション・プロパティー**」ペインにホスト・アドレスを入力します。
   ホスト・アドレスは、解決可能な IP アドレスまたは解決可能なパスとマシン名です。
5. 「**ユーザー**」または「**SSH 鍵**」を選択します。

オプション	説明
ユーザー	このオプションをクリックして既存のユーザーを指定するか、ユーザー ID とパスワードを入力します。ユーザーには、**sudo** 特権がセットアップされている必要があります。以下のようにして、フィールドに入力します。 **既存のユーザーの使用** アプリケーション・サーバーについて以前に入力済みのユーザー名とパスワードを使用するには、このチェック・ボックスを選択します。「**ユーザーの選択**」リストでユーザーを選択します。 **ユーザー ID** アプリケーション・サーバーのユーザー名を入力します。仮想マシンがドメインに接続される場合、ユーザー ID はデフォルトの *domain¥name* 形式に従います。ユーザーがローカル管理者の場合は、*local_administrator* 形式を使用します。 Kerberos ベースの認証の場合に限り、ユーザー ID は username@FQDN 形式で指定する必要があります。完全修飾ドメイン名で指定されたドメイン上の鍵配布センター (KDC) からチケット許可チケット (TGT) を取得するには、登録されたパスワードを使用してユーザー名を認証できる必要があります。 **パスワード** アプリケーション・サーバーのパスワードを入力します。
SSH 鍵	SSH 鍵を使用するには、このオプションをクリックします。「**SSH 鍵を選択します**」リストから鍵を選択します。

6. Oracle 12c 以降のバージョンでマルチスレッド・データベースを保護するには、データベースの資格情報を指定します。

a)「**データベースを取得します**」をクリックして、ホスト・サーバー上にある、追加する Oracle データベースを検出してリストします。

各 Oracle データベースは、その名前、状況、およびデータベースについて資格情報が以前に指定されているかどうかの指標と共にリストされます。

b) 保護するマルチスレッド・データベースごとに、「**資格情報を設定**」をクリックして、ユーザー ID とパスワードを指定します。あるいは、「**ユーザーの選択**」リストから既存のユーザーを選択できます。

SYSDBA 特権を持つ Oracle データベース・ユーザーの資格情報を指定する必要があります。

7.「**最大同時データベース数**」で、サーバーで同時にバックアップするデータベースの最大数を設定します。

多数のデータベースを同時にバックアップすると、データのコピー時に各データベースで複数のスレッドが使用され、帯域幅が消費されるため、サーバーのパフォーマンスに影響が及びます。サーバー・リソースに対する影響を制御して、実動操作に対する影響を最小限に抑えるには、このオプションを使用してください。

8.「**保存**」をクリックします。IBM Spectrum Protect Plus により、ネットワーク接続が確認され、アプリケーション・サーバーが IBM Spectrum Protect Plus データベースに追加され、インスタンスがカタログされます。

接続が失敗したことを示すメッセージが表示される場合は、項目を確認してください。項目が正確であっても接続が失敗する場合は、システム管理者に連絡して接続を確認してください。

次のタスク

Oracle アプリケーション・サーバーを追加した後、以下のアクションを実行します。

アクション	方法
アプリケーション・サーバーにユーザー許可を割り当てます。	298 ページの『役割の作成』を参照してください。

関連概念

293 ページの『ユーザー・アクセスの管理』
役割ベースのアクセス制御を使用すると、IBM Spectrum Protect Plus ユーザー・アカウントから使用可能なリソースや許可を設定できます。

関連タスク

234 ページの『Oracle データのバックアップ』
スナップショットを使用して Oracle 環境をバックアップするには、バックアップ・ジョブを使用します。

237 ページの『Oracle データのリストア』
Oracle 環境をスナップショットからリストアするには、リストア・ジョブを使用します。IBM Spectrum Protect Plus は、ジョブ定義の作成時に選択されたバージョンから vSnap クローンを作成してネットワーク・ファイル・システム (NFS) 共有を作成します。IBM Spectrum Protect Plus エージェントは、リストア・ジョブを実行する Oracle サーバーにその共有をマウントします。Oracle Real Application Clusters (RAC) の場合は、リストア・ジョブはクラスター内のすべてのノード上で実行されます。

Oracle リソースの検出

Oracle リソースは、アプリケーション・サーバーが IBM Spectrum Protect Plus に追加されると、自動的に検出されます。しかし、インベントリー・ジョブを実行すると、アプリケーション・サーバーの追加以降に行われた変更を検出できます。

手順

インベントリー・ジョブを実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Oracle**」 > 「**バックアップ**」をクリックします。
2. Oracle インスタンスのリストで、インスタンスを選択するか、必要なリソースにナビゲートできるインスタンスのリンクをクリックします。例えば、インスタンス内の個別のデータベースについてインベントリー・ジョブを実行したい場合は、インスタンス・リンクをクリックしてから、仮想マシンを選択してください。

3.「**インベントリーの実行**」をクリックします。

Oracle アプリケーション・サーバーへの接続のテスト

Oracle ホストへの接続をテストすることができます。テスト機能は、ホストとの通信を検証し、IBM Spectrum Protect 仮想アプライアンスとホストとの間で DNS 設定をテストします。

手順

接続をテストするには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Oracle**」 > 「**バックアップ**」をクリックします。
2.「**アプリケーション・サーバーの管理**」をクリックします。
3. ホストのリストで、そのホスト用の「**アクション**」メニューの「**テスト**」をクリックします。

Oracle データのバックアップ

スナップショットを使用して Oracle 環境をバックアップするには、バックアップ・ジョブを使用します。

始める前に

以下の情報を確認します。

- IBM Spectrum Protect Plus が Oracle データをサーバー間で移動するときにファイル・システム権限が正しく保持されていることを確認するには、Oracle ユーザー (例えば、oracle、oinstall、dba) のユーザーとグループの ID がすべてのサーバーで一貫していることを確認してください。推奨される uid と gid の値については、Oracle 資料を参照してください。
- Oracle インベントリー・ジョブが Oracle バックアップ・ジョブと同時またはその直後に実行される場合、バックアップ・ジョブ中に一時マウントが作成されているためにコピー・エラーが発生することがあります。ベスト・プラクティスとして、Oracle インベントリー・ジョブを Oracle バックアップ・ジョブと重ならないようにスケジュールに入れてください。
- 複数のバックアップ・ジョブを使用して単一の Oracle データベースのログ・バックアップを構成しないでください。ログ・バックアップが有効な状態で単一の Oracle データベースが複数のジョブ定義に追加されると、あるジョブからのログ・バックアップにより、次のジョブでバックアップされる前にログが切り捨てられる可能性があります。このため、特定時点リストア・ジョブが失敗する可能性があります。
- 選択した特定時点から先回のバックアップ・ジョブが実行された時点までの期間に 1 つ以上のデータ・ファイルがデータベースに追加されている場合には、特定時点リカバリーはサポートされません。

次のアクションを実行してください。

- IBM Spectrum Protect Plus ユーザーがバックアップとリストアの操作を実装するには、その前に、そのユーザーに役割とリソース・グループを割り当てる必要があります。「**アカウント**」ペインで、リソースおよびバックアップとリストアの操作に対するアクセス権限をユーザーに付与します。詳しくは、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。
- バックアップするプロバイダーを登録します。詳しくは、232 ページの『Oracle アプリケーション・サーバーの追加』を参照してください。
- SLA ポリシーを構成します。詳しくは、73 ページの『バックアップ・ポリシーの作成』を参照してください。

このタスクについて

最初の基本バックアップ時に、IBM Spectrum Protect Plus は vSnap ボリュームおよび NFS 共有を作成します。増分バックアップ時には、以前に作成されたボリュームが再使用されます。IBM Spectrum Protect Plus エージェントは、バックアップが実行される Oracle サーバーに共有をマウントします。

Oracle Real Application Clusters (RAC) の場合は、バックアップは、クラスター内の任意の 1 つノードから実行されます。バックアップが完了すると、IBM Spectrum Protect Plus エージェントは、Oracle サーバーから共有をアンマウントして、バックアップ・ボリュームの vSnap スナップショットを作成します。

Oracle 12c 以降のバージョンでは、IBM Spectrum Protect Plus はマルチスレッド・データベースを保護できます。IBM Spectrum Protect Plus でマルチスレッド・データベースを保護できるようにする手順については、232 ページの『Oracle アプリケーション・サーバーの追加』を参照してください。

手順

Oracle バックアップ・ジョブを定義するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Oracle**」をクリックします。
2. バックアップする Oracle ホーム、データベース、および ASM ディスク・グループを選択します。検索機能を使用して使用可能なインスタンスを検索します。
3. 「**SLA ポリシーの選択**」をクリックして、バックアップ・データ基準に適合する 1 つ以上の SLA ポリシーをジョブ定義に追加します。
4. デフォルトのオプションを使用してジョブ定義を作成するには、「**保存**」をクリックします。

   ジョブは、選択した SLA ポリシーで定義されたとおりに実行されます。ジョブを手動で実行するには、「**ジョブと操作**」 > 「**スケジュール**」をクリックします。ジョブを選択して、「**アクション**」 > 「**開始**」をクリックします。

   ヒント:「**実行**」ボタンは単一のデータベース・バックアップについてのみ有効であり、該当のデータベースに SLA ポリシーが適用されている必要があります。
5. ジョブ定義を作成する前にオプションを編集するには、「**オプションの選択**」をクリックします。ジョブ定義オプションを設定します。

   ログ・バックアップを有効にします

   Oracle の特定時点リストアを実行できるようにするには、「**ログ・バックアップを有効にする**」を選択する必要があります。

   IBM Spectrum Protect Plus がログ・バックアップ・ボリュームを自動的に作成してアプリケーション・サーバーにマウントすることを許可するには、「**ログ・バックアップを有効にします**」を選択します。IBM Spectrum Protect Plus は、その後、既存の 1 次アーカイブ・ログの場所を検出し、cron を使用してスケジュール・ジョブを構成します。スケジュール・ジョブでは、「**頻度**」設定で指定された頻度で、1 次ロケーションからそのログ・バックアップ・ボリュームへのトランザクション・ログ・バックアップが実行されます。

   「**頻度**」は、「SLA ポリシー」設定に指定されたデータベース・バックアップの頻度とは関係のない値に設定できます。例えば、「SLA ポリシー」はデータベースを 1 日に 1 回バックアップするように構成して、ログ・バックアップの頻度は 30 分ごとに 1 回に設定することができます。

   Oracle RAC の場合は、IBM Spectrum Protect Plus は、ボリュームをマウントして、各クラスター・ノードで cron ジョブを構成します。スケジュールがトリガーされると、ジョブにより、いずれか 1 つのアクティブ・ノードがログ・バックアップを実行している間に他のノードが何もアクションを実行しないように内部的に調整されます。

   IBM Spectrum Protect Plus は、SLA ポリシーの保存設定に基づいて独自のログ・バックアップ・ボリューム内のログの保存を自動的に管理します。

   データベースの 1 次アーカイブ・ログ・ロケーションから古いアーカイブ・ログを自動的に削除するには、「**バックアップの正常終了後、ソース・ログを切り捨てる**」を選択します。このオプションが選択解除されても、1 次ログ宛先のアーカイブ・ログは削除されないため、データベース管理者は既存のログ保存ポリシーを使用してこれらのログを継続的に管理する必要があります。このオプションが選択される場合、IBM Spectrum Protect Plus は、データベース・バックアップが正常に終了するたびに 1 次ログ・ロケーションから不要なアーカイブ・ログを削除します。

   オプション「**バックアップの正常終了後、ソース・ログを切り捨てます**」を選択する場合は、「**1 次ログの保存日数**」設定を使用して 1 次ログの保存を設定します。この設定により、1 次アーカイブ・ログ・ロケーションに保存されるアーカイブ・ログの数量が制御されます。例えば、「**1 次ログの保存日数**」が **3** に設定される場合、IBM Spectrum Protect Plus は、データベース・バックアップが正常に終了するたびに、3 日を経過したアーカイブ・ログをすべて 1 次アーカイブ・ログ・ロケーションから削除します。

   データベースごとの最大並列ストリーム数

バックアップ・ストレージへのデータベースごとの最大データ・ストリームを設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値を「**1**」に設定すると、複数のデータベースのバックアップを並列に実行できます。複数の並列ストリームでバックアップ速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体のシステム・パフォーマンスに影響を与えることがあります。

6. ジョブ固有の情報が正しいことを確認したら、「**保存**」をクリックします。
7. 追加のオプションを構成するには、「**SLA ポリシーのステータス**」セクションで、ジョブに関連付けられている「**ポリシー・オプション**」フィールドをクリックします。追加のポリシー・オプションを設定します。

   事前スクリプトと事後スクリプト

   事前スクリプトまたは事後スクリプトを実行します。事前スクリプトおよび事後スクリプトは、ジョブの実行前または実行後にジョブ・レベルで実行できるスクリプトです。Windows ベースのマシンはバッチ・スクリプトと PowerShell スクリプトをサポートし、Linux ベースのマシンはシェル・スクリプトをサポートします。

   「**事前スクリプト**」セクションまたは「**事後スクリプト**」セクションで、アップロード済みのスクリプトと、スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択します。スクリプトが実行されるアプリケーション・サーバーを選択する場合は、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーは、「**システム構成**」 > 「**スクリプト**」ページで構成されます。

   ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、「**スクリプト・エラー時にジョブ/タスクを続行**」を選択します。

   このオプションが有効になっている場合、事前スクリプトまたは事後スクリプトの処理がゼロ以外の戻りコードで完了すると、バックアップまたはリストアの操作は試行され、事前スクリプト・タスクの状況は「完了」として報告されます。事後スクリプトがゼロ以外の戻りコードで完了すると、事後スクリプト・タスクの状況は「完了」として報告されます。

   このオプションが無効になっている場合は、バックアップまたはリストアは試行されず、事後スクリプトまたは事後スクリプトのタスク状況は「失敗」として報告されます。

   リソースの除外

   単一または複数の除外パターンを使用して、特定のリソースをバックアップ・ジョブから除外します。リソースを除外するには、完全一致を使用するか、あるいは、パターンの前 (*test) またはパターンの後 (test*) にワイルドカード・アスタリスクを指定します。

   単一パターン内で複数のアスタリスク・ワイルドカードを指定することもできます。パターンでは、標準の英数字のほか、特殊文字 -、_、および * を使用できます。

   複数のフィルターはセミコロンで区切ります。

   リソースのフルバックアップを 強制します

   バックアップ・ジョブ定義の特定の仮想マシンまたはデータベースに対して基本バックアップ操作を強制的に実行します。複数のリソースはセミコロンで区切ります。

次のタスク

バックアップ・ジョブ定義を作成した後、以下のアクションを実行します。

アクション	方法
Oracle リストア・ジョブ定義を作成します。	237 ページの『Oracle データのリストア』を参照してください。

関連概念

250 ページの『バックアップ操作とリストア操作のスクリプトの構成』

事前スクリプトと事後スクリプトは、バックアップ・ジョブとリストア・ジョブがジョブ・レベルで実行される前または後に実行できるスクリプトです。サポートされるスクリプトには、Linux ベースのマシン用のシェル・スクリプトや、Windows ベースのマシン用の Batch および PowerShell スクリプトがあります。

スクリプトはローカル側で作成され、「**スクリプト**」ページを使用して環境にアップロードされてから、ジョブ定義に適用されます。

Oracle データのリストア

Oracle 環境をスナップショットからリストアするには、リストア・ジョブを使用します。IBM Spectrum Protect Plus は、ジョブ定義の作成時に選択されたバージョンから vSnap クローンを作成してネットワーク・ファイル・システム (NFS) 共有を作成します。IBM Spectrum Protect Plus エージェントは、リストア・ジョブを実行する Oracle サーバーにその共有をマウントします。Oracle Real Application Clusters (RAC) の場合は、リストア・ジョブはクラスター内のすべてのノード上で実行されます。

始める前に

以下の前提条件をすべて満たしてください。

- Oracle バックアップ・ジョブの作成および実行。手順については、234 ページの『Oracle データのバックアップ』を参照してください。
- IBM Spectrum Protect Plus ユーザーがデータをリストアできるようにするには、その前に、そのユーザーに適切な役割とリソース・グループを割り当てる必要があります。「**アカウント**」ペインを使用して、リソースおよびバックアップ/リストア操作へのアクセス権限をユーザーに付与してください。手順については、293 ページの『第 13 章 ユーザー・アクセスの管理』を参照してください。

以下の制約事項を確認してください。

- 選択した時点から先回のバックアップ・ジョブが実行された時点までの期間に 1 つ以上のデータ・ファイルがデータベースに追加されている場合には、特定時点リカバリーはサポートされません。
- バックアップ・ジョブの実行時に Oracle データベースがマウントされているが開いてはいない場合、IBM Spectrum Protect Plus は、**自動拡張性**と最大サイズに関するデータベース**一時ファイル**の設定を判別できません。このリストア・ポイントからデータベースをリストアした場合、一時ファイルが不明なため、IBM Spectrum Protect Plus は、元の設定値を使用して**一時ファイル**を再作成することができません。代わりに、デフォルトの設定値「AUTOEXTEND ON」と「MAXSIZE 32767M」を使用して**一時ファイル**が作成されます。リストア・ジョブの完了後に、手動で設定値を更新できます。
- IBM Spectrum Protect アーカイブからリストアする 場合、ファイルはジョブの開始前にテープからステージング・プールにマイグレーションされます。リストアのサイズによっては、このプロセスが完了するまで数時間かかることもあります。

このタスクについて

以下のリストア・モードがサポートされています。

インスタント・アクセス・モード
インスタント・アクセス・モードでは、共有をマウントした後、それ以上のアクションは実行されません。ユーザーは、vSnap ボリューム内のファイルを使用して任意のカスタム・リカバリーを実行できます。

テスト・モード
テスト・モードでは、エージェントは vSnap ボリュームからデータ・ファイルを直接使用して新規データベースを作成します。

実動モード
実動モードでは、エージェントはまず vSnap ボリュームから 1 次ストレージにファイルをリストアし、次にそのリストアされたファイルを使用して新規データベースを作成します。

手順

Oracle リストア・ジョブを定義するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**アプリケーション**」 > 「**Oracle**」 > 「**リストア・ジョブの作成**」をクリックして、「スナップショットのリストア」ウィザードを開きます。

   ヒント：

- 「スナップショットのリストア」ウィザードは、「**ジョブと操作**」 > 「**リストア・ジョブの作成**」 > 「**Oracle**」をクリックして開くこともできます。
- 「スナップショットのリストア」ウィザードで現在の選択内容の概要を確認するには、ウィザードのナビゲーション・ペインの情報アイコン にカーソルを移動します。
- ウィザードのオプションのページをバイパスするには、「**オプションのステップをスキップする**」を選択します。

2. 「**ソースの選択**」ページで、以下のステップを実行します。
   a) リスト内のソースをクリックして、リストア操作に使用できるデータベースを表示します。検索機能を使用して使用可能なインスタンスを検索し、表示されたインスタンスを「**表示**」フィルターで切り替えることもできます。
   b) リストア操作のソースとして使用するデータベースの横にあるプラス・アイコン をクリックします。複数のデータベースをリストから選択できます。

      選択したソースが、データベース・リストの隣にあるリストア・リストに追加されます。リストから項目を削除するには、その項目の横にあるマイナス・アイコン をクリックします。
   c) 「**次へ**」をクリックして先に進みます。
3. 「**ソース・スナップショット**」ページで、リストアするデータベースのインスタンスを指定します。以下のフィールドに入力し、「**次へ**」をクリックして先に進みます。いくつかのフィールドは、関連フィールドを選択するまで表示されません。

オプション	説明
リストア・タイプ	リストア・ジョブのタイプを選択します。 **オンデマンド: スナップショット** データベース・スナップショットから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **オンデマンド: 特定時点** データベースの特定時点バックアップから 1 回限りのリストア・ジョブを実行します。リストア・ジョブは、ウィザードが完了すると即時に開始されます。 **繰り返し** スケジュールに従って実行する反復特定時点リストア・ジョブを作成します。
リストア・ロケーションのタイプ	データのリストア元のロケーションのタイプを選択します。 **サイト** スナップショットがバックアップされたサイト 。サイトは、「**システム構成**」 > 「**サイト**」ペインで定義されます。 **クラウド・オフロード** スナップショットがオフロードされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・オフロード** スナップショットがオフロードされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。 **クラウド・アーカイブ** スナップショットがアーカイブされたクラウド ・サーバー。クラウド・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」ペインで定義されます。 **リポジトリー・アーカイブ** スナップショットがアーカイブされたリポジトリー ・サーバー。リポジトリー・サーバーは、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」ペインで定義されます。

オプション	説明
ロケーションの選択 (Select a location)	サイトからデータをリストアする場合は、以下のリストア・ロケーションのいずれかを選択します。 **デモ** スナップショットのリストア元のデモンストレーション・サイト。 **1 次** スナップショットのリストア元の 1 次サイト・ロケーション。 **2 次** スナップショットのリストア元の 2 次サイト・ロケーション。 クラウドまたはリポジトリー・サーバーからデータをリストアする場合は、「**ロケーションの選択**」メニューからサーバーを選択します。
日付セレクター	オンデマンド・スナップショット・リストア操作の場合、日付範囲を指定して、その日付範囲内で使用可能なスナップショットを表示します。
リストア・ポイント	オンデマンド・スナップショット・リストア操作の場合、選択したデータ範囲内で使用可能なスナップショットのリストからスナップショットを 選択します。
リストア・ジョブに代替 vSnap サーバーを使用します	クラウド・リソースまたはリポジトリー・サーバーからデータをリストアする場合は、このボックスを選択して代替 vSnap サーバーを指定してから、「**代替 vSnap の選択**」メニューからサーバーを選択します。 クラウド・リソースまたはリポジトリー・サーバーへオフロードまたはアーカイブされたリストア・ポイントからデータをリストアする場合、操作を完了するためのゲートウェイとして vSnap サーバーが使用されます。デフォルトでは、リストアを完了するために使用される vSnap サーバーは、バックアップとオフロードの操作を完了するために使用されるのと同じ vSnap サーバーです。vSnap サーバーの負荷を軽減するために、ゲートウェイとして機能する代替の vSnap サーバーを選択できます。

4. 「**宛先の設定**」ページで、データベースをリストアする場所を指定して、「**次へ**」をクリックします。

   元の位置にリストアする
   元のサーバーにデータベースをリストアするには、このオプションを選択します。

   代替の位置にリストアする
   オリジナル・サーバーとは異なるローカル宛先にデータベースをリストアするには、このオプションを選択します。その後、使用可能なサーバーのリストから代替ロケーションを選択します。

5. 「**リストア方式**」ページで、テスト・モード、実動モード、またはインスタント・アクセス・モードでリストア・ジョブをデフォルトで実行するように設定します。

   テスト・モードまたは実動モードの場合、オプションで、リストアされるデータベースの新規名を入力できます。

   実動モードの場合は、データベースを展開して新規フォルダー名を入力することで、リストアされるデータベース用に新規フォルダーを指定できます。

   「**次へ**」をクリックして先に進みます。

   ジョブが作成された後、「**ジョブ・セッション**」ペインで、そのジョブをテスト・モード、実動モード、またはインスタント・アクセス・モードで実行できます。

6. 「**ジョブ・オプション**」ページで、リストア・ジョブのその他のオプションを構成し、「**次へ**」をクリックして先に進みます。

   リカバリー・オプション
   以下の特定時点リカバリー・オプションを設定します。

   バックアップの最後までリカバリーします
   選択されたデータベースをバックアップの 作成時の状態にリストアします。

特定時点までリカバリーします
Oracle バックアップ・ジョブ定義を使用してログ・バックアップを有効にしている場合、Oracle リストア・ジョブ定義の作成時に特定時点リストア・オプションを選択できます。以下のいずれかのオプションを選択して、「**保存**」をクリックします。

- **時刻別**。特定の日時からの特定時点リカバリーを構成するには、このオプションを選択します。
- **SCN 別**。システム変更番号 (SCN) 別に特定時点リカバリーを構成するには、このオプションを選択します。

IBM Spectrum Protect Plus は、選択された特定時点の直前および直後のリストア・ポイントを検出します。リカバリーの実行中は、古いデータ・バックアップ・ボリュームと新しいログ・バックアップ・ボリュームがマウントされています。特定時点が最後のバックアップより後である場合は、一時的なリストア・ポイントが作成されます。

アプリケーション・オプション
以下のアプリケーション・オプションを設定します。

既存のデータベースを上書きします
選択済みデータベースをリストア・ジョブが上書きすることを許可するには、このオプションを有効にします。デフォルトでは、このオプションは選択されません。

データベースごとの最大並列ストリーム数
バックアップ・ストレージからのデータベースごとの並列データ・ストリームの最大数を設定します。この設定は、ジョブ定義内の各データベースに適用されます。このオプションの値が 1 に設定される場合でも、複数のデータベースを並列にリストアできます。複数の並列ストリームによってリストア速度が向上する可能性はありますが、帯域幅使用量が大きくなって全体的なシステム・パフォーマンスに影響を与えることがあります。

このオプションは、Oracle データベースを元のデータベース名を使用してオリジナル・ロケーションにリストアする場合にのみ適用可能です。

初期化パラメーター
このオプションは、リカバリー済みのデータベースを Oracle のテスト・ワークフローや実動ワークフローで始動するために使用される初期化パラメーターを制御します。

ソース。このオプションはデフォルトです。IBM Spectrum Protect Plus は、ソース・データベースと同じ初期化パラメーターを使用しますが、以下の変更を加えます。

- **control_files**、**db_recovery_file_dest**、または **log_archive_dest_*** などのパスを含むパラメーターが更新され、リカバリー済みボリュームの名前変更済みマウント・ポイントに基づく新しい名前が反映されます。
- パスがソース・サーバーと異なる場合は、宛先サーバー上の Oracle Base ディレクトリーの下の適切な位置を指すように、**audit_file_dest** および **diagnostic_dest** などのパラメーターが更新されます。
- データベースに新規名を指定した場合は、その新規名を反映するように、**db_name** パラメーターおよび **db_unique_name** パラメーターが更新されます。
- **instance_number**、**thread**、および **cluster_database** など、クラスター関連のパラメーターは、宛先の該当の値に応じて IBM Spectrum Protect Plus で自動的に設定されます。

宛先。IBM Spectrum Protect Plus で使用される初期化パラメーターが入ったテンプレート・ファイルを指定して、初期化パラメーターをカスタマイズします。

指定するパスは、宛先サーバー上に存在するプレーン・テキスト・ファイルを指す必要があり、IBM Spectrum Protect Plus のユーザーが読めるものでなければなりません。このファイルは、Oracle `pfile` フォーマットで、以下の形式の行で構成されている必要があります。

```
name = value
```

文字 # で始まるコメントは無視されます。

IBM Spectrum Protect Plus は、テンプレート `pfile` を読み取り、リカバリー済みデータベースの始動に使用される新規 `pfile` に項目をコピーします。ただし、テンプレート内の以下のパラ

メーターは無視されます。代わりに、IBM Spectrum Protect Plus は、ソース・データベースからの適切な値を反映するか、リカバリー済みボリュームの名前変更されたマウント・パスに基づく新規パスを反映するように、以下のパラメーターの値を設定します。

- **control_files**
- **db_block_size**
- **db_create_file_dest**
- **db_recovery_file_dest**
- **log_archive_dest**
- **spfile**
- **undo_tablespace**

また、**instance_number**、**thread**、および **cluster_database** など、クラスター関連のパラメーターは、宛先の該当の値に応じて IBM Spectrum Protect Plus で自動的に設定されます。

高度なオプション
以下の高度なジョブ定義オプションを設定します。

ジョブが失敗したとき、即時にクリーンアップを実行します
リカバリーが失敗した場合にリストア操作の一部として割り振り済みのリソースを自動的にクリーンアップするには、このオプションを有効にします。

セッションの上書きを許可します
リカバリー時に既存のデータベースを同じ名前のデータベースで置き換える場合は、このオプションを選択します。インスタント・ディスク・リストアをデータベースに対して実行したときに、同じ名前のデータベースが宛先のホストまたはクラスターで既に実行中になっていた場合、IBM Spectrum Protect Plus は、既存のデータベースをシャットダウンしてからリカバリー済みデータベースを始動します。このオプションを選択していない場合、IBM Spectrum Protect Plus が同じ名前で実行中のデータベースを検出すると、リストア・ジョブは失敗します。

いずれかが失敗しても、ほかのデータベースのリストアを続行します
直前のリソース・リカバリーが失敗した場合、シリーズ内のリソースのリカバリーを切り替えます。このオプションが有効になっていない場合、リソースのリカバリーが失敗すると、リストア・ジョブは停止します。

プロトコルの優先度 (インスタント・アクセスの場合のみ)
複数のストレージ・プロトコルが使用可能な場合、ジョブで優先するプロトコルを選択します。選択可能なプロトコルは、「**iSCSI**」および「**ファイバー・チャネル**」です。

マウント・ポイント接頭部
インスタント・アクセス・リストア操作の場合に、マウント・ポイントの送信先パスの接頭部を指定します。

7. オプション: 「**スクリプトの適用**」ページで、操作の実行前または実行後にジョブ・レベルで実行できるスクリプトを指定します。Windows オペレーティング・システムはバッチ・スクリプトと PowerShell スクリプトをサポートし、Linux オペレーティング・システムはシェル・スクリプトをサポートしています。

事前スクリプト
アップロードされたスクリプト、および事前スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このチェック・ボックスを選択します。事前スクリプトが実行されるアプリケーション・サーバーを選択するには、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーは、「**システム構成**」>「**スクリプト**」ページで構成します。

事後スクリプト
アップロードされたスクリプト、および事後スクリプトが実行されるアプリケーション・サーバーまたはスクリプト・サーバーを選択するには、このチェック・ボックスを選択します。事後スクリプトが実行されるアプリケーション・サーバーを選択するには、「**スクリプト・サーバーの使用**」チェック・ボックスをクリアします。スクリプトおよびスクリプト・サーバーは、「**システム構成**」>「**スクリプト**」ページで構成します。

スクリプト・エラー時にジョブ/タスクを続行
ジョブに関連付けられているスクリプトが失敗した場合にジョブの実行を続行するには、このチェック・ボックスを選択します。

このチェック・ボックスを選択すると、事前スクリプトまたは事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、バックアップ操作またはリストア操作が試行され、事前スクリプト・タスク状況は「完了」と報告されます。事後スクリプトの処理がゼロ以外の戻りコードで完了した場合、事後スクリプト・タスク状況は「完了」と報告されます。

このチェック・ボックスをクリアすると、バックアップまたはリストアは試行されず、事前スクリプトまたは事後スクリプトのタスク状況は「失敗」と報告されます。

8. 「**スケジュール**」ページで、以下のいずれかのアクションを実行します。
   - オンデマンド・ジョブを実行している場合は、「**次へ**」をクリックします。
   - 反復ジョブをセットアップしている場合は、ジョブ・スケジュールの名前を入力して、リストア・ジョブの頻度と開始時刻を指定します。「**次へ**」をクリックします。
9. 「**確認**」ページで、リストア・ジョブの設定を確認して、「**実行**」をクリックし、ジョブを作成します。

タスクの結果

「**実行**」をクリックした後でオンデマンド・ジョブが始まるとまもなく、「**onDemandRestore**」レコードが「**ジョブ・セッション**」ペインに追加されます。リストア操作の進行状況を表示するには、ジョブを展開します。ダウンロード・アイコン  をクリックして、ログ・ファイルをダウンロードすることもできます。

「**ジョブと操作**」 > 「**スケジュール**」ページでスケジュールを開始すると、スケジュールされた開始時刻に反復ジョブが始まります。

実行中のジョブはすべて、「**ジョブと操作**」 > 「**実行中のジョブ**」ページで表示できます。

次のタスク

Oracle データベースは常に非マルチスレッド・モードでリストアされます。リストアしたデータベースが元はマルチスレッド・モードであった場合は、リストア操作の完了後に、手動で資格情報を構成して、データベースをマルチスレッド・モードに切り替える必要があります。

関連概念

250 ページの『バックアップ操作とリストア操作のスクリプトの構成』
事前スクリプトと事後スクリプトは、バックアップ・ジョブとリストア・ジョブがジョブ・レベルで実行される前または後に実行できるスクリプトです。サポートされるスクリプトには、Linux ベースのマシン用のシェル・スクリプトや、Windows ベースのマシン用の Batch および PowerShell スクリプトがあります。スクリプトはローカル側で作成され、「**スクリプト**」ページを使用して環境にアップロードされてから、ジョブ定義に適用されます。

関連タスク

232 ページの『Oracle アプリケーション・サーバーの追加』
Oracle アプリケーション・サーバーが追加されると、そのアプリケーション・サーバーに関連付けられているインスタンスおよびデータベースのインベントリーがキャプチャーされ、IBM Spectrum Protect Plus に追加されます。このプロセスにより、バックアップとリストアのジョブを実行したり、レポートを実行したりできるようになります。

第 9 章 IBM Spectrum Protect Plus の保護

災害復旧シナリオの基礎データベースをバックアップして、IBM Spectrum Protect Plus アプリケーションを保護します。構成設定、登録済みリソース、リストア・ポイント、バックアップ・ストレージ設定、検索データ、およびジョブ情報が、関連した SLA ポリシーで定義された vSnap サーバーにバックアップされます。

IBM Spectrum Protect Plus アプリケーションのバックアップ

関連する SLA ポリシーに定義されている vSnap サーバーに、IBM Spectrum Protect Plus 構成設定、SLA ポリシー、登録済みリソース、バックアップ・ストレージ設定、リストア・ポイント、検索データ、およびインポート済みの鍵と証明書をバックアップします。

始める前に

適切な SLA ポリシーを使用できることを確認してください。バックアップ・ジョブを最適化するために、IBM Spectrum Protect Plus のバックアップ用に SLA ポリシーを作成します。 システム負荷を軽減するために、IBM Spectrum Protect Plus バックアップ・ジョブ中に他のジョブの実行がスケジュールに入れられていないことを確認してください。SLA ポリシーを作成するには、89 ページの『SLA ポリシーの作成』を参照してください。

制約事項 : IBM Spectrum Protect Plus バックアップ SLA ポリシーのターゲットとしてオンボード vSnap サーバーを選択することはできません。オンボード vSnap サーバーは、localhost という名前で、IBM Spectrum Protect Plus アプライアンスが最初にデプロイされるときに自動的にインストールされます。バックアップ用の SLA ポリシーを作成する場合は、2 次外部 vSnap サーバーをターゲットとして選択してください。

IBM Spectrum Protect Plus カタログは、同じロケーション、または災害復旧シナリオでは代替の IBM Spectrum Protect Plus ロケーションにリストアできます。

手順

IBM Spectrum Protect Plus データをバックアップするには、以下のようにします。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**IBM Spectrum Protect Plus**」 > 「**バックアップ**」をクリックします。
2. IBM Spectrum Protect Plus カタログのバックアップ操作に関連付ける SLA ポリシーを選択します。SLA ポリシーは、カタログ・バックアップのスケジューリングのほか、バックアップの宛先、複製、およびオフロードの設定を定義します。カタログ・バックアップ・データをクラウド・リソースおよびリポジトリー・サーバーにオフロードすることもできます。
3. 「**保存**」をクリックして、ジョブ定義を作成します。

タスクの結果

ジョブは、選択した SLA ポリシーで定義されたとおりに実行されます。あるいは、「**ジョブと操作**」 > 「**スケジュール**」をクリックして、ジョブを手動で実行することもできます。次に、「**スケジュール**」タブでジョブを選択して、「**アクション**」 > 「**開始**」をクリックします。手順については、80 ページの『バックアップ・ジョブの開始』を参照してください。

IBM Spectrum Protect Plus アプリケーションのリストア

vSnap サーバーにバックアップされた IBM Spectrum Protect Plus の構成設定、リストア・ポイント、検索データ、およびジョブ情報をリストアします。 データは、同じロケーションまたは別の IBM Spectrum Protect Plus ロケーションにリストアできます。

© Copyright IBM Corp. 2017, 2019

このタスクについて

重要 : IBM Spectrum Protect Plus リストア操作により、IBM Spectrum Protect Plus 仮想アプライアンスまたは代替仮想アプライアンスのロケーションにあるすべてのデータが 上書きされます。データのリストア中は、すべての IBM Spectrum Protect Plus 操作が停止します。ユーザー・インターフェースにアクセスできなくなり、実行中のジョブはすべてキャンセルされます。バックアップ操作とリストア操作の間に作成されたスナップショットは保存されません。

オフロードされたクラウド・バックアップをリストアする場合は、クラウド・リソースまたはリポジトリー・サーバーが代替の IBM Spectrum Protect Plus ロケーションに登録されている必要があります。

手順

IBM Spectrum Protect Plus データをリストアするには、以下のようにします。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**IBM Spectrum Protect Plus**」 > 「**リストア**」をクリックします。
2. vSnap サーバー、クラウド・リソース、またはリポジトリー・サーバーを選択します。

   データは、同じロケーション、または災害復旧シナリオでは代替ロケーションにリストアできます。

   サーバーに使用できるスナップショットが表示されます。
3. リストアするカタログ・スナップショットの「**リストア**」をクリックします。
4. 以下のいずれかのリストア・モードを選択します。

   カタログをリストアして、スケジュールに入れられたすべてのジョブを中断します
   カタログはリストアされ、すべてのスケジュール・ジョブは中断状態のままになります。どのスケジュール・ジョブも開始されません。そのため、カタログ項目の検証とテストや新規ジョブの作成が可能になります。通常、このオプションは DevOps のユース・ケースで使用されます。

   カタログをリストアします
   カタログはリストアされ、カタログ・バックアップにキャプチャーされているすべてのスケジュール・ジョブの実行は続行されます。通常、このオプションは災害復旧時に使用されます。
5. 「**リストア**」をクリックします。
6. リストア・ジョブを実行するには、ダイアログ・ボックスで「**はい**」をクリックします。

IBM Spectrum Protect Plus リストア・ポイントの管理

「**リストア・ポイントの保存**」ペインを使用して、IBM Spectrum Protect Plus カタログ内のリストア・ポイントをバックアップ・ジョブ名で検索したり、その作成日や有効期限を表示したり、割り当てられている保存をオーバーライドしたりすることができます。

このタスクについて

スナップショットが複製関係またはオフロード関係でロックされている場合、ジョブ・セッションを期限切れにしても、スナップショットおよび関連するリカバリー・ポイントは削除されません。複製またはオフロードに対応したジョブを実行して、ロックを以降のスナップショットに変更してください。スナップショットおよびリカバリー・ポイントは、次のメンテナンス・ジョブの実行時に削除されます。

手順

ジョブ・セッションを期限切れにするように設定するには、以下のようにします。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**IBM Spectrum Protect Plus**」 > 「**リストア・ポイントの保存**」をクリックします。
2. 「バックアップ・セッション」タブで、目的のジョブ・セッションまたはリストア・ポイントを検索します。検索機能の使用法について詳しくは、311 ページの『付録 A 検索ガイドライン』を参照してください。
3. フィルターを使用して、ジョブ・タイプや関連するバックアップ・ジョブが開始された日付範囲に関する検索を調整できます。

4. 検索アイコン をクリックします。
5. 期限切れにするジョブ・セッションを選択します。
6. 「**アクション**」リストから以下のいずれかのオプションを選択します。
   - 「**満了**」は、単一のジョブ・セッションを期限切れにするために使用します。
   - 「**すべてのジョブ・セッションの満了**」は、選択するジョブで期限切れ前のジョブ・セッションをすべて期限切れにするために使用します。
7. 期限切れを確認するには、ダイアログ・ボックスで「**はい**」をクリックします。

タスクの結果
ジョブ・セッションは、次のメンテナンス・ジョブの実行時に削除されます。
関連概念
247 ページの『ジョブ・タイプ』
IBM Spectrum Protect Plus におけるバックアップ操作、リストア操作、メンテナンス操作、およびインベントリー操作の実行に、ジョブを使用します。

カタログからの IBM Spectrum Protect Plus リソースの削除

「**リストア・ポイントの保存**」ペインの「**仮想マシン / データベース**」タブを使用して、IBM Spectrum Protect Plus カタログ内のリソースに関連付けられているカタログ・メタデータを期限切れにすることができます。 リソースは、インベントリー・ジョブを介してカタログに追加されています。リソースを期限切れにすると、リストア・ポイントに関連付けられているメタデータがカタログから削除されます。これにより、カタログ内のスペースが解放され、リカバリー画面からリストア・ポイントが削除されます。

このタスクについて
カタログからリソースを期限切れにしても、vSnap サーバーまたは 2 次バックアップ・ストレージから関連のスナップショットが削除されることはありません。

手順

カタログからリソースを期限切れにするには、以下のようにします。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**IBM Spectrum Protect Plus**」 > 「**リストア・ポイントの保存**」をクリックします。
2. 「**仮想マシン / データベース**」タブをクリックします。
3. フィルターを使用してリソース・タイプで検索し、検索ストリングを入力してリソースを名前で検索します。検索機能の使用法について詳しくは、311 ページの『付録 A 検索ガイドライン』を参照してください。
4. 検索アイコン をクリックします。
5. リソースに関連付けられている削除アイコン をクリックします。
6. 期限切れを確認するには、ダイアログ・ボックスで「**はい**」をクリックします。

タスクの結果
リソースに関連付けられているカタログ・メタデータがカタログから削除されます。
関連概念
247 ページの『ジョブ・タイプ』
IBM Spectrum Protect Plus におけるバックアップ操作、リストア操作、メンテナンス操作、およびインベントリー操作の実行に、ジョブを使用します。

第 10 章 ジョブと操作

「**ジョブと操作**」ウィンドウを使用して、ジョブのモニター、ジョブ・ヒストリーの確認、ジョブのスケジュール、アクティブ・リソースの表示、ジョブとスケジュールの再実行や一時停止を行います。

ジョブとリソースを表示して管理するには、「**ジョブと操作**」をクリックして、該当するタブをクリックします。

- 「**実行中のジョブ**」は、実行中のバックアップ・ジョブ、インベントリー・ジョブ、メンテナンス・ジョブ、およびリストア・ジョブを表示します。
- 「**ジョブ・ヒストリー**」には、失敗したジョブ、処理が警告で完了したジョブ、および正常に実行されたジョブが表示されます。ジョブを選択して「**ダウンロード (.zip)**」をクリックすることで、ジョブ・ログをダウンロードできます。
- 「**アクティブ・リソース**」は、アプリケーションとハイパーバイザーのアクティブ・リソースを表示します。
- 「**スケジュール**」には、ジョブ・スケジュールが表示されます。オンデマンド・ジョブを開始したり、選択したジョブのスケジュールを一時停止したりすることができます。編集アイコン  を使用して、ジョブ・スケジュールを編集することもできます。

「**リストア・ジョブの作成**」をクリックして、リストアのオンデマンド・ジョブや定期ジョブを作成することもできます。リストア・ジョブの作成方法については、次の表にあるリンクをクリックしてください。

表 22. リストア・ジョブの作成

タスク	説明
ハイパーバイザーのリストア・ジョブの作成	以下のトピックを参照してください。 • 111 ページの『VMware データのリストア』 • 127 ページの『Hyper-V データのリストア』
アプリケーションのリストア・ジョブの作成	以下のトピックを参照してください。 • 150 ページの『Db2 データのリストア』 • 166 ページの『Microsoft Exchange データベースのリストア』 • 206 ページの『MongoDB データのリストア』 • 237 ページの『Oracle データのリストア』 • 225 ページの『SQL Server データのリストア』

ジョブ・タイプ

IBM Spectrum Protect Plus におけるバックアップ操作、リストア操作、メンテナンス操作、およびインベントリー操作の実行に、ジョブを使用します。

バックアップ・ジョブとリストア・ジョブは、ユーザーが定義します。これらのジョブを作成した後、いつでもジョブを変更できます。メンテナンス・ジョブとインベントリー・ジョブは事前定義されているので、変更できません。

ジョブがスケジュールで実行するように設定されている場合であっても、すべてのジョブをオンデマンドで実行できます。また、スケジュールで実行するように設定されたジョブの保留も解除も可能です。

選択可能なジョブ・タイプは、以下のとおりです。

© Copyright IBM Corp. 2017, 2019

バックアップ
バックアップ・ジョブでは、バックアップするリソース、およびそれらのリソースに適用する SLA ポリシー (複数の場合あり) が定義されます。各 SLA ポリシーは、ジョブがいつ実行されるかを定義します。SLA ポリシーで定義されたスケジュールを使用してジョブを実行するか、オンデマンドでジョブを実行することができます。

ジョブ名は自動的に生成され、リソース・タイプの後に、ジョブに使用される SLA ポリシーが続きます。例えば、SLA ポリシー「ゴールド」に関連した SQL Server リソースのバックアップ・ジョブは `sql_Gold` になります。

リストア
リストア・ジョブでは、データをリストアする元のリストア・ポイントが定義されます。例えば、ハイパーバイザー・データをリストアしようとする場合、リストア・ポイントは仮想マシンにすることができます。アプリケーション・データをリストアしようとする場合、リストア・ポイントはデータベースにすることができます。ジョブを実行するスケジュールを作成するか、オンデマンドでジョブを実行することができます。

ジョブ名は、ジョブをオンデマンドで実行するか、スケジュールで実行するかによって異なります。オンデマンドでリストア操作を実行する場合、ジョブ名 `onDemandRestore` が自動生成されます。

スケジュールで実行するジョブを作成する場合は、ジョブ名を指定する必要があります。

メンテナンス
メンテナンス・ジョブは、保留状態のジョブが削除されるときに、IBM Spectrum Protect Plus によって作成されたリソースと関連オブジェクトを削除するために、一日に 1 回実行されます。

クリーンアップ手順では、ストレージ装置上のスペースを再利用し、IBM Spectrum Protect Plus カタログをクリーンアップし、関連したスナップショットを削除します。メンテナンス・ジョブでは、削除されたジョブに関連したカタログ・データも削除されます。

ジョブ名は `Maintenance` です。

インベントリー
インベントリー・ジョブは、リソースを IBM Spectrum Protect Plus に追加するときに自動的に実行されます。ただし、リソースが追加されて以降に生じた変更を検出するために、いつでもインベントリー・ジョブを実行できます。

インベントリー・ジョブ名は、`Default Application Server Inventory`、`Default Hypervisor Inventory`、および `Default Storage Server Inventory` です。

ジョブの開始

いずれのジョブも、スケジュールで実行するよう設定されている場合でも、オンデマンドで実行できます。

手順

ジョブを開始するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**ジョブと操作**」をクリックして、「**スケジュール**」タブをクリックします。
2. 実行するジョブを選択して、「**アクション**」 > 「**開始**」をクリックします。
   ジョブが開始され、「**実行中のジョブ**」タブに追加されます。

次のタスク

ジョブ・ログの詳細を表示するには、「**実行中のジョブ**」タブでジョブをクリックします。

ログ画面に以下の詳細が表示されます。

- 状況: メッセージがエラー・メッセージ、警告メッセージ、または情報メッセージのいずれであるかを示します。
- 時刻: メッセージのタイム・スタンプを示します。
- ID: メッセージの固有 ID を示します (該当する場合)。

- 説明: メッセージ・テキストを示します。

「**ダウンロード (.zip)**」をクリックして、ページからジョブ・ログをダウンロードすることができます。ジョブをキャンセルするには、「**アクション**」 > 「**キャンセル**」をクリックします。

ジョブの一時停止と再開

スケジュール済みのジョブや実行中のジョブの一時停止と再開が可能です。スケジュール済みのジョブを一時停止すると、そのジョブは、再開されるまで実行されません。

手順

ジョブ・スケジュールを一時停止して解放するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**ジョブと操作**」をクリックして、「**スケジュール**」タブをクリックします。
2. 一時停止するジョブを選択して、「**アクション**」 > 「**スケジュールの一時停止**」をクリックします。
3. ジョブ・スケジュールを再開するには、「**アクション**」 > 「**スケジュールの保留解除**」をクリックします。

ジョブのキャンセル

実行中のジョブをキャンセルできます。

手順

ジョブのキャンセルは、以下の手順で実行します。

1. ナビゲーション・ペインで、「**ジョブと操作**」をクリックして、「**スケジュール**」タブをクリックします。
2. 実行中のジョブ・セッションをキャンセルするには、目的のジョブに関連付けられている「**アクション**」メニューをクリックしてから、「**キャンセル**」をクリックします。

部分的に完了したバックアップ・ジョブの再実行

バックアップ・ジョブの最後のインスタンスが部分的に完了していた場合、そのジョブを再実行して、スキップされた仮想マシンおよびデータベースをバックアップすることができます。

このタスクについて

バックアップ・ジョブの再実行は、元の部分的に完了したバックアップ・ジョブと同じセッション ID でのみ可能です。再実行の対象として選択した部分的なバックアップ・ジョブ以降、同じリソースのバックアップは正常に実行されていない可能性があります。

注 : バックアップ・ジョブの再実行は、ハイパーバイザーまたはデータベース・バックアップの失敗に対してのみ可能です。以下のイベントは、バックアップ・ジョブの再実行操作にふさわしくありません。

- VM バックアップが FLI 障害で完了した。
- ストレージ・システムについてスナップショット 圧縮障害が発生した。
- バックアップ・ジョブが、カタログ・エラーなどの不明な問題で失敗した。
- リソースが vCenter にない。

ログ・バックアップがサポートされているアプリケーションの 場合、再実行機能を使用しているときには、ログ・バックアップは無効になりません。オンデマンド・バックアップまたは再実行機能を使用せずにジョブが次に開始されると、ログ・バックアップは適用可能なデータベースについて無効になっています。

手順

部分的に完了したバックアップ操作を再実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**ジョブと操作**」をクリックしてから、「**ジョブ・ヒストリー**」タブをクリックします。
2. 検索機能とフィルターを使用して、部分的に完了したバックアップ・ジョブの最後のインスタンスを見つけます。
3. 該当するジョブ・インスタンスを選択してから、「**再実行**」をクリックします。

   注:

   バックアップ・ジョブが再実行できない場合、「**再実行**」オプションが選択不可になっています。

   すべての SLA オプションと、元のジョブに関連付けられている除外事項はいずれも、再実行操作に含まれます。部分的なバックアップ完了以降に、オプションや除外事項の変更は適用されません。再実行されたジョブが正常に完了すると、ジョブ要約が更新されて、成功が示されます。

単一のリソースのバックアップ

ハイパーバイザーまたはアプリケーション・サーバーが SLA ポリシーに関連付けられている場合、オンデマンド・バックアップ操作を実行することにより、単一の仮想マシンまたはアプリケーションを即時にバックアップできます。ハイパーバイザーまたはアプリケーション・サーで「**実行**」を選択すると、オンデマンド・バックアップ操作を実行できます。このオプションは、既存の SLA ポリシーが該当のリソースに関連付けられていると有効になります。

このタスクについて

単一リソースに対するバックアップ・ジョブの実行は、複製やオフロード操作ではなく、バックアップ操作に対してのみ適用できます。

ログ・バックアップがサポートされているアプリケーションの場合、オンデマンド・バックアップまたは再実行機能を使用しているときには、ログ・バックアップは無効になりません。オンデマンド・バックアップまたは再実行機能を使用せずにジョブが次に開始されると、ログ・バックアップは適用可能なデータベースについて無効になっています。

手順

単一仮想マシンまたはアプリケーション・サーバーのオンデマンド・バックアップ・ジョブを実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**保護の管理**」をクリックします。バックアップ操作のタイプに応じて、「**ハイパーバイザー**」 > 「**バックアップ**」、または「**アプリケーション**」 > 「**バックアップ**」を選択してください。
2. リストされているインスタンスのいずれかをクリックして、関連付けられている仮想マシンまたはアプリケーションのリソースを表示します。

   ハイパーバイザーまたはアプリケーション・サーバーは、既存の SLA ポリシーに関連付けられている必要があります。
3. 「**実行**」をクリックします。

   仮想マシンまたはアプリケーションが複数の SLA ポリシーのメンバーになっている場合は、オンデマンド・ジョブについて実行する SLA ポリシーを選択してください。
4. バックアップ・ジョブを確認するために、ダイアログ・ボックスで「**OK**」をクリックします。

バックアップ操作とリストア操作のスクリプトの構成

事前スクリプトと事後スクリプトは、バックアップ・ジョブとリストア・ジョブがジョブ・レベルで実行される前または後に実行できるスクリプトです。サポートされるスクリプトには、Linux ベースのマシン用のシェル・スクリプトや、Windows ベースのマシン用の Batch および PowerShell スクリプトがあります。

スクリプトはローカル側で作成され、「**スクリプト**」ページを使用して環境にアップロードされてから、ジョブ定義に適用されます。

始めに

ハイパーバイザーでスクリプトを使用するには、以下の考慮事項を検討してください。

- スクリプトを実行するユーザーには、「**サービスとしてログオン**」権限が有効になっている必要があります。この権限は、事前スクリプトと事後スクリプトの実行に必要です。この権限について詳しくは、Add the Log on as a service Right to an Account を参照してください。
- Windows Remote Shell (WinRM) が有効でなければなりません。

スクリプトのアップロード

サポートされるスクリプトには、Linux ベースのマシンの場合はシェル・スクリプトが、また、Windows ベースのマシンの場合はバッチ・スクリプトと PowerShell スクリプトがあります。スクリプトは、オペレーティング・システムの関連ファイル・フォーマットを使用して作成する必要があります。

手順

スクリプトをアップロードするには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**スクリプト**」をクリックします。
2. 「**スクリプト**」セクションで、「**スクリプトのアップロード**」をクリックします。
   「**スクリプトのアップロード**」ペインが表示されます。
3. 「**参照**」をクリックして、アップロードするローカル・スクリプトを選択します。
4. 「**保存**」をクリックします。
   スクリプトは「**スクリプト**」テーブルに表示され、サポートされるジョブに適用できます。

次のタスク

スクリプトをアップロード後、以下のアクションを実行します。

アクション	方法
スクリプトを、それが実行されるサーバーに追加します。	251 ページの『サーバーへのスクリプトの追加』を参照してください。

サーバーへのスクリプトの追加

スクリプトを、それが実行されるサーバーに追加します。

手順

以下のステップを実行して、スクリプトをサーバーに指定します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**スクリプト**」をクリックします。
2. 「**スクリプト・サーバー**」セクションで、「**スクリプト・サーバーの追加**」をクリックします。
   「**スクリプト・サーバー・プロパティー**」ペインが表示されます。
3. サーバー・オプションを設定してください。

   ホスト・アドレス

   解決可能な IP アドレスまたは解決可能なパスとマシン名を入力してください。

   既存のユーザーの使用

   プロバイダー用に以前に入力されたユーザー名とパスワードを選択できるようにします。

   ユーザー名

   プロバイダー用のユーザー名を入力します。SQL サーバーを入力する場合、仮想マシンがドメインに接続されているのであれば、ユーザー ID はデフォルトの *domain¥name* フォーマットに従います。ユーザーがローカル管理者の場合、フォーマット *local_administrator* が使用されます。

パスワード

プロバイダー用のパスワードを入力します。

OS タイプ

アプリケーション・サーバーのオペレーティング・システムを選択します。

4.「**保存**」をクリックします。

第 11 章 IBM Spectrum Protect Plus システム環境の構成および保守

システム管理タスクには、バックアップ・ストレージの追加、サイトの管理、Lightweight Directory Access Protocol (LDAP) サーバーまたは Simple Mail Transfer Protocol (SMTP) サーバーの登録、クラウド・リソース用の鍵と証明書の管理があります。

メンテナンス・タスクには、IBM Spectrum Protect Plus 仮想アプライアンスの構成の検討、トラブルシューティング用のログ・ファイルの収集、Secure Sockets Layer (SSL) 証明書の管理があります。

大部分の場合、IBM Spectrum Protect Plus は仮想アプライアンスにインストールされます。仮想アプライアンスにはアプリケーションとインベントリーが含まれています。メンテナンス・タスクの実行は、vSphere Client で行うか、IBM Spectrum Protect Plus コマンド・ラインを使用するか、または Web ベースの管理コンソールで行います。

メンテナンス・タスクはシステム管理者が実行します。システム管理者は通常、vSphere および ESX インフラストラクチャーを設計または実装した上級レベルのユーザー、もしくは IBM Spectrum Protect Plus、VMware、および Linux コマンド・ラインの使用法を理解しているユーザーです。

インフラストラクチャーの更新は、IBM の更新機能によって管理されます。管理コンソールは、IBM Spectrum Protect Plus の機能や基礎のインフラストラクチャー・コンポーネント (オペレーティング・システムやファイル・システムを含む) を更新するための 1 次手段です。また、vSnap スタンドアロン・インスタンス用に、Z File System (ZFS) 更新パッケージも用意されています。

重要 : IBM Spectrum Protect Plus の基礎コンポーネントの更新には、IBM が提供する更新機能のみを使用してください。

2 次バックアップ・ストレージの管理

vSnap サーバーは、スナップショットの 1 次バックアップ・ロケーションです。すべての IBM Spectrum Protect Plus 環境に少なくとも 1 つの vSnap サーバーがあります。オプションで、スナップショットを vSnap サーバーからクラウド・ストレージ・システムまたはリポジトリー・サーバーにオフロードできます。

2 次ストレージへのスナップショット・データのオフロードについては、6 ページの『2 次バックアップ・ストレージへのオフロード』を参照してください。

クラウド・ストレージの管理

長期データ保護のためにクラウド・ストレージにオフロードすることができます。

バックアップ・ストレージ・プロバイダーとしての Amazon S3 クラウド・ストレージの追加

Amazon S3 クラウド・ストレージを追加して、IBM Spectrum Protect Plus がデータを S3 にオフロードできるようにします。

始める前に

クラウド・オブジェクトに必要な鍵を構成します。手順については、265 ページの『アクセス・キーの追加』を参照してください。

以下のステップでクラウド・ストレージを追加する前に、IBM Spectrum Protect Plus データ用のクラウド・ストレージ・バケットが作成されていることを確認してください。バケットの作成方法については、Amazon Simple Storage Service Documentation を参照してください。

手順

Amazon S3 クラウド・ストレージをバックアップ・ストレージ・プロバイダーとして追加するには、以下のステップを実行します。

© Copyright IBM Corp. 2017, 2019

1. ナビゲーション・メニューで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」をクリックします。
2. 「**クラウドの追加**」をクリックします。
3. 「**プロバイダー**」リストから「**Amazon S3**」を選択します。
4. 「**クラウドの登録**」ペインのフィールドに入力します。

   名前
   クラウド・ストレージを識別するために役立つ分かりやすい名前を入力します。

   地域
   クラウド・ストレージの Amazon Web サービス (AWS) の地域エンドポイントを選択します。

   既存のキーの使用
   ストレージについて以前に入力済みのキーを選択できます。その後、「**キーを選択します**」リストからキーを選択します。

   このオプションを選択しない場合は、以下のフィールドに入力してキーを追加します。

   キー名
   キーを識別するために役立つ分かりやすい名前を入力します。

   アクセス・キー
   AWS アクセス・キーを入力します。アクセス・キーは、AWS マネジメントコンソールで作成されます。

   秘密鍵
   AWS 秘密鍵を入力します。秘密鍵は、AWS マネジメントコンソールで作成されます。
5. 「**バケットの取得**」をクリックして、オフロードのターゲットにするバケットを選択します。

   バケットが生成された後、「**オフロード・バケット (Offload bucket)**」フィールドと「**アーカイブ・バケット (Archive bucket)**」フィールドが表示されます。
6. 「**オフロード・バケット (Offload bucket)**」フィールドで、オフロードのターゲットにするバケットを選択します。
7. オプション: 「**アーカイブ・バケット (Archive bucket)**」フィールドで、アーカイブのターゲットにするクラウド・ストレージ・リソースを選択します。

   データをアーカイブすると、フル・データ・コピーが作成され、長期にわたる保護、コスト、およびセキュリティー上のメリットが得られます。データのアーカイブについて詳しくは、6 ページの『2 次バックアップ・ストレージへのオフロード』のクラウド・アーカイブ・ストレージへのデータのコピーに関する情報を参照してください。
8. 「**登録**」をクリックします。

   クラウド・ストレージがクラウド・サーバー・テーブルに追加されます。

次のタスク
S3 ストレージを追加した後、以下のアクションを実行します。

アクション	方法
バックアップ・ジョブに使用される SLA ポリシーにクラウド・ストレージを関連付けます。	SLA ポリシーを作成するには、89 ページの『SLA ポリシーの作成』を参照してください。 既存の SLA ポリシーを変更するには、93 ページの『SLA ポリシーの編集』を参照してください。

バックアップ・ストレージ・プロバイダーとしての IBM Cloud Object Storage の追加
IBM Cloud Object Storage を追加して、IBM Spectrum Protect Plus がデータを IBM Cloud にオフロードできるようにします。

始める前に

クラウド・オブジェクトに必要な鍵と証明書を構成します。詳しくは、265 ページの『アクセス・キーの追加』および265 ページの『証明書の追加』を参照してください。

以下のステップでクラウド・ストレージを追加する前に、IBM Spectrum Protect Plus データ用のクラウド・ストレージ・バケットが作成されていることを確認してください。バケットの作成方法については、About IBM Cloud Object Storage を参照してください。

手順

IBM Cloud Object Storage をバックアップ・ストレージ・プロバイダーとして追加するには、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」をクリックします。
2. 「**クラウドの追加**」をクリックします。
3. 「**プロバイダー**」リストから「**IBM Cloud Object Storage**」を選択します。
4. 「**クラウドの登録**」ペインのフィールドに入力します。

   名前
   クラウド・ストレージを識別するために役立つ分かりやすい名前を入力します。

   エンドポイント
   クラウド・ストレージのエンドポイントを選択します。

   既存のキーの使用
   ストレージについて以前に入力済みのキーを選択できます。その後、「**キーを選択します**」リストからキーを選択します。

   このオプションを選択しない場合は、以下のフィールドに入力してキーを追加します。

   キー名
   キーを識別するために役立つ分かりやすい名前を入力します。

   アクセス・キー
   アクセス・キーを入力します。

   秘密鍵
   秘密鍵を入力します。

   証明書
   証明書をリソースに関連付ける方式を選択します。

   アップロード
   「**参照**」を選択してクリックし、証明書を見つけて、「**アップロード**」をクリックします。

   コピーと貼り付け
   証明書の名前を入力し、証明書の内容をコピーして貼り付ける場合に選択します。その後、「**作成**」をクリックします。

   既存の使用
   以前にアップロード済みの証明書を使用する場合に選択します。

   パブリック IBM Cloud Object Storage を追加する場合は、証明書は必要ありません。
5. 「**バケットの取得**」をクリックして、オフロードのターゲットにするバケットを選択します。

   バケットが生成された後、「**オフロード・バケット (Offload bucket)**」フィールドと「**アーカイブ・バケット (Archive bucket)**」フィールドが表示されます。
6. 「**オフロード・バケット (Offload bucket)**」フィールドで、オフロードのターゲットにするバケットを選択します。
7. オプション: 「**アーカイブ・バケット (Archive bucket)**」フィールドで、アーカイブのターゲットにするクラウド・ストレージ・リソースを選択します。

   データをアーカイブすると、フル・データ・コピーが作成され、長期にわたる保護、コスト、およびセキュリティー上のメリットが得られます。データのアーカイブについて詳しくは、6 ページの『2 次バックアップ・ストレージへのオフロード』のクラウド・アーカイブ・ストレージへのデータのコピーに関する情報を参照してください。
8. 「**登録**」をクリックします。

   クラウド・ストレージがクラウド・サーバー・テーブルに追加されます。

次のタスク
IBM Cloud Object Storage を追加した後、以下のアクションを実行します。

アクション	方法
バックアップ・ジョブに使用される SLA ポリシーにクラウド・ストレージを関連付けます。	SLA ポリシーを作成するには、89 ページの『SLA ポリシーの作成』を参照してください。 既存の SLA ポリシーを変更するには、93 ページの『SLA ポリシーの編集』を参照してください。

バックアップ・ストレージ・プロバイダーとしての Microsoft Azure クラウド・ストレージの追加
Microsoft Azure クラウド・ストレージを追加して、IBM Spectrum Protect Plus がデータを Microsoft Azure Blob ストレージにオフロードできるようにします。

始める前に
以下のステップでクラウド・ストレージを追加する前に、IBM Spectrum Protect Plus データ用のクラウド・ストレージ・バケットが作成されていることを確認してください。バケットの作成方法については、Azure 資料を参照してください。

手順
Microsoft Azure クラウド・ストレージをバックアップ・ストレージ・プロバイダーとして追加するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」をクリックします。
2. 「**クラウドの追加**」をクリックします。
3. 「**プロバイダー**」リストから「**Microsoft Azure Blob Storage**」を選択します。
4. 「**クラウドの登録**」ペインのフィールドに入力します。

   名前
   クラウド・ストレージを識別するために役立つ分かりやすい名前を入力します。

   エンドポイント
   クラウド・ストレージのエンドポイントを選択します。

   既存のキーの使用
   ストレージについて以前に入力済みのキーを選択できます。その後、「**キーを選択します**」リストからキーを選択します。

   このオプションを選択しない場合は、以下のフィールドに入力してキーを追加します。

   キー名
   キーを識別するために役立つ分かりやすい名前を入力します。

   ストレージ・アカウント名
   Microsoft Azure アクセス・ストレージのアカウント名を入力します。これは、Azure 管理ポータルから取得します。

   ストレージ・アカウント共有鍵
   Azure 管理ポータルのいずれかのキー・フィールド (key1 または key2) に示される Microsoft Azure キーを入力します。
5. 「**バケットの取得**」をクリックして、オフロードのターゲットにするバケットを選択します。

   バケットが生成された後、「**オフロード・バケット (Offload bucket)**」フィールドと「**アーカイブ・バケット (Archive bucket)**」フィールドが表示されます。
6. 「**オフロード・バケット (Offload bucket)**」フィールドで、オフロードのターゲットにするバケットを選択します。
7. オプション: 「**アーカイブ・バケット (Archive bucket)**」フィールドで、アーカイブのターゲットにするクラウド・ストレージ・リソースを選択します。

データをアーカイブすると、フル・データ・コピーが作成され、長期にわたる保護、コスト、およびセキュリティー上のメリットが得られます。データのアーカイブについて詳しくは、6 ページの『2 次バックアップ・ストレージへのオフロード』のクラウド・アーカイブ・ストレージへのデータのコピーに関する情報を参照してください。

8. 「**登録**」をクリックします。
   クラウド・ストレージがクラウド・サーバー・テーブルに追加されます。

次のタスク

Microsoft Azure ストレージを追加した後、以下のアクションを実行します。

アクション	方法
バックアップ・ジョブに使用される SLA ポリシーにクラウド・ストレージを関連付けます。	SLA ポリシーを作成するには、89 ページの『SLA ポリシーの作成』を参照してください。 既存の SLA ポリシーを変更するには、93 ページの『SLA ポリシーの編集』を参照してください。

クラウド・ストレージの設定の編集

クラウド・ストレージ・プロバイダーの設定を編集して、クラウド環境の変更を反映させます。

手順

クラウド・ストレージ・プロバイダーを編集するには、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」をクリックします。
2. クラウド・プロバイダーに関連付けられている編集アイコン をクリックします。
   「**クラウドの更新**」ペインが表示されます。
3. クラウド・プロバイダーの設定を修正して、「**更新**」をクリックします。

クラウド・ストレージの削除

クラウド・ストレージ・プロバイダーを削除して、クラウド環境の変更を反映させます。プロバイダーを削除する前に、プロバイダーがどの SLA ポリシーにも関連付けられていないことを確認してください。

手順

クラウド・ストレージ・プロバイダーを削除するには、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**クラウド**」をクリックします。
2. プロバイダーに関連付けられている削除アイコン をクリックします。
3. 「**はい**」をクリックしてプロバイダーを削除します。

リポジトリー・サーバー・ストレージの管理

長期データ保護のためにリポジトリー・サーバーにオフロードすることができます。現行リリースの IBM Spectrum Protect Plus の場合、リポジトリー・サーバーは IBM Spectrum Protect サーバー バージョン 8.1.7 以降でなければなりません。磁気テープにアーカイブする 場合は、IBM Spectrum Protect サーバー バージョン 8.1.8 以降が必要です。

オフロード・ターゲットとしての IBM Spectrum Protect サーバー の構成

IBM Spectrum Protect サーバー に対してデータをオフロードするには、最初に、IBM Spectrum Protect Plus をサーバーに対してオブジェクト・クライアントとしてセットアップする 必要があります。

このタスクについて

オブジェクト・クライアントをセットアップすると 、IBM Spectrum Protect サーバー への安全な接続を有効にするために鍵と証明書が提供されます。これらは、IBM Spectrum Protect Plus でリポジトリー・サーバーを追加するのに必要です。

オブジェクト・クライアントを追加するには、IBM Spectrum Protect サーバー 環境に精通しており、Operations Center または IBM Spectrum Protect サーバー の管理コマンドを使った作業経験があることが必要です。支援が必要な場合は、IBM Spectrum Protect 管理者に連絡してください。

IBM Spectrum Protect Plus は、IBM Spectrum Protect サーバー に対するオフロードを認識しますが、後続の IBM Spectrum Protect サーバー の複製操作は認識しません。

オフロード・ターゲットとしての IBM Spectrum Protect の構成に関する資料は、以下のように IBM Knowledge Center で入手できます。

- 構成プロセスの概要については、IBM Spectrum Protect Plus からのデータのオフロードを参照。
- オフロード・プロセスの前提条件については、IBM Spectrum Protect Plus からのデータのオフロードの準備を参照。
- AIX オペレーティング・システム情報については、Configuring to offload data in AIX® environments を参照。
- Linux オペレーティング・システムまたは Windows オペレーティング・システムの情報については、Configuring to offload data in Linux and Windows environments を参照。

関連タスク

263 ページの『バックアップ・ストレージ・プロバイダーとしてのリポジトリー・サーバーの追加』
IBM Spectrum Protect Plus がデータをサーバーにオフロードできるようにリポジトリー・サーバーを追加します。

IBM Spectrum Protect Plus からのデータのオフロードの準備

データを IBM Spectrum Protect Plus から IBM Spectrum Protect にオフロードする前に、IBM Spectrum Protect 環境で準備ステップを実行してください。

手順

1. データ・オフロード操作のために使用する予定の IBM Spectrum Protect Plus オブジェクト・クライアントに対する IBM Spectrum Protect サーバー・ポートをオープンできることを確認します。デフォルトのポート番号は 9000 です。オブジェクト・クライアントとエージェント間にファイアウォールがある場合、ファイアウォールを経由して該当するポートにアクセスできるようにオブジェクト・エージェントを構成します。
2. データ・オフロード操作の使用を予定しているポリシー・ドメインの設定を確認します。オブジェクト・クライアント・ノードは、IBM Spectrum Protect サーバーの管理コマンド **REGISTER NODE** または **UPDATE NODE** を使用してノードが登録または更新されたときに、このポリシー・ドメインに関連付けられます。

   IBM Spectrum Protect Plus オフロード操作用のポリシー・ドメインを指定する場合の考慮事項は、以下のとおりです。

   - ノードの割り当て先のドメインにはバックアップ・コピー・グループが必要です。オブジェクト・クライアント・ノードに保管されるオブジェクトは常にバックアップ・オブジェクトになります。アーカイブ・コピー・グループは必要ありません。
   - コンテナー・ストレージ・プールを使用する必要があります。コピー・グループ `Copy Destination` で指定されているストレージ・プールは、ディレクトリー・コンテナー・ストレージ・プールまたはクラウド・コンテナー・ストレージ・プールのどちらかでなければなりません。

- すべてのオブジェクトは一意的に名前が付けられています。オブジェクトの非アクティブ・バージョンはありません。そのため Versions Data Exists フィールドを 1 に設定できます。
- バックアップ・コピー・グループにはアクティブ・バージョンのみが含まれているため、「Retain Extra Versions」および「Retain Only Version」の各フィールドは 0 に設定できます。
- IBM Spectrum Protect サーバーは、オブジェクトが削除される時刻を制御します。バックアップ・コピー・グループを削除できるようにオブジェクト・クライアント・ノードが有効になっていることを確認してください。

例: IBM Spectrum Protect Plus オフロード操作のポリシー・ドメインに関する詳細情報の表示

オブジェクト・クライアント・ノードのコピー・グループの設定を表示します。

```
query copygroup format=detailed
```

```
                Policy Domain Name: TAPSRV03_OBJECT
                   Policy Set Name: SET1
                   Mgmt Class Name: BACK_DISK
                   Copy Group Name: STANDARD
                   Copy Group Type: Backup
              Versions Data Exists: 1
             Versions Data Deleted: 0
             Retain Extra Versions: 0
               Retain Only Version: 0
                         Copy Mode: Modified
                Copy Serialization: Shared Static
                    Copy Frequency: 0
                  Copy Destination: DEDUPPOOL
Table of Contents (TOC) Destination:
     Last Update by (administrator): JBASIL
              Last Update Date/Time: 01/17/2019 14:38:05
                   Managing profile:
                    Changes Pending: No
```

AIX システムへのデータのオフロード

データを IBM Spectrum Protect Plus から AIX 上の IBM Spectrum Protect サーバーにオフロードすることができます。

このタスクについて

IBM Spectrum Protect オブジェクト・エージェントは、IBM AIX オペレーティング・システムで直接実行することはできません。ただし、最初に Linux x86_64 オペレーティング・システムにオブジェクト・エージェントをセットアップすることで、AIX システムの IBM Spectrum Protect オブジェクト・クライアントに、IBM Spectrum Protect Plus データをオフロードできます。スタンドアロンのオブジェクト・エージェントは、Linux x86_64 オペレーティング・システムでのみ使用可能です。

IBM Spectrum Protect Plus オブジェクト・クライアントが Linux x86_64 上の IBM Spectrum Protect オブジェクト・エージェントにデータを送信した後、オブジェクト・エージェントが、AIX 上の IBM Spectrum Protect オブジェクト・クライアントにデータを転送します。

手順

データを IBM Spectrum Protect Plus から AIX 上の IBM Spectrum Protect サーバーにオフロードするには、以下のステップを実行します。

1. AIX サーバーで、以下の IBM Spectrum Protect サーバー 管理コマンドを発行します。

   ```
   setopt EnableAIXS3Interface Yes
   ```

2. AIX サーバーで、以下の IBM Spectrum Protect サーバー 管理コマンドを発行して、オブジェクト・エージェントを定義します。上位アドレス (HLA) および下位アドレス (LLA) を設定するには、オブジェクト・エージェントが使用するホスト・システムおよびポートの IP アドレスを使用します。

```
define server object_agent_name
hla=object_agent_host_system_ip_address
lla=object_agent_port objectagent=yes
```

ヒント: オブジェクト・エージェント・ポートのデフォルト値は 9000 です。ローカル・オブジェクト・エージェントが既にシステムで実行されている場合、AIX サーバー用に構成されるオブジェクト・エージェントは、既存のオブジェクト・エージェントのポート番号とは異なるポート番号を使用する必要があります。

3. オブジェクト・エージェント・ホスト・システムに、以下のスクリプトをダウンロードします。
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/startObjectAgent.sh
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc.u
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/delObjectAgentSvc.sh

   IBM Spectrum Protect Plus または IBM Spectrum Protect サーバー のいずれかを、オブジェクト・エージェント・ホスト・システムにインストールできます。

   IBM Spectrum Protect サーバー がインストールされた場合は、サーバー・ディレクトリー内の spObjectAgent ファイルを使用することができるため、エージェントとそのスクリプトを再ダウンロードする必要はありません。
4. 以下のファイルに実行権限が設定されていることを確認します。
   - spObjectAgent
   - startObjectAgent.sh
   - spObjectAgent.rc
   - spObjectAgent.rc.u
   - delObjectAgentSvc.sh
5. AIX サーバー・システムから Linux 上のオブジェクト・エージェント・ホスト・システム上のディレクトリーに、以下の 2 つのアイテムをコピーします。
   - オブジェクト・エージェント・サーバー・ディレクトリー
   - サーバーのパブリック証明書

   オブジェクト・エージェント・サーバー・ディレクトリーは **DEFINE SERVER** コマンドを実行したときに作成されています。ディレクトリーには以下のファイルおよび証明書が含まれています。
   - オブジェクト・エージェント・サービスを作成して開始するための構成ファイル
   - オブジェクト・エージェントとサーバー間の通信用の証明書

   オブジェクト・エージェント・サーバー・ディレクトリーが、サーバー・インスタンス・ディレクトリー */server_instance_home_dir/object_agent_name* に作成されます。 例えば次の例のようにします。

   /home/tsminst1/OBJAGENT1

   サーバーのパブリック証明書 (cert256.arm) は、通常はサーバー・インスタンス・ディレクトリー内にあります。

6. 前のステップでコピーしたオブジェクト・エージェント・サーバー・ディレクトリー内で、オブジェクト・エージェント構成ファイル (spObjectAgent_*objectagentname_serverport*.config) を見つけます。

   例: spObjectAgent_OBJAGENT1_1500.config

   構成ファイルで、以下のファイルの場所を更新します。例えば、次のようにします。

   ```
   objagentexe=¥"/opt/tivoli/tsm/server/bin/spObjectAgent¥"
      keystore="/home/tsminst1/OBJAGENT1/agentcert.p12"
      pwdfile="/home/tsminst1/OBJAGENT1/agentcert.pwd"
      serverkeypub="/home/tsminst1/OBJAGENT1/cert256.arm"
      agentconfig=¥"/home/tsminst1/OBJAGENT1/spObjectAgent_OBJAGENT1_1500.config¥"
   ```

7. AIX サーバーの IP アドレスを使用して、オブジェクト・エージェント構成ファイルの **SERVERHLA** パラメーターをオーバーライドします。

   ```
   serverhla=aix_server_ip_address
   ```

   ヒント: オブジェクト・エージェントはこの値を使用して IBM Spectrum Protect サーバー を見つけます。

8. ホスト・システム 上でオブジェクト・エージェントを作成して開始するには、構成ファイルを指定して startObjectAgent.sh スクリプトを実行します。

   ```
   startObjectAgent.sh spObjectAgent_objectagentname_serverport.config
   ```

9. オブジェクト・エージェント・クライアントを AIX サーバーに登録するには、次の IBM Spectrum Protect サーバー・コマンドを発行します。

   ```
   register node nodename type=objectclient
   ```

   重要: ログイン・ユーザー ID とパスワードが自動的に生成されるので、記録しておきます。この資格情報は、オブジェクト・エージェントに接続する際に必要になります。

10. IBM Spectrum Protect Plus オブジェクト・クライアントをオブジェクト ・エージェントに接続するには、IBM Spectrum Protect Plus のオンライン資料にアクセスして、バックアップ・ストレージ・プロバイダーとしてのリポジトリー・サーバーの追加の指示に従ってください。

Linux システムおよび *Windows* システムへのデータのオフロード

データを IBM Spectrum Protect Plus から Linux または Windows 上の IBM Spectrum Protect サーバーにオフロードすることができます。

手順

データを IBM Spectrum Protect Plus から Linux または Windows 上の IBM Spectrum Protect サーバーにオフロードするには、以下のステップを実行します。

1. オブジェクト・エージェントをセットアップします。

   a) Operations Center メニュー・バーで、「**サーバー**」をクリックします。

   b) サーバー行を選択して、「**詳細**」をクリックします。

   c) 左のナビゲーション・ペインにある「**オブジェクト・エージェント**」を選択し、オブジェクト・エージェントを作成してオブジェクト・エージェント・サービスを開始するためのステップを実行します。オブジェクト・エージェントに対する認証を行う際は、生成された証明書を使用します。

   ヒント: あるいは、IBM Spectrum Protect サーバーの管理コマンド **DEFINE SERVER** を使用して、オブジェクト・エージェントを作成します。OBJECTAGENT=YES を指定してください。IBM Spectrum Protect サーバーをホスティングしているシステム 上でオブジェクト・エージェント・サービスを開始することで、構成を完了します。

2. オブジェクト・クライアントをセットアップします。

   ヒント: 対応するオブジェクト・エージェントを作成する前にオブジェクト・クライアントを作成すると、対応するオブジェクト・エージェントを作成する場合、「クライアントの追加」ウィザードによりオブジェクト・エージェントの作成が強制されます。

a) Operations Center メニュー・バーで、「**クライアント**」をクリックします。

b)「クライアント」テーブルで、「**+ クライアント**」をクリックします。

c)「オブジェクト・クライアント」を選択し、「**クライアントの追加**」ウィザードの指示に従います。

ウィザードの完了後、サーバー上のオブジェクト・エージェントと通信するためのエンドポイントと、安全に接続するためのアクセス・キー ID および秘密アクセス・キーが提供されます。IBM Spectrum Protect Plus は、オブジェクト・クライアントとして使用される場合には、その要求をエンドポイントに送信して、アクセス・キー ID と秘密アクセス・キーを使用する必要があります。

ヒント : あるいは、コマンド **REGISTER NODE** を使用して、オブジェクト・クライアントを作成します。TYPE=OBJECTCLIENT を指定してください。

オブジェクト・エージェント・サービスの削除
オブジェクト・エージェントが IBM Spectrum Protect サーバーから削除された場合、そのオブジェクト・エージェント・サービスをホスト・システムから削除する必要があります。オブジェクト・エージェントの削除プロセスを実行するには、対応するサービスを削除してください。

始める前に

Linux オペレーティング・システムでオブジェクト・エージェント・サービスを削除するには、オブジェクト・エージェント構成ファイルを指定して delObjectAgentSvc.sh スクリプトを実行する必要があります。root ユーザー ID でオブジェクト・エージェント・ホスト・システムにログインできることを 確認してください。

Windows オペレーティング・システムでオブジェクト・エージェント・サービスを削除するには、オブジェクト・エージェント構成ファイルを指定して delObjectAgentSvc.cmd バッチ・ファイルを実行する必要があります。オブジェクト・エージェント・ホスト・システムにログオンするための Windows 管理者権限があることを確認してください。

手順

1. サーバー管理コマンド **QUERY SERVER** を発行して、IBM Spectrum Protect サーバーからオブジェクト・エージェントが削除されていることを検証してください。
2. コマンド・ラインを開きます。
3. 以下のコマンドを 1 行で指定して発行します。サンプルにはデフォルト・サーバー・ディレクトリーが使用されています。

   Linux

   ```
   /opt/tivoli/tsm/server/bin/delObjectAgentSvc.sh
   /object_agent_config_path/spObjectAgent_objectagentname_server_port.config
   ```

   Windows

   ```
   "C:¥Program Files¥Tivoli¥TSM¥server¥delObjectAgentSvc.cmd"
   "object_agent_config_path¥spObjectAgent_objectagentname_server_port.config"
   ```

   ここで、

   object_agent_config_path

   オブジェクト・エージェントの構成パスを指定します。

   objectagentname

   オブジェクト・エージェントの名前を指定します。

   server_port

   IBM Spectrum Protect サーバーサーバーのポート番号を指定します。

バックアップ・ストレージ・プロバイダーとしてのリポジトリー・サーバーの追加

IBM Spectrum Protect Plus がデータをサーバーにオフロードできるようにリポジトリー・サーバーを追加します。

始める前に

リポジトリー・サーバーに必要な鍵および認証を構成します。手順については、265 ページの『アクセス・キーの追加』および 265 ページの『証明書の追加』を参照してください。

IBM Spectrum Protect Plus の現行リリースでは、リポジトリー・サーバーは IBM Spectrum Protect サーバー でなければなりません。

IBM Spectrum Protect Plus を、IBM Spectrum Protect サーバーに対するオブジェクト・クライアントとして構成します。オブジェクト・クライアント・ノードは、オフロード・データの転送と保管を行います。セットアップ手順を完了すると、ウィザードにより、サーバー上のオブジェクト・エージェントと通信するためのエンドポイントと、安全に接続するためのアクセス ID、秘密鍵、および証明書が提供されます。258 ページの『オフロード・ターゲットとしての IBM Spectrum Protect サーバー の構成』

証明書は、ペイン「**サーバー**」 > 「**オブジェクト・エージェント**」 > 「**エージェント証明書**」にナビゲートして、IBM Spectrum Protect サーバー Operations Center から取得できます。あるいは、コマンド `openssl s_client -showcerts -connect <ip-address>:9000 </dev/null 2>/dev/null | openssl x509` を入力して IBM Spectrum Protect Plus アプライアンスから証明書を取得できます。

オフロード保存設定は、IBM Spectrum Protect Plus の関連 SLA ポリシーによって完全に制御されます。IBM Spectrum Protect サーバー コピー・グループ保存設定は、オフロード操作には使用されません。

手順

IBM Spectrum Protect サーバー をバックアップ・ストレージ・プロバイダーとして追加するには、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」をクリックします。
2. 「**リポジトリー・サーバーの追加**」をクリックします。
3. 「**リポジトリー・サーバーの登録**」ペインの各フィールドに入力します。

   名前
   リポジトリー・サーバーの識別に役立つように、分かりやすい名前を入力します。

   ホスト名
   リポジトリー・サーバー・オブジェクト・エージェントの高水準アドレス (HLA) を入力します。IBM Spectrum Protect `q serv OBJAGENT f=d` コマンドを実行すると、この情報を取得できます。

   ポート
   リポジトリー・サーバーの通信ポートを入力します。

   既存の鍵を使用
   リポジトリー用に、以前に入力された鍵を選択してから、その鍵を「**鍵の選択**」リストから選択できるようにします。

   このオプションを選択しない場合は、以下のフィールドに入力して、鍵を追加します。

   キー名
   キーの識別に役立つように、分かりやすい名前を入力します。

   アクセス・キー
   アクセス・キーを入力します。

   秘密鍵
   秘密鍵を入力します。

   証明書
   証明書をリソースに関連付ける方式を選択します。証明書をコピーする場合、テキスト BEGIN 行と END 行が含まれている必要があります。

アップロード
「**参照**」を選択してクリックし、証明書を見つけて、「**アップロード**」をクリックします。

コピーと貼り付け
証明書の名前を入力することを選択し、証明書の内容をコピー・アンド・ペーストしてから、「**作成**」をクリックします。

既存の使用
以前にアップロードした証明書を使用することを選択します。

4. 「**登録**」をクリックします。
   IBM Spectrum Protect サーバーは、リポジトリー・サーバー・テーブルに追加されます。

次のタスク
リポジトリー・サーバーを追加したら、以下のアクションを実行します。

アクション	方法
リポジトリー・サーバーを、バックアップ・ジョブに使用される SLA ポリシーに関連付けます。	SLA ポリシーを作成する場合は、89 ページの『SLA ポリシーの作成』を参照します。 既存の SLA ポリシーを修正する場合は、93 ページの『SLA ポリシーの編集』を参照してください。

リポジトリー・サーバーの設定の編集
ご使用のクラウド環境で変更を反映するよう、リポジトリー・サーバー・プロバイダーの設定を編集します。

手順

リポジトリー・サーバー・プロバイダーを編集するには、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」をクリックします。
2. 目的のリポジトリー・サーバー・プロバイダーに関連付けられている編集アイコン をクリックします。
   「**リポジトリー・サーバーの更新**」ペインが表示されます。
3. 目的のリポジトリー・サーバー・プロバイダーの設定を修正してから、「**更新**」 をクリックします。

リポジトリー・サーバーの削除
ご使用の環境で変更を反映するよう、リポジトリー・サーバー・プロバイダーを削除します。プロバイダーがいずれの SLA ポリシーにも関連付けられていないことを確認したうえで、そのプロバイダーを削除してください。

手順

リポジトリー・サーバー・プロバイダーを削除するには、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**バックアップ・ストレージ**」 > 「**リポジトリー・サーバー**」をクリックします。
2. 目的のリポジトリー・サーバー・プロバイダーに関連付けられている削除アイコン をクリックします。
3. 「**はい**」をクリックしてプロバイダーを削除します。

鍵と証明書の管理

クラウド・リソースとリポジトリー・サーバーは、オフロード宛先の役目をするために資格情報が必要です。アクセス・キーや秘密鍵は、クラウド・リソースまたはリポジトリー・サーバーのインターフェースによって提供されます。これらの鍵は、オフロード宛先のユーザー名とパスワードの役目をし、IBM Spectrum Protect Plus がアクセスできるようにします。一部のオフロード宛先には、データ・セキュリティーを強化するために証明書も必要です。

オフロード宛先へのアクセスに資格情報を必要とする、IBM Spectrum Protect Plus 内のリソースを使用する場合は、「**既存のキーを使用**」または「**既存の証明書を使用**」を選択し、関連する鍵または証明書を選択します。

アクセス・キーの追加

クラウド・リソースまたはリポジトリー・サーバーの資格情報を提供するために、アクセス・キーを追加します。

手順

キーを追加するには、以下のステップを実行します。

1. クラウド・リソースまたはリポジトリー・サーバーのインターフェースからアクセス ・キーと秘密鍵を作成します。アクセス・キーと秘密鍵を書き留めてください。
2. ナビゲーション・メニューで、「**システム構成**」 > 「**鍵および証明書**」をクリックします。
3. 「**アクセス・キー**」セクションで、「**アクセス・キーの追加**」をクリックします。
4. 「**鍵のプロパティー**」ペインで各フィールドに入力します。

   名前

   アクセス・キーの識別に役立つように、分かりやすい名前を入力します。

   アクセス・キー

   クラウド・リソースまたはリポジトリー・サーバーのアクセス・キーを入力してください。Microsoft Azure の場合は、ストレージ・アカウント名を入力します。

   秘密鍵

   クラウド・リソースまたはリポジトリー・サーバーの秘密鍵を入力してください。Microsoft Azure の場合は、いずれかのキー・フィールド (key1 または key2) の鍵を入力します。
5. 「**保存**」をクリックします。
   この鍵は、「**アクセス・キー**」テーブルに表示され、「**既存の鍵を使用**」オプションからリソースにアクセスするのに資格情報を必要とする機能を使用している場合に選択できます。

アクセス・キーの削除

アクセス・キーは、廃止されたら削除してください。ご使用のクラウド・リソースまたはリポジトリー・サーバーに、必ず、新しいアクセス・キーを再割り当てしてください。

手順

アクセス・キーを削除する場合、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**鍵および証明書**」をクリックします。
2. アクセス・キーに関連付けられている削除アイコン ✕ をクリックします。
3. 「**はい**」をクリックしてアクセス・キーを削除します。

証明書の追加

クラウド・リソースまたはリポジトリー・サーバーの資格情報を提供するには、証明書を追加します。

手順

証明書を追加するには、以下のステップを実行します。

1. クラウド・リソースまたはリポジトリー・サーバーから証明書をエクスポートします。
2. ナビゲーション・メニューで、「**システム構成**」 > 「**鍵および証明書**」をクリックします。
3. 「**証明書**」セクションで、「**証明書の追加**」をクリックします。
4. 「**証明書プロパティー**」ペインのフィールドに入力します。

   タイプ

   クラウド・リソースまたはリポジトリー・サーバーのタイプを選択します。

証明書

証明書を追加する方式を選択します。

アップロード
証明書をローカル側で参照する場合に選択します。

コピーと貼り付け
証明書の名前を入力し、証明書の内容をコピーして貼り付ける場合に選択します。

5.「**保存**」をクリックします。
「**証明書**」テーブルに鍵が表示されます。リソースにアクセスするために、「**既存の証明書を使用**」オプションを使用して資格情報を使用する必要がある機能を利用する場合に、鍵を選択できます。

証明書の削除

証明書が古くなった場合には削除します。必ず、クラウド・リソースまたはリポジトリー・サーバーに新しい証明書を再割り当てしてください。

手順

証明書を削除するには、次のステップを完了します。

1. ナビゲーション・メニューで、「**システム構成**」 >「**鍵および証明書**」をクリックします。
2. 証明書に関連付けられている削除アイコン ✕ をクリックします。
3.「**はい**」をクリックして証明書を削除します。

SSH 鍵の追加

Oracle、Db2、および MongoDB の各アプリケーション・サーバーのほか、vCenter および Hyper-V 下の仮想マシン上でのファイルの索引付け操作やリストア操作など、Linux ベースのリソースのために資格情報を提供するには、SSH 鍵を追加します。SSH 鍵により、ご使用のリソースと IBM Spectrum Protect Plus との間でセキュア接続が実現されます。

始める前に

- SSH サービスがサーバー上のポート 22 で実行し、IBM Spectrum Protect Plus が SSH を使用してサーバーに接続できるように、何らかのファイアウォールが構成されている必要があります。SSH 用の SFTP サブシステムも 使用可能でなければなりません。
- 公開 SSH 鍵は、IBM Spectrum Protect Plus エージェント・ユーザー用の該当の authorized_keys ファイルに入っています。通常、このファイルは、/home/<username>/.ssh/authorized_keys 内にあります。.ssh ディレクトリー、およびその下にあるすべてのファイルは、その許可が 600 に設定されている必要があります。

手順

鍵を追加するには、以下のステップを実行します。

1. ご使用のリソースで、SSH 鍵を生成します。例えば、Oracle サーバー上で、`ssh-keygen` コマンドを入力して、指示に従います。
2.「鍵を保存するファイルを入力」というプロンプトが出されたら、ファイルと場所 (例: `/root/sshkey`) を入力します。
3. ステップ 2 で入力したサーバー上の /root の場所で、ファイル `sshkey.pub` に公開鍵が含まれます。これは、後に、IBM Spectrum Protect Plus に割り当てられたユーザーとしてログインしているときに `cd ~/.ssh` を実行した後で、コピー・アンド・ペーストされて、`authorized_keys` ファイルに保存されます。
4. IBM Spectrum Protect Plus ナビゲーション・ペインで、「**システム構成**」 >「**鍵および証明書**」をクリックします。
5.「**SSH 鍵**」セクションで、「**アクセス・キーの追加**」をクリックします。
6.「**SSH 鍵のプロパティー**」ペインで各フィールドに入力します。

名前

SSH 鍵の識別に役立つように、分かりやすい名前を入力します。

ユーザー

目的のリソースおよび SSH 鍵に関連付けられているユーザーを入力します。

秘密鍵

秘密鍵をコピー・アンド・ペーストします。この鍵は、sshkey ファイルに入っています。

7. 「**保存**」をクリックします。
   この鍵は、「**SSH 鍵**」テーブルに表示され、「**鍵**」オプションからリソースにアクセスするのに 資格情報を必要とする機能を使用している場合に選択できます。

SSH 鍵の削除
SSH 鍵は、廃止されたら削除してください。必ず、新しい SSH 鍵をご使用のリソースに再割り当てしてください。

手順

SSH 鍵を削除する場合、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**鍵および証明書**」をクリックします。
2. SSH 鍵に関連付けられている削除アイコン ✕ をクリックします。
3. 「**はい**」をクリックしてアクセス・キーを削除します。

サイトの管理

サイトは、環境内のデータ配置の管理に使用される IBM Spectrum Protect Plus ポリシー構造です。

サイトは、データセンターなどの物理的なものでも、部門や組織などの論理的なものでもかまいません。IBM Spectrum Protect Plus コンポーネントは、データ・パスをローカライズし、最適化するためにサイトに割り当てられます。1 つの IBM Spectrum Protect Plus デプロイメントには、物理ロケーションあたり 1 つ以上のサイトが常にあります。

デフォルトでは、IBM Spectrum Protect Plus 環境には、1 次サイト、2 次サイト、およびデモ・サイトがあります。

サイトの追加

IBM Spectrum Protect Plus にサイトを追加した後で、そのサイトにバックアップ・ストレージ・サーバーを割り当てることができます。

手順

サイトを追加するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**サイト**」をクリックします。
2. 「**サイトの追加**」をクリックします。
   「**サイト・プロパティー**」ペインが表示されます。
3. サイト名を入力します。
4. オプション: 定義済みのスケジュールに関するネットワーク・アクティビティーを 管理するには、サイト複製およびオフロード操作のスループットを 変更します。
   a) 「**スロットルの有効化**」チェック・ボックスを選択します。
   b) 「**速度**」フィールドでスループットを 調整します。
      1) 上矢印または下矢印をクリックして、スループットの 速度の数値を変更します。
      2) スループットの 単位を選択します。選択項目には、「**バイト/秒**」、 「**KB/秒**」、「**MB/秒**」、「**GB/秒**」があります。

   デフォルトのスループットは 100 MB/秒 (メガバイト/秒) です。

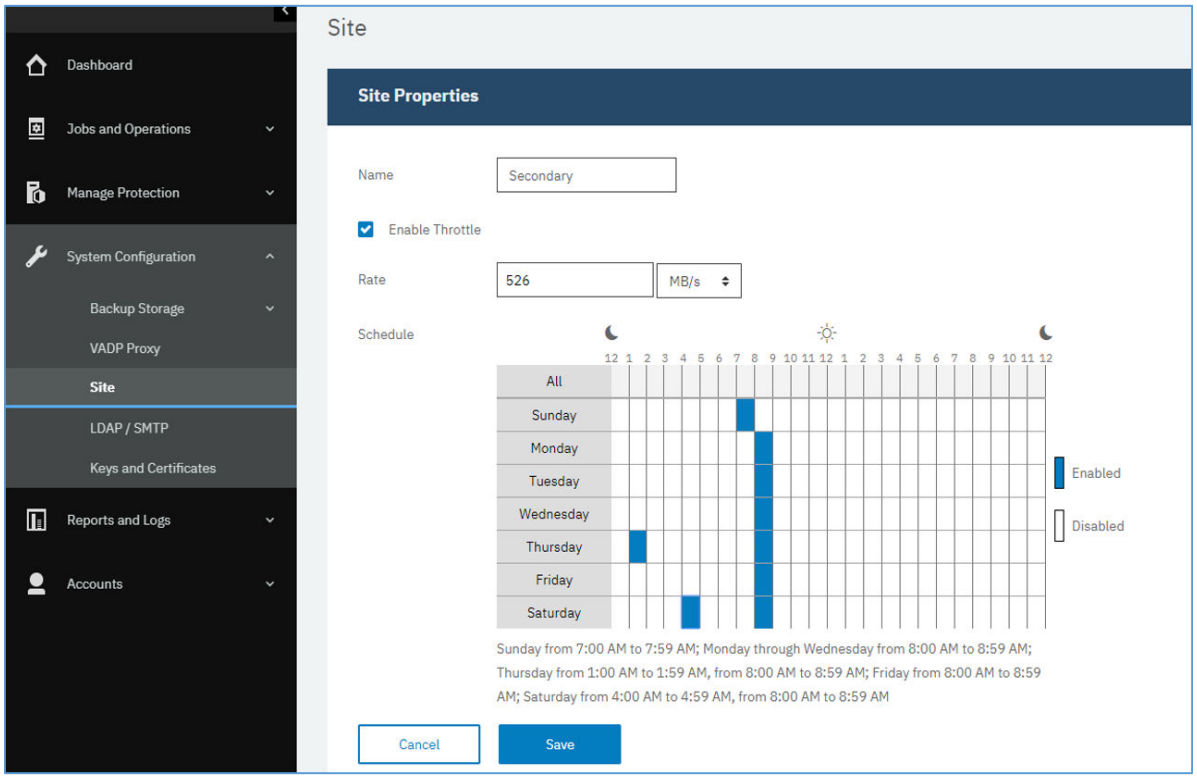


図 29. スループット向上のためのさまざまな時間に対する異なるスロットル速度の有効化

c) 週次スケジュール・テーブルで、スロットル用の毎日の時間を選択するか、スロットル用の特定の曜日と時間を選択します。

ヒント: 時間を選択するには、テーブル内でタイム・スロットをクリックします。選択したタイム・スロットが強調表示されます。タイム・スロットをクリアするには、強調表示されているタイム・スロットをクリックします。すべての曜日について同じタイム・スロットを選択するには、「**すべて**」行でタイム・スロットをクリックします。

選択を行うと、スロットルが設定された日と時間がスケジュール・テーブルの下にリストされます。

5. 「**保存**」をクリックすると、変更がコミットされ、ペインが閉じます。

タスクの結果

該当のサイトはサイト ・テーブルに表示され、新規および既存のバックアップ・ストレージ・サーバーに適用できます。

サイトの編集

IBM Spectrum Protect Plus 環境で変更を反映するよう、サイト情報を修正します。

手順

サイトを編集するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**サイト**」をクリックします。
2. サイトに関連付けられている編集アイコン をクリックします。
   「**サイト・プロパティー**」ペインが表示されます。
3. サイト名を修正します。
4. オプション: 定義済みのスケジュールに関するネットワーク・アクティビティーを 管理するには、サイト複製およびオフロード操作のスループットを変更します。
   a) 「**スロットルの有効化**」チェック・ボックスを選択します。
   b) 「**速度**」フィールドでスループットを 調整します。

1) 上矢印または下矢印をクリックして、スループットの速度の数値を変更します。
2) スループットの単位を選択します。選択項目には、「**バイト/秒**」、「**KB/秒**」、「**MB/秒**」、「**GB/秒**」があります。

デフォルトのスループットは 100 MB/秒 (メガバイト/秒) です。

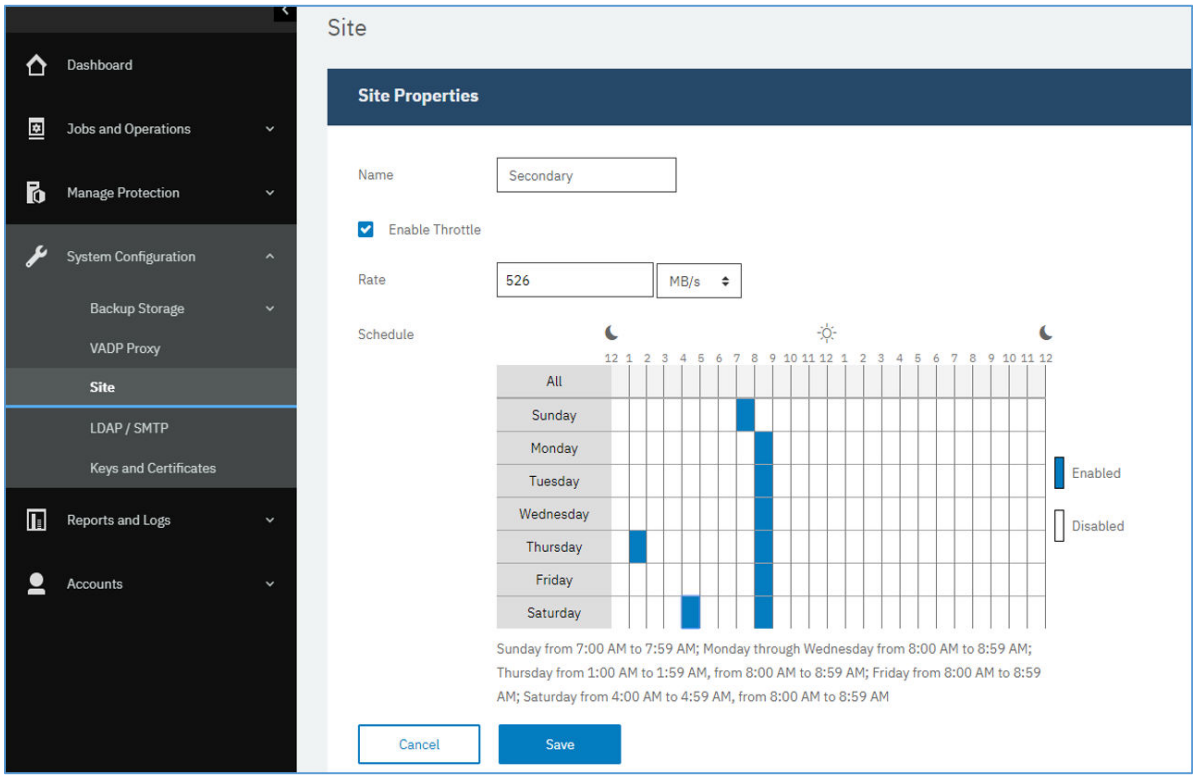


図 *30.* スループット向上のためのさまざまな時間に対する異なるスロットル速度の有効化

c) 週次スケジュール・テーブルで、スロットル用の毎日の時間を選択するか、スロットル用の特定の曜日と時間を選択します。

ヒント: 時間を選択するには、テーブル内でタイム・スロットをクリックします。選択したタイム・スロットが強調表示されます。タイム・スロットをクリアするには、強調表示されているタイム・スロットをクリックします。すべての曜日について同じタイム・スロットを選択するには、「**すべて**」行でタイム・スロットをクリックします。

選択を行うと、スロットルが設定された日と時間がスケジュール・テーブルの下にリストされます。

5.「**保存**」をクリックすると、変更がコミットされ、ペインが閉じます。

サイトの削除

サイトは、廃止されたら削除してください。必ず、バックアップ・ストレージを別のサイトに再割り当てしてから、サイトを削除してください。

手順

サイトを削除するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**サイト**」をクリックします。
2. サイトに関連付けられている削除アイコン ✕ をクリックします。
3.「**はい**」をクリックしてサイトを削除します。

LDAP サーバーと SMTP サーバーの管理

ユーザー・アカウントやレポート機能で使用するために、IBM Spectrum Protect Plus で使用する Lightweight Directory Access Protocol (LDAP) サーバーおよび Simple Mail Transfer Protocol (SMTP) サーバーを追加できます。

関連タスク

302 ページの『LDAP グループのユーザー・アカウントの作成』
IBM Spectrum Protect Plus への LDAP グループのユーザー・アカウントの追加

290 ページの『レポートのスケジューリング』
カスタマイズしたレポートを、特定の時刻に実行するよう IBM Spectrum Protect Plus でスケジュールできます。

LDAP サーバーの追加

LDAP グループを使用して IBM Spectrum Protect Plus ユーザー・アカウントを作成するには、LDAP サーバーを追加する必要があります。これらのアカウントにより、ユーザーは、LDAP ユーザー名とパスワードを使用して IBM Spectrum Protect Plus にアクセスすることができます。IBM Spectrum Protect Plus 仮想アプライアンスのインスタンスに 関連付けることができる LDAP サーバーは 1 つのみです。

このタスクについて

Microsoft Active Directory サーバーまたは OpenLDAP サーバー OpenLDAP では、通常、Active Directory と一緒に使用される sAMAaccountName ユーザー・フィルターをサポートしていないことに注意してください。また、**memberOf** オプションが OpenLDAP サーバー上で有効になっている必要があります。

手順

LDAP サーバーを登録するには、以下のステップを実行してください。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**LDAP/SMTP**」をクリックします。
2. 「**LDAP サーバー**」ペインで、「**LDAP サーバーの追加**」をクリックします。
3. 「**LDAP サーバー**」ペインで、以下のフィールドに入力します。

ホスト・アドレス

LDAP サーバーのホストまたは論理名の IP アドレス

ポート

LDAP サーバーが listen しているポート。代表的なデフォルト・ポートは、非 SSL 接続の場合は 389、SSL 接続の場合は 636 です。

SSL

LDAP サーバーへの安全な接続を確立するには、SSL オプションを有効にします。

既存のユーザーの使用

LDAP サーバーについて以前に入力されたユーザー名とパスワードを選択できるようにします。

バインド名

LDAP サーバーへの接続を認証するために使用されるバインド識別名。 IBM Spectrum Protect Plus は、単純バインドをサポートします。

パスワード

バインド識別名に関連付けられているパスワード。

基本 DN

ユーザーおよびグループを検出できる場所。

ユーザー・フィルター

特定の基準に適合する Base DN 内のユーザーのみを選択するためのフィルター。有効なデフォルト・ユーザー・フィルターの例として、`cn={0}` があります。

ヒント：

- **sAMAccountName** Windows ユーザー命名属性を使用して認証を有効にするには、フィルターを `samaccountname={0}` に設定します。このフィルターが設定されている場合、ユーザーは、ユーザー名のみを使用して IBM Spectrum Protect Plus にログインします。ドメインは含まれません。
- ユーザー・プリンシパル名 (UPN) 命名属性を使用して認証を有効にするには、フィルターを `userprincipalname={0}` に設定します。このフィルターが設定されている場合、ユーザーは、username@domain 形式を使用して IBM Spectrum Protect Plus にログインします。
- LDAP に関連付けられている E メール・アドレスを使用して認証を有効にするには、フィルターを `mail={0}` に設定します。

「**ユーザー・フィルター**」設定は、ユーザーの IBM Spectrum Protect Plus 表示に示されるユーザー名のタイプも制御します。

ユーザー RDN

ユーザーの相対識別パス。ユーザー・レコードを検出できるパスを指定してください。 有効なデフォルト RDN の例として、`cn=Users` があります。

グループ RDN

グループの相対識別パス。グループがユーザー・パスとは異なるレベルにある場合は、グループ・レコードを検出できるパスを指定してください。

4. 「**保存**」をクリックします。

タスクの結果

IBM Spectrum Protect Plus は、以下のアクションを実行します。

1. ネットワーク接続が確立されたことを確認する。
2. LDAP サーバーをデータベースに追加する。

SMTP サーバーが追加された後、「**LDAP サーバーの追加**」ボタンは使用できなくなります。

次のタスク

接続に失敗したことを示すメッセージが返された場合には、入力を確認してください。入力が正しいのに、接続に失敗する場合は、ネットワーク管理者に連絡して、接続を確認してください。

関連タスク

302 ページの『LDAP グループのユーザー・アカウントの作成』
IBM Spectrum Protect Plus への LDAP グループのユーザー・アカウントの追加

SMTP サーバーの追加

スケジュールされたレポートを E メール受信者に送信するためには、SMTP サーバーを追加する必要があります。IBM Spectrum Protect Plus 仮想アプライアンスのインスタンスに 関連付けることができる SMTP サーバーは 1 つのみです。

手順

SMTP サーバーを追加するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**システム構成**」 > 「**LDAP/SMTP**」をクリックします。
2. 「**SMTP サーバー**」ペインで、「**SMTP サーバーの追加**」をクリックします。
3. 「**SMTP サーバー**」ペインで、以下のフィールドに入力します。

ホスト・アドレス

ホストの IP アドレス、または SMTP サーバーのパスとホスト名。

ポート

追加するサーバーの通信ポート。代表的なデフォルト・ポートは、非 SSL 接続の場合は 25、SSL 接続の場合は 443 です。

ユーザー名

SMTP サーバーにアクセスするのに使用される名前。

パスワード

ユーザー名に関連付けられたパスワード。

タイムアウト

E メールのタイムアウト値 (ミリ秒)。

From アドレス

IBM Spectrum Protect Plus からの E メール通信に関連付けられたアドレス。

件名の接頭部

IBM Spectrum Protect Plus から送信された E メールの件名行に追加する接頭部。

4. 「**保存**」をクリックします。

タスクの結果

IBM Spectrum Protect Plus は、以下のアクションを実行します。

1. ネットワーク接続が確立されたことを確認する。
2. サーバーをデータベースに追加する。

接続に失敗したことを示すメッセージが返された場合には、入力を確認してください。入力が正しいのに、接続に失敗する場合は、ネットワーク管理者に連絡して、接続を確認してください。

SMTP 接続をテストするには、「**テスト SMTP サーバー**」ボタンをクリックしてから、E メール・アドレスを入力します。「**送信**」をクリックします。接続を確認するために、テスト E メール・メッセージがその E メール・アドレスに送信されます。

SMTP サーバーが追加された後、「**SMTP サーバーの追加**」ボタンは使用できなくなります。

次のタスク

関連タスク

290 ページの『レポートのスケジューリング』
カスタマイズしたレポートを、特定の時刻に実行するよう IBM Spectrum Protect Plus でスケジュールできます。

LDAP サーバーまたは SMTP サーバーの設定の編集

ご使用の IBM Spectrum Protect Plus 環境で変更を反映するよう、LDAP サーバーまたは SMTP サーバーの設定を編集します。

手順

LDAP サーバーまたは SMTP サーバーの設定を編集するには、以下のステップを実行します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**LDAP/SMTP**」をクリックします。
2. 目的のサーバーに関連付けられている編集アイコン をクリックします。
   編集ペインが表示されます。
3. 目的のサーバーの設定を修正してから、「**保存**」をクリックします。

LDAP サーバーまたは SMTP サーバーの削除

LDAP サーバーまたは SMTP サーバーは、廃止されたら削除してください。サーバーが IBM Spectrum Protect Plus によって使用されていないことを確認したうえで、サーバーを削除します。

手順

LDAP サーバーまたは SMTP サーバーを削除するには、次のステップを完了します。

1. ナビゲーション・メニューで、「**システム構成**」 > 「**LDAP/SMTP**」をクリックします。
2. 目的のサーバーに関連付けられている削除アイコン ✕ をクリックします。
3. 「**はい**」をクリックしてサーバーを削除します。

グローバル設定の適用

管理者は、「**グローバル設定**」ペインで、IBM Spectrum Protect Plus のすべての操作に適用される設定を管理できます。

始める前に

グローバル設定を管理できるのは、管理者資格情報を持つユーザーのみです。

このタスクについて

「**グローバル設定**」ペインには、IBM Spectrum Protect Plus のすべての操作に適用されるパラメーターのデフォルト値が示されます。設定は、アプリケーション、保護、およびセキュリティーの 3 つのカテゴリーで編成されます。

次の表に、グローバル設定のデフォルト値を示します。

表 *23.* グローバル設定のデフォルト値

設定	デフォルト値	単位 (該当する場合)
バックアップ・セッションの同時アプリケーション・サーバー	0	
vSnap フリー警告パーセンテージ (%)	30	パーセンテージ (%)
vSnap フリー・エラー・パーセンテージ (%)	20	パーセンテージ (%)
VM グループ・サイズ (GB) 別の VM のグループ化 (Group VMs by VM Group size (GB))	5120	ギガバイト
グループ内の VM 数別の VM のグループ化 (Group VMs by Number of VMs in group)	20	
VMware 接続タイムアウト	300	秒
バックアップ更新間隔	300	秒
パスワードの最小長	8	文字

「**グローバル設定**」ペインでデフォルト値を変更できます。

手順

1. ナビゲーション・ペインで、「**システム構成**」 > 「**グローバル設定**」をクリックします。
2. グローバル設定の値を更新します。以前に入力した値からデフォルトに戻すには、リセット・アイコン をクリックします。

設定	説明
アプリケーション	**バックアップ・セッションの同時アプリケーション・サーバー** バックアップ・セッション当たりの同時アプリケーション・サーバーの最大数。
バックアップ (ハイパーバイザー/アプリケーション)	**vSnap フリー警告パーセンテージ (%)** vSnap ストレージ・プール内の残りのフリー・スペースのパーセンテージしきい値。警告はジョブ・ログに表示されます。例えば、10 という値が指定されている場合、vSnap ストレージ・プールの残りのフリー・スペースが 10% 以下であると警告が表示されます。 **vSnap フリー・エラー・パーセンテージ (%)** vSnap ストレージ・プール内の残りのフリー・スペースのパーセンテージしきい値。エラーはジョブ・ログに表示されます。例えば、5 という値が指定されている場合、vSnap ストレージ・プールの残りのフリー・スペースが 5% 以下であるとエラーが表示されます。
ハイパーバイザー	**VM のグループ化** 仮想マシンはグループにまとめることができます。グループは、グループに含まれている VM の数またはグループに含まれている VM のサイズで定義できます。 **VMware 接続タイムアウト** 接続されている vCenter に対して実行されたコマンドの完了を IBM Spectrum Protect Plus が待機する時間。指定された時間内に操作が完了しなければ、その操作はエラーとしてログに記録されます。この設定は、VMware ハイパーバイザーのみに適用されます。 **バックアップ更新間隔** データ転送の進行に関するメッセージがジョブ・ログで更新される頻度。
セキュリティー	**パスワードの最小長** IBM Spectrum Protect Plus のパスワードの最小長。デフォルトでは、パスワードの最小長は 8 文字ですが、それよりも長いパスワードを指定できます。この値は、すべてのユーザー・アカウントに適用されます。

注 : VM グループ化の場合、4 つの VM グループがあり、各 VM グループには最大 5 つの VM を入れることができます。各グループは 1 つの宛先ボリューム (データ・ストリーム) に対応します。サイズ計算に基づき、一度に最大 20 の VM (4 つのデータ・ストリーム) を作成できます。

管理コンソールへのログオン

IBM Spectrum Protect Plus 仮想アプライアンスの 構成を確認するには、管理コンソールにログオンします。表示できる情報には、全般的なシステム設定、ネットワーク、およびプロキシー設定が含まれます。

手順

管理コンソールにログオンするには、以下のステップを実行します。

1. サポートされるブラウザーで、次の URL を入力します。

```
https://HOSTNAME:8090/
```

ここで、*HOSTNAME* は、アプリケーションがデプロイされている 仮想マシンの IP アドレスです。

2. ログイン・ウィンドウで、「**認証タイプ**」リストから以下のいずれかの認証タイプを選択します。

認証タイプ	ログオン情報
IBM Spectrum Protect Plus	SYSADMIN 特権を持つ IBM Spectrum Protect Plus ユーザーとしてログオンするには、管理者ユーザー名とパスワードを入力します。
システム	システム・ユーザーとしてログオンするには、`serveradmin` のパスワードを入力します。デフォルトのパスワードは sppDP758 です。初回ログオン中にこのパスワードの変更を求めるプロンプトが表示されます。

次のタスク

IBM Spectrum Protect Plus 仮想アプライアンスの 構成を確認します。

関連概念

11 ページの『システム 要件』

IBM Spectrum Protect Plus をインストールする前に、ストレージ環境にインストールする予定の製品やその他のコンポーネントのハードウェア要件とソフトウェア要件を検討してください。

297 ページの『役割の管理』

役割は、リソース・グループで定義されるリソースに対して実行できるアクションを定義します。リソース・グループは、アカウントから使用できるリソースを定義し、役割は、リソースと対話する許可を設定します。

タイム・ゾーンの設定

管理コンソールを使用して、IBM Spectrum Protect Plus アプライアンスのタイム ・ゾーンを設定します。

手順

タイム・ゾーンを設定するには、以下のステップを実行します。

1. サポートされているブラウザーで、次の URL を入力します。

```
https://HOSTNAME:8090/
```

   ここで、*HOSTNAME* は、アプリケーションがデプロイされている 仮想マシンの IP アドレスです。

2. ログイン・ウィンドウで、「**認証タイプ**」リストから以下のいずれかの認証タイプを選択します。

認証タイプ	ログイン情報
IBM Spectrum Protect Plus	SYSADMIN 特権を持つ IBM Spectrum Protect Plus ユーザーとしてログインするには、ご使用の管理者ユーザー名とパスワードを入力します。
システム	システム・ユーザーとしてログインするには、`serveradmin` パスワードを入力します。デフォルトのパスワードは sppDP758 です。最初のログイン時にこのパスワードの変更を求めるプロンプトが表示されます。

3. 「**システム・アクションの実行**」をクリックします。
4. 「**タイム・ゾーンの変更**」セクションで、ご使用のタイム・ゾーンを選択します。

   操作が正常に終了したことを示すメッセージが表示されます。すべての IBM Spectrum Protect Plus ログとスケジュールで、選択したタイム・ゾーンが反映されます。選択したタイム・ゾーンは、ユーザー ID **serveradmin** でログインした場合に、IBM Spectrum Protect Plus アプライアンスでも 表示されます。

5. 現行のタイム・ゾーンを表示するには、管理コンソールのメイン・ページから「**製品情報**」を選択します。

管理コンソールからの SSL 証明書のアップロード

IBM Spectrum Protect Plus で安全な接続を確立するために、管理コンソールを使用して、HTTPS 証明書または LDAP 証明書などの SSL 証明書をアップロードできます。

このタスクについて

HTTPS 証明書の場合、`.cer` 拡張子または `.crt` 拡張子を持つ PEM エンコード証明書がサポートされます。

LDAP/Hyper-V 証明書の場合は、`.cer` 拡張子または `.crt` 拡張子を持つ DER エンコード証明書がサポートされます。LDAP SSL 証明書をアップロードする場合は、IBM Spectrum Protect Plus が LDAP サーバーと接続していることと、その LDAP サーバーが実行中であることを確認してください。

ASCII およびバイナリー・フォーマットの証明書は、標準の `.pem`、`.cer`、および `.crt` の各ファイル拡張子で受け入れられます。ただし、管理コンソール証明書のインポート機能を使用して、アプライアンス SSL Web サーバー通信を更新することはできません。ASCII およびバイナリー・フォーマットの証明書をアップロードするには、277 ページの『コマンド・ラインからの SSL 証明書のアップロード』に記載されているとおりに、コマンド・ラインを使用してください。

手順

SSL 証明書をアップロードするには、以下のステップを実行します。

1. エクスポートする証明書の名前については、ネットワーク管理者に問い合わせてください。
2. サポートされているブラウザーで、ご使用のコンピューターに証明書をエクスポートします。ご使用のコンピューター上の証明書の場所を書き留めます。証明書のエクスポートのプロセスは、ご使用のブラウザーによって異なります。
3. サポートされているブラウザーで、次の URL を入力します。

   ```
   https://HOSTNAME:8090/
   ```

   ここで、*HOSTNAME* は、アプリケーションがデプロイされている 仮想マシンの IP アドレスです。
4. ログオン・ウィンドウで、「**認証タイプ**」リストから以下のいずれかの認証タイプを選択します。

認証タイプ	ログオン情報
IBM Spectrum Protect Plus	SYSADMIN 特権を持つ IBM Spectrum Protect Plus ユーザーとしてログオンするには、ご使用の管理者ユーザー名とパスワードを入力します。
システム	システム・ユーザーとしてログオンするには、`serveradmin` パスワードを入力します。デフォルトのパスワードは `sppDP758` です。最初のログオン時にこのパスワードの変更を求めるプロンプトが表示されます。

5. 「**証明書の管理**」をクリックします。
6. 「**参照**」をクリックし、アップロードしたい証明書を選択します。
7. 「**HTTPS 用の SSL 証明書のアップロード**」をクリックします。
8. アプリケーションがデプロイされている 仮想マシンを再始動します。

コマンド・ラインからの SSL 証明書のアップロード

ASCII およびバイナリー・フォーマットの証明書をアップロードするには、IBM Spectrum Protect Plus 仮想アプライアンスのコマンド・ラインを使用します。証明書は、標準の `.pem`、`.cer`、および `.crt` の各ファイル拡張子で受け入れられます。

このタスクについて

このプロセスでは、秘密鍵、公開鍵、およびチェーン証明書を 1 つの PKCS12 フォーマット・ファイル (.p12 拡張子を持つ PFX ファイルと呼ばれる場合が多い) にパッケージ化し、これを手動で IBM Spectrum Protect Plus Java 鍵ストアにインポートする必要があります。手順では、専用、公開、およびすべてのサポートするセキュリティー・オブジェクトが、*name*`.p12` という名前の PKCS12 フォーマットにパッケージされたご使用のセキュリティー・ベンダーにより既に提供されていることを前提としています。

このファイルがない場合には、必要な証明書署名要求を生成するために、別個のサーバーおよび/または OpenSSL を使用してセキュリティー・ベンダーと作業を行う必要があります。専用、公開、およびチェーン証明書オブジェクトを、以下に参照する必要なファイルにパッケージ化します。

手順

name`.p12` ファイルをインポートするには、以下のステップを実行します。

1. IBM Spectrum Protect Plus 仮想アプライアンス上でユーザー ID **serveradmin** を使用してログオンします。

   初期パスワードは sppDP758 です。
2. コマンド・ラインで、次のコマンドを実行します。

   ```
   /usr/java/latest/bin/keytool -importkeystore -deststorepass ecx-beta -
   destkeystore /opt/virgo/configuration/keystore -srckeystore NAME.p12 -
   srcstoretype PKCS12
   ```
3. 仮想アプライアンスを再始動します。

仮想アプライアンスへのログオン

コマンド・ラインにアクセスするには、vSphere Client を使用して IBM Spectrum Protect Plus 仮想アプライアンスにログオンします。コマンド・ラインには、VMware 環境でも Hyper-V 環境でもアクセスできます。

VMware での仮想アプライアンスへのアクセス

VMware 環境では、コマンド・ラインにアクセスするには、vSphere Client を使用して IBM Spectrum Protect Plus 仮想アプライアンスにログオンします。

手順

仮想アプライアンスのコマンド・ラインにアクセスするには、以下のステップを実行します。

1. vSphere Client で、IBM Spectrum Protect Plus がデプロイされている仮想マシンを選択します。
2. 「**サマリ**」タブで、「**コンソールを開く**」を選択して、コンソール内でクリックします。
3. 「**ログイン**」を選択して、ユーザー名とパスワードを入力します。デフォルトのユーザー名は `serveradmin` で、デフォルトのパスワードは sppDP758 です。

次のタスク

仮想アプライアンスを管理するためのコマンドを入力します。ログオフするには、`exit` と入力します。

Hyper-V での仮想アプライアンスへのアクセス

Hyper-V 環境では、コマンド・ラインにアクセスするには、vSphere Client を使用して IBM Spectrum Protect Plus 仮想アプライアンスにログオンします。

手順

仮想アプライアンスのコマンド・ラインにアクセスするには、以下のステップを実行します。

1. Hyper-V マネージャーで、IBM Spectrum Protect Plus がデプロイされている仮想マシンを選択します。
2. 仮想マシンを右クリックして、「**接続**」をクリックします。
3. 「**ログイン**」を選択して、ユーザー名とパスワードを入力します。デフォルトのユーザー名は `serveradmin` で、デフォルトのパスワードは `sppDP758` です。

次のタスク

仮想アプライアンスを管理するためのコマンドを入力します。ログオフするには、`exit` と入力します。

ネットワーク接続のテスト

IBM Spectrum Protect Plus Service Tool は、ホスト・アドレスとポートをテストして、接続を確立できるかどうかを確認します。Service Tool を使用すると、IBM Spectrum Protect Plus とノードとの間に接続を確立できるかどうかを確認できます。

Service Tool は IBM Spectrum Protect Plus コマンド・ラインから実行するか、.jar ファイルを使用してリモート側から実行できます。接続を確立できる場合、このツールは緑色のチェック・マークに戻ります。接続を確立できない場合は、エラー状態が、考えられる原因とアクションと一緒に表示されます。

このツールでは、以下のエラー状態のガイダンスが提供されます。

- タイムアウト
- 接続は拒否されました。
- 不明なホスト
- 経路なし

コマンド・ライン・インターフェースからのサービス・ツールの実行

IBM Spectrum Protect Plus 仮想アプライアンスのコマンド・ライン・インターフェースからサービス・ツールを開始して、Web ブラウザーでそのツールを実行できます。次に、サービス・ツールを使用して、IBM Spectrum Protect Plus とノード間のネットワーク接続を検証できます。

手順

1. `serveradmin` ユーザー ID を使用して IBM Spectrum Protect Plus 仮想アプライアンスにログインし、コマンド・プロンプトにアクセスします。次のコマンドを発行します。

   ```
   # sudo bash
   ```

2. 以下のコマンドを発行してファイアウォールでポート 9000 を開きます。

   ```
   # firewall-cmd –add-port=9000/tcp
   ```

3. 以下のコマンドを発行してツールを実行します。

   ```
   # java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxdd.jar
   ```

4. ツールに接続するには、ブラウザーで以下の URL を入力します。

   ```
   http://hostname:9000
   ```

   ここで、*hostname* は、アプリケーションがデプロイされている仮想マシンの IP アドレスを指定します。

5. テストするノードを指定するには、以下のフィールドに入力します。

   ホスト
   テストしたいノードのホスト名または IP アドレス。

   ポート
   テストする接続ポート。
6. 「**保存**」をクリックします。
7. ツールを実行するには、ツールの上にカーソルを合わせてから、緑色の「**実行**」ボタンをクリックします。
   接続が確立できない場合、考えられる原因とアクションとともにエラー状態が表示されます。
8. コマンド・ラインで以下のコマンドを発行して、ツールを停止します。

```
ctl-c
```

9. ファイアウォールをリセットして、ご使用のストレージ環境を保護します。以下のコマンドを発行します。

```
# firewall-cmd --zone=public --remove-port=9000/tcp
# firewall-cmd --runtime-to-permanent
# firewall-cmd --reload
```

注: `firewall-cmd` コマンドがご使用のシステムでは使用できない場合は、ファイアウォールを手動で編集して必要なポートを追加し、`iptables` を使用してファイアウォールを再始動してください。ファイアウォール規則の編集について詳しくは、https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1adv_firewallportopenexamples.htm で『**Firewall configuration using iptables**』セクションを参照してください。

リモートでのサービス・ツールの実行

You can download the Service Tool as a .jar file from the IBM Spectrum Protect Plus ユーザー・インターフェースからサービス・ツールを .jar ファイルとしてダウンロードできます。次に、サービス・ツールを使用して、IBM Spectrum Protect Plus とノードとの間の接続をリモートでテストできます。

手順

1. IBM Spectrum Protect Plus ユーザー・インターフェースで、ユーザー・メニューをクリックしてから、「**テスト・ツールのダウンロード**」をクリックします。
   .jar ファイルがワークステーションにダウンロードされます。
2. ツールをコマンド・ライン・インターフェースから 起動します。ツールが起動されるシステム 上でのみ、Java™ が必要です。ツールによりテストされるエンドポイントまたはターゲット・システムでは、Java は必要ありません。
   以下のコマンドは、Linux 環境でツールを起動します。

```
# java -jar -Dserver.port=9000 /<tool path >/ngxdd.jar
```

3. ツールに接続するには、ブラウザーで以下の URL を入力します。

```
http://hostname:9000
```

   ここで、*hostname* は、アプリケーションがデプロイされている 仮想マシンの IP アドレスを指定します。
4. テストするノードを指定するには、以下のフィールドに入力します。

   ホスト
   テストしたいノードのホスト名または IP アドレス。

   ポート
   テストする接続ポート。
5. 「**保存**」をクリックします。

6. ツールを実行するには、ツールの上にカーソルを合わせてから、緑色の「**実行**」ボタンをクリックします。
   接続が確立できない場合、考えられる原因とアクションとともにエラー状態が表示されます。
7. コマンド・ラインで以下のコマンドを発行して、ツールを停止します。

```
ctl-c
```

仮想ディスクの追加

vCenter を使用して、新しい仮想ディスク (ハード・ディスク) を IBM Spectrum Protect Plus 仮想アプライアンスに追加できます。

IBM Spectrum Protect Plus 仮想アプライアンスをデプロイする 場合、デプロイメント時に指定する 1 つのデータ・ストアにすべての仮想ディスクをデプロイできます。仮想アプライアンス内にディスクを追加し、それを論理ボリューム・マネージャー (LVM) として構成できます。次に、新しいディスクを新規ボリュームとしてマウントするか、新しいディスクを仮想アプライアンス内の既存のボリュームに接続することができます。

ディスクの区画を検討するには、**fdisk -l** コマンドを使用します。**pvdisplay** コマンドと **vgdisplay** コマンドを使用すると、IBM Spectrum Protect Plus 仮想アプライアンス上の物理ボリュームとボリューム・グループを検討できます。

仮想アプライアンスへのディスクの追加

vCenter クライアントを使用して、仮想マシンの設定を編集します。

始める前に

コマンドを実行するには、セキュア・シェル (SSH) を使用して IBM Spectrum Protect Plus 仮想アプライアンスのコマンド・ラインに接続し、ユーザー ID `serveradmin` を使用してログインする必要があります。デフォルトの初期パスワードは `sppDP758` です。初回ログインのときにパスワードの変更のためのプロンプトが表示されます。

手順

IBM Spectrum Protect Plus 仮想アプライアンスにディスクを 追加するには、vCenter クライアントから以下のステップを実行します。

1. vCenter クライアントから、以下のステップを実行してください。
   a)「**ハードウェア**」タブで、「**追加**」をクリックします。
   b)「**新規仮想ディスクの作成**」を選択します。
   c) 必要なディスク・サイズを選択します。「**位置**」セクションで、以下のいずれかのオプションを選択します。
   - 現在のデータ・ストアを使用する場合は、 「**この仮想マシンに格納**」を選択します。
   - 仮想ディスク用に 1 つ以上のデータ・ストアを指定する場合は、「**データ・ストアまたはデータ・ストア・クラスターを指定**」を選択します。「**参照**」をクリックして、新規データ・ストアを選択します。

   d)「**詳細オプション**」タブは、デフォルトの値のままにします。
   e) 変更内容を確認して、保存します。
   f) 仮想マシンの「**設定の編集**」オプションをクリックして、新規ハード・ディスクを表示します。
2. 仮想アプライアンスをリブートせずに、新規 SCSI デバイスを追加します。IBM Spectrum Protect Plus アプライアンスのコンソールから、以下のコマンドを発行します。

```
echo "-- -" > /sys/class/scsi_host/host#/scan
```

   ここで、# は最新のホスト番号です。

新規ディスクからアプライアンス・ボリュームへのストレージ容量の追加

仮想アプライアンスにディスクを 追加すると、新規ディスクを仮想アプライアンス内の既存のボリュームに接続できます。

始める前に

コマンドを実行するには、SSH を使用して IBM Spectrum Protect Plus 仮想アプライアンスのコンソールに接続し、ユーザー ID **serveradmin** を使用してログインする必要があります。デフォルトの初期パスワードは sppDP758 です。初回ログインのときにパスワード変更のためのプロンプトが表示されます。

このタスクについて

このタスクを実行する必要があるのは、新規ディスクのストレージ容量を既存のアプライアンス・ボリュームに追加する場合だけです。ディスクを新規ボリュームとして追加した場合は、このタスクを実行する必要はありません。

手順

新規ディスクからアプライアンス・ボリュームにストレージ容量を追加するには、仮想アプライアンスのコンソールから以下の手順を実行します。

1. 新規ディスク用に区画をセットアップし、その区画を Linux LVM タイプに設定するには、以下のステップを実行します。
   a) 以下の **fdisk** コマンドを使用して、新規ディスクを開きます。

```
[serveradmin@localhost ~]# fdisk /dev/sdd
```

   fdisk ユーティリティーが 対話モードで開始されます。以下のような出力が表示されます。

```
Device contains neither a valid DOS partition table, nor Sun, SGI or
OSF disklabel
Building a new DOS disklabel with disk identifier 0xb1b293df.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
Warning: invalid flag 0x0000 of partition table 4 will be corrected by
w(rite)
WARNING: DOS-compatible mode is deprecated. It's strongly recommended
to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help):
```

   a) **fdisk** コマンド・ラインで、**n** サブコマンドを入力して区画を追加します。

```
Command (m for help): n
```

   以下のコマンド・アクション選択項目が表示されます。

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
```

   b) **p** コマンド・アクションを入力して、1 次区画を選択します。
   区画番号を求めるプロンプトが出されます。

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
Partition number (1-4):
```

   c) 区画番号プロンプトで、区画番号 1 を入力します。

```
Partition number (1-4): 1
```

以下のプロンプトが表示されます。

```
First cylinder (1-2610, default 1):
```

d)「First cylinder」プロンプトには、何も入力しないでください。**Enter** キーを押します。
以下の出力とプロンプトが表示されます。

```
First cylinder (1-2610, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
```

e)「Last cylinder」プロンプトには、何も入力しないでください。**Enter** キーを押します。
表示される出力は次のとおりです。

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
Using default value 2610
Command (m for help):
```

f) **fdisk** コマンド・ラインで、**t** サブコマンドを入力して区画のシステム ID を変更します。

```
Command (m for help): t
```

区画タイプを識別する 16 進コードの入力が求められます。

```
Selected partition 1
Hex code (type L to list codes):
```

g) 16 進コードのプロンプトで、16 進コード 8e を入力して Linux LVM 区画タイプを指定します。
表示される出力は次のとおりです。

```
Hex code (type L to list codes): 8e
Changed system type of partition 1 to 8e (Linux LVM)
Command (m for help):
```

h) **fdisk** コマンド・ラインで **w** サブコマンドを入力し、区画テーブルを書き込んで **fdisk** ユーティリティーを終了します。

```
Command (m for help): w
```

表示される出力は次のとおりです。

```
Command (m for help): w (write table to disk and exit)
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

2. ディスクへの変更を確認するには、**fdisk -l** コマンドを発行します。
3. 物理ボリューム (PV) の現在のリストを確認するには、**pvdisplay** コマンドを発行します。
4. 新規物理ボリューム (PV) を作成するには、**pvcreate /dev/sdd1** コマンドを発行します。
5. /dev/sdd1 から新規 PV を表示するには、**pvdisplay** コマンドを発行します。
6. ボリューム・グループ (VG) を確認するには、**vgdisplay** コマンドを実行します。
7. 物理ボリューム (PV) をボリューム・グループ (VG) に追加して VG のスペースを増やすには、以下のコマンドを発行します。

```
vgextend data_vg /dev/sdd1
```

8. data_vg が拡張されていて使用する論理ボリューム (または /data ボリューム) に使用可能なフリー・スペースがあることを確認するには、**vgdisplay** コマンドを発行します。

9. 論理ボリューム (LV) の /data ボリュームを確認するには、**lvdisplay** コマンドを発行します。/data ボリュームの使用量が表示されます。
10. LV /data ボリュームの容量を総ボリューム容量に追加するには、**lvextend** コマンドを発行します。以下の例では、100 GB のボリュームに 20 GB のスペースが追加されています。

```
[serveradmin@localhost ~]# lvextend -L120gb -r /dev/data_vg/data
Size of logical volume data_vg/data changed from 100.00 GiB to 120.00 GiB .
Logical volume data successfully resized
resize2fs 1.41.12 (date)
Filesystem at /dev/mapper/data_vg-data is mounted on /data; on-line
resizing required
old desc_blocks = 7, new_desc_blocks = 8
Performing an on-line resize of /dev/mapper/data_vg-data to 31195136
(4k) blocks.
The filesystem on /dev/mapper/data_vg-data is now 31195136 blocks
long.
```

上記のコマンドを実行すると、/data ボリュームのサイズが **lvdisplay** コマンド出力に 120 GB と表示されます。

```
[serveradmin@localhost ~]# lvdisplay
--- Logical volume ---
LV Path: /dev/data_vg/data
LV Name: data
VG Name: data_vg
LV UUID: [uuid]
LV Write Access: read/write
LV Creation host, time localhost.localdomain, [date, time]
LV Status: available
# open: 1
LV Size: 120.00 GiB
Current LE: 30208
Segments : 2
Allocation inherit
Read ahead sectors: auto
- currently set to: 256
Block device: 253:1
[serveradmin@localhost ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 14G 2.6G 11G 20% /
tmpfs 16G 0 16G 0% /dev/shm
/dev/sda1 240M 40M 188M 18% /boot
/dev/mapper/data_vg-data
118G 6.4G 104G 6% /data
/dev/mapper/data2_vg-data2
246G 428M 234G 1% /data2
```

第 12 章 レポートおよびログの管理

IBM Spectrum Protect Plus は事前定義された複数のレポートを用意しています。これらのレポートは、お客様のレポート作成要件を満たすようにカスタマイズすることができます。IBM Spectrum Protect Plus でユーザーが実行するアクションのログも提供されます。

レポートのタイプ

事前定義されたレポートをカスタマイズして、バックアップ・ストレージの使用率や、システム環境のその他の側面をモニターすることができます。

レポートは、最新のインベントリー・ジョブによって収集されたデータに基づいて作成されます。すべてのカタログ作成ジョブや後続のデータベース圧縮ジョブが完了した後、レポートを生成できます。次のタイプのレポートを実行できます。

- バックアップ・ストレージの使用状況レポート
- 保護レポート
- システム・レポート
- 仮想マシン環境レポート

レポートには、レポート内の個々の値の検索、垂直スクロール、列ソートなどの対話式の要素が含まれています。

バックアップ・ストレージの使用状況レポート

IBM Spectrum Protect Plus は、ストレージの使用率や、バックアップ・ストレージの状況 (vSnap サーバーなど) を表示するバックアップ・ストレージの使用状況レポートを提供します。

バックアップ・ストレージの使用状況レポートを表示するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. 「**レポート**」ペインで「**バックアップ・ストレージの使用状況**」を展開します。

使用可能なレポートは次のとおりです。

VM のバックアップ使用率
バックアップ・ストレージ上の仮想マシン (VM) バックアップの使用率 (以下のデータを含む) を確認します。

- 各 VM の名前、ロケーション、関連ハイパーバイザー。
- VM の保護に使用される SLA ポリシー。
- バックアップ・ストレージのロケーション。バックアップ・ストレージには、ディスクのホスト名または IP アドレス、クラウド・サーバーの名前、またはリポジトリー・サーバーの名前を指定できます。
- 各 VM バックアップのサイズ。
- 各 VM で使用可能なリストア・ポイントの数。

VMware 仮想マシンの場合、結果を絞り込んで VMware タグを持つ VM を表示するには、「**タグ**」ドロップダウン・メニューから使用可能なタグを 1 つ以上選択します。デフォルト値は「**すべて**」です。これは、すべての VM バックアップのデータを表示します。

vSnap ストレージの使用状況レポート
可用性状況、フリー・スペース、使用済みスペースを含めて、vSnap サーバーのストレージ使用状況を検討します。vSnap ストレージの使用状況レポートには、vSnap サーバーの概要と、各 vSnap サーバーで保護されている個々の仮想マシンとデータベースの詳細表示の両方が表示されます。

レポート・オプションを使用して、表示する特定の vSnap サーバーをフィルターに掛けます。各 vSnap サーバーで保護されている個々の仮想マシンとデータベースの詳細表示には、「**vSnap ストレージによ**

© Copyright IBM Corp. 2017, 2019

り保護されているリソースの表示」を選択します。レポートのこの領域には、仮想マシンの名前、関連したハイパーバイザー、ロケーション、および vSnap サーバーの圧縮/重複排除率が表示されます。

IBM Spectrum Protect Plus で表示されるストレージ容量と使用状況の値は、ダッシュボードに表示される値と、vSnap ストレージの使用状況レポートに表示される値との間で異なる場合があります。ダッシュボードにはライブ情報が表示されますが、レポートには、前回実行されたインベントリー・ジョブからのデータが反映されます。丸めのアルゴリズムの相違による変動もあります。

関連概念

289 ページの『レポートのアクション』
IBM Spectrum Protect Plus でレポートを実行、保存、またはスケジュールすることができます。

285 ページの『レポートのタイプ』
事前定義されたレポートをカスタマイズして、バックアップ・ストレージの使用率や、システム環境のその他の側面をモニターすることができます。

保護レポート

IBM Spectrum Protect Plus は、リソースの保護状況を表示するレポートを提供します。レポートを表示し、必要なアクションを取ると、ユーザー定義のリカバリー・ポイント目標パラメーターを使用して、確実に、データが保護されるようにすることができます。

保護レポートを表示するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. 「**レポート**」ペインで「**保護**」を展開します。

使用可能なレポートは次のとおりです。

保護された VM と無保護の VM レポート

保護された VM と無保護の VM レポートを実行して、仮想マシンの保護状況を表示します。このレポートは、バックアップ・ジョブの開始前に IBM Spectrum Protect Plus インベントリーに追加された仮想マシンの総数を表示します。

レポート・オプションを使用して、ハイパーバイザー・タイプでフィルターに掛けたり、表示する特定のハイパーバイザーを選択します。

レポートで無保護の仮想マシンを除外するには、「**無保護の VM の非表示**」を選択します。

2 次バックアップ・ストレージにバックアップされていない仮想マシンを除外するには、「**バックアップがオフロードされた VM のみ表示**」を選択します。

「**要約表示**」に、仮想マシンの保護状況の概要が表示されます。これには、保護されていない仮想マシンと保護されている仮想マシンの数、保護されている仮想マシンの管理対象容量などが含まれます。管理対象容量とは、仮想マシンの使用されている容量です。 「**詳細の表示**」には、保護されている仮想マシンと保護されていない仮想マシンに関する詳細情報 (名前やロケーションを含む) が表示されます。

保護されたデータベースと無保護のデータベース・レポート

保護されたデータベースと無保護のデータベース・レポートを実行して、データベースの保護状況を表示します。このレポートは、バックアップ・ジョブの開始前に IBM Spectrum Protect Plus インベントリーに追加されたデータベースの総数を表示します。

レポート・オプションを使用して、表示するアプリケーション・タイプ、アプリケーション・サーバー、アプリケーション・サーバー・タイプでフィルターに掛けます。

ハイパーバイザー・ベースのバックアップ・ジョブを使用して保護されているデータベースを除外するには、「**ハイパーバイザー・バックアップの一環として保護されているデータベースの非表示**」を選択します。

レポートで無保護のデータベースを除外するには、「**無保護のデータベースの非表示**」を選択します。

「**要約表示**」に、アプリケーション・サーバーの保護状況の概要が表示されます。これには、保護されていないデータベースと保護されているデータベースの数、保護されているデータベースのフロントエンド容量などが含まれます。フロントエンド容量とは、データベースの使用されている容量です。「**詳細の表示**」には、保護されているデータベースと保護されていないデータベースに関する詳細情報 (名前やロケーションを含む) が表示されます。

VM バックアップ・ヒストリー・レポート

VM バックアップ・ヒストリー・レポートを実行して、特定の仮想マシンの保護ヒストリーを検討します。 このレポートを実行するには、少なくとも 1 つの仮想マシンが「**VM**」オプションで指定されていなければなりません。複数の仮想マシン名を選択できます。

レポート・オプションを使用して、失敗したジョブまたは成功したジョブ、および前回のバックアップの時刻でフィルターに掛けます。このレポートは、特定の SLA ポリシーでさらにフィルターに掛けることができます。「**詳細の表示**」で、関連したジョブの横にあるプラス・アイコン をクリックして、ジョブが失敗した理由や、成功したバックアップのサイズなどのジョブの 詳細を表示します。

データベース・バックアップ・ヒストリー・レポート

データベース・バックアップ・ヒストリー・レポートを実行して、特定のデータベースの保護ヒストリーを検討します。 このレポートを実行するには、少なくとも 1 つのデータベースが「**データベース**」オプションで指定されていなければなりません。複数のデータベースを選択できます。

レポート・オプションを使用して、失敗したジョブまたは成功したジョブ、および前回のバックアップの時刻でフィルターに掛けます。このレポートは、特定の SLA ポリシーでさらにフィルターに掛けることができます。「**詳細の表示**」で、関連したジョブの横にあるプラス・アイコン をクリックして、ジョブが失敗した理由や、成功したバックアップのサイズなどのジョブの 詳細を表示します。

VM SLA ポリシー RPO 適合レポート

VM SLA ポリシー RPO 適合レポートは、SLA ポリシーで定義されたリカバリー・ポイント目標に関連して仮想マシンを表示します。このレポートは、以下の情報を表示します。

- 適合している仮想マシン
- 適合していない仮想マシン
- 前回のバックアップ・ジョブ・セッションが失敗した仮想マシン

レポート・オプションを使用して、ハイパーバイザー・タイプでフィルターに掛けたり、表示する特定のハイパーバイザーを選択します。このレポートは、定義された RPO に適合している仮想マシンか、または適合していない仮想マシンでさらにフィルターに掛けることができます。

データベース SLA ポリシー RPO 適合レポート

データベース SLA ポリシー RPO 適合レポートは、SLA ポリシーで定義されたリカバリー・ポイント目標に関連してデータベースを表示します。このレポートは、以下の情報を表示します。

- 適合しているデータベース
- 適合していないデータベース
- 前回のバックアップ・ジョブ・セッションが失敗したデータベース

レポート・オプションを使用して、アプリケーション・タイプでフィルターに掛けたり、表示する特定のアプリケーション・サーバーを選択します。このレポートは、定義された RPO に適合しているデータベースまたは適合していないデータベース、もしくは (vSnap にバックアップされたデータを含む) 保護タイプ、もしくは複製を使用してさらにフィルターに掛けることができます。

関連概念

285 ページの『レポートのタイプ』

事前定義されたレポートをカスタマイズして、バックアップ・ストレージの使用率や、システム環境のその他の側面をモニターすることができます。

システム・レポート

IBM Spectrum Protect Plus は、ストレージ・システム情報、ジョブ、ジョブ状況を含めて、構成の状況の詳細を表示するシステム・レポートを提供します。

システム・レポートを表示するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. 「**レポート**」ペインで「**システム**」を展開します。

使用可能なレポートは次のとおりです。

構成レポート
使用可能なアプリケーション・サーバー、ハイパーバイザー、バックアップ・ストレージの構成を検討します。レポート・オプションを使用して、表示する構成タイプをフィルターに掛けます。このレポートには、リソースの名前、リソース・タイプ、関連したサイト、SSL 接続状況が表示されます。

ジョブ・レポート
構成内の使用可能なジョブを検討します。このレポートを実行して、タイプ別のジョブ、ジョブの平均所要時間、正常な実行のパーセンテージを表示します。レポート・オプションを使用して、表示するジョブ・タイプをフィルターに掛け、一定の期間に正常に実行されたジョブを表示します。「**要約表示**」には、タイプ別のジョブが、ジョブ・セッションの実行回数、完了回数、失敗回数と一緒にリストされます。「その他」としてリストされているジョブ・セッションは、打ち切られたジョブ、部分的に実行されたジョブ、現在実行中のジョブ、スキップされたジョブ、または停止されたジョブです。「**詳細の表示**」で、関連したジョブの横にあるプラス・アイコン をクリックして、バックアップ・ジョブによって保護されている仮想マシン、平均実行時間、および次にスケジュールされている実行時間 (ジョブがスケジュールされている場合) などのジョブの詳細を表示します。

ライセンス・レポート
ライセンス交付された機能に関連した、IBM Spectrum Protect Plus 環境の構成を検討します。このレポートには、以下のセクションとフィールドが表示されます。

仮想マシン保護
「**VM の総数**」フィールドに、ハイパーバイザー・バックアップ・ジョブにより保護されている仮想マシンの総数に加えて、アプリケーション・バックアップ・ジョブ (ハイパーバイザー・バックアップ・ジョブではなく) により保護されているアプリケーション・データベースをホスティングする仮想マシンの数が表示されます。「**フロントエンド容量**」フィールドには、これらの仮想マシンの使用済みのサイズが表示されます。

物理マシン保護
「**物理サーバーの総数**」フィールドに、アプリケーション・バックアップ・ジョブにより保護されているデータベースをホスティングする物理アプリケーション・サーバーの総数が表示されます。「**フロントエンド容量**」フィールドには、これらの物理アプリケーション・サーバーの使用済みのサイズが表示されます。

バックアップ・ストレージの使用状況 (vSnap)
「**vSnap サーバーの総数**」フィールドに、IBM Spectrum Protect Plus でバックアップの宛先として構成されている vSnap サーバーの数が表示されます。「**ターゲット容量**」フィールドに、レプリカ宛先ボリュームを除いて、vSnap サーバーの使用済みの合計容量が表示されます。

関連概念
285 ページの『レポートのタイプ』
事前定義されたレポートをカスタマイズして、バックアップ・ストレージの使用率や、システム環境のその他の側面をモニターすることができます。

VM 環境レポート

IBM Spectrum Protect Plus は、仮想マシンやデータ・ストアのストレージ使用率や状況を表示する仮想マシン環境レポートを提供します。

仮想マシン環境レポートを表示するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. 「**レポート**」ペインで「**VM 環境**」を展開します。

使用可能なレポートは次のとおりです。

VM データ・ストア・レポート

合計フリー・スペース、プロビジョンされたスペース、容量を含めて、データ・ストアのストレージ使用状況を検討します。このレポートを実行して、データ・ストア、データ・ストア上の仮想マシンの数、使用可能なスペースのパーセンテージを表示します。レポート・オプションを使用して、ハイパーバイザー・タイプでフィルターに掛けたり、表示する特定のハイパーバイザーを選択します。「**詳細の表示フィルター**」は、使用済みスペースのパーセンテージに基づいて、「**詳細の表示**」に表示されるデータ・ストアを制御します。「**孤立データ・ストアのみの表示**」フィルターを使用して、仮想マシンが

割り当てられていないデータ・ストア、またはアクセス不能状態にある仮想マシンを表示します。データ・ストアが孤立状態にある理由は、「**詳細の表示**」の「**データ・ストア**」フィールドに表示されます。

VM LUN レポート

仮想マシンの論理装置番号 (LUN) のストレージ使用状況を検討します。このレポートを実行して、LUN、関連したデータ・ストア、容量、ストレージ・ベンダーを表示します。レポート・オプションを使用して、ハイパーバイザー・タイプでフィルターに掛けたり、表示する特定のハイパーバイザーを選択します。「**孤立データ・ストアのみの表示**」フィルターを使用して、仮想マシンが割り当てられていないデータ・ストア、またはアクセス不能状態にある仮想マシンを表示します。

VM スナップショット・スプロール・レポート

このレポートには、ハイパーバイザー・リソースの保護に使用されるスナップショットの経過時間、名前、および数が表示されます。レポート・オプションを使用して、ハイパーバイザー・タイプでフィルターに掛けたり、表示する特定のハイパーバイザーを選択します。「**スナップショット作成時間**」フィルターを使用して、特定の期間のスナップショットを表示します。

VM スプロール・レポート

電源がオフになっている仮想マシン、電源がオンになっている仮想マシン、中断状態の仮想マシンを含めて、仮想マシンの状況を検討します。このレポートを実行して、使用されていない仮想マシン、それらの仮想マシンの電源がオフになった日時、および仮想マシン・テンプレートを表示します。レポート・オプションを使用して、ハイパーバイザー・タイプでフィルターに掛けたり、表示する特定のハイパーバイザーを選択します。このレポートは、前回の電源オフ以降の日数や前回の中断以降の日数を含めて、電源状態の時間の経過でさらにフィルターに掛けることができます。「**クイック・ビュー**」セクションには、電源状態に基づいて、仮想マシン上の使用済みスペースとフリー・スペースを表す円グラフが表示されます。すべてのホストまたは特定のホスト上の仮想マシンを表示するには、「**ハイパーバイザー**」フィルターを使用します。「**詳細の表示**」内の情報は、電源状態で分類されます。仮想マシン・テンプレートには、別個の表が表示されます。

VM ストレージ・レポート

このレポートで仮想マシンと関連データ・ストアを検討します。関連したデータ・ストアと、それらのデータ・ストアにプロビジョニングされているスペースを表示します。レポート・オプションを使用して、ハイパーバイザー・タイプでフィルターに掛けたり、表示する特定のハイパーバイザーを選択します。「**詳細の表示**」には、関連したデータ・ストア、および仮想ディスク・ファイルに割り振られているデータ・ストア上のスペース量が表示されます。

関連概念

285 ページの『レポートのタイプ』
事前定義されたレポートをカスタマイズして、バックアップ・ストレージの使用率や、システム環境のその他の側面をモニターすることができます。

レポートのアクション

IBM Spectrum Protect Plus でレポートを実行、保存、またはスケジュールすることができます。

レポートの実行

デフォルトのパラメーターを使用して IBM Spectrum Protect Plus レポートを実行することも、カスタム・パラメーターを使用してカスタマイズされたレポートを作成することもできます。

手順

レポートを実行するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. レポート・タイプを展開して、実行するレポートを選択します。
3. カスタム・パラメーターまたはデフォルトのパラメーターのどちらかを使用してレポートを実行します。

- カスタム・パラメーターを使用してレポートを実行するには、「**オプション**」セクションでパラメーターを設定して、「**実行**」をクリックします。パラメーターは、各レポートに固有のものです。
- デフォルトのパラメーターを使用してレポートを実行するには、「**実行**」をクリックします。

次のタスク

「**レポート**」ペインで、該当のレポートを確認します。

関連概念

285 ページの『レポートおよびログの管理』

IBM Spectrum Protect Plus は事前定義された複数のレポートを用意しています。これらのレポートは、お客様のレポート作成要件を満たすようにカスタマイズすることができます。IBM Spectrum Protect Plus でユーザーが実行するアクションのログも提供されます。

カスタム・レポートの作成

IBM Spectrum Protect Plus でカスタム・パラメーターを使用して事前定義レポートを変更し、カスタマイズしたレポートを保存できます。

手順

レポートを作成するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. 事前定義レポートを選択します。
3. カスタマイズしたパラメーターを設定します。
4. 以下のいずれかの環境で実行するレポートを定義します。
   - オンデマンドで実行する。
   - スケジュールのパラメーターで定義されたとおりにレポートを実行するスケジュールを作成する。
5. カスタマイズした名前でレポートを保存します。

次のタスク

該当のレポートを実行し、「**レポート**」ペインでレポートを確認します。

関連概念

285 ページの『レポートおよびログの管理』

IBM Spectrum Protect Plus は事前定義された複数のレポートを用意しています。これらのレポートは、お客様のレポート作成要件を満たすようにカスタマイズすることができます。IBM Spectrum Protect Plus でユーザーが実行するアクションのログも提供されます。

レポートのスケジューリング

カスタマイズしたレポートを、特定の時刻に実行するよう IBM Spectrum Protect Plus でスケジュールできます。

手順

レポートをスケジュールするには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**レポート**」をクリックします。
2. レポート・タイプを選択します。
3. スケジュールするレポートを選択します。
4. 「**オプション**」セクションでレポートのパラメーターを編集します。
5. レポートの「**名前**」フィールドと「**記述**」フィールドに値を入力します。
6. レポートのパラメーターを設定します。
7. 「**レポートのスケジュール**」セクションで、「**スケジュールの定義**」をクリックします。
8. レポートのトリガーを定義します。

9. スケジュールされたレポートを E メール形式で受信するアドレスを入力してから、「**受信者の追加**」をクリックします。
10. 「**保存**」をクリックします。

次のタスク

レポートが実行された後、受信者はそのレポートを確認できます。レポートは E メールで配信されます。

関連概念

285 ページの『レポートおよびログの管理』
IBM Spectrum Protect Plus は事前定義された複数のレポートを用意しています。これらのレポートは、お客様のレポート作成要件を満たすようにカスタマイズすることができます。IBM Spectrum Protect Plus でユーザーが実行するアクションのログも提供されます。

アクションのための監査ログの収集

監査ログを収集し、IBM Spectrum Protect Plus で実行されたアクションの検索が可能です。

手順

監査ログを収集するには、次のように行います。

1. ナビゲーション・ペインで、「**レポートとログ**」 > 「**監査ログ**」をクリックします。
2. IBM Spectrum Protect Plus で実行されたアクションのログを確認します。情報には、アクションを実行したユーザーと、アクションの説明が含まれています。
3. IBM Spectrum Protect Plus での特定のユーザーのアクションを検索するために、ユーザー検索フィールドにユーザー名を入力します。
4. オプション: 「**フィルター**」セクションを展開して、表示されたログをさらにフィルターに掛けます。特定のアクションの説明と、アクションが実行された日付範囲を入力します。
5. 検索アイコン をクリックします。
6. 監査ログを `.csv` ファイルとしてダウンロードするために、「**ダウンロード**」をクリックしてから、ファイルを保存する場所を選択します。

関連概念

301 ページの『ユーザー・アカウントの管理』
ユーザーが IBM Spectrum Protect Plus にログオンし、使用可能な機能を使用する前に、IBM Spectrum Protect Plus でユーザー・アカウントを作成しておく必要があります。

第 13 章 ユーザー・アクセスの管理

役割ベースのアクセス制御を使用すると、IBM Spectrum Protect Plus ユーザー・アカウントから使用可能なリソースや許可を設定できます。

個々のユーザーに合わせて IBM Spectrum Protect Plus を調整して、そのユーザーに必要な機能やリソースへのアクセス権を付与することができます。

リソースが IBM Spectrum Protect Plus から使用可能になった後、ハイパーバイザーや個々の画面などの上位の IBM Spectrum Protect Plus 項目と一緒にリソース・グループに追加することができます。

次に、リソース・グループに関連付けられているユーザーが実行できるアクションを定義するために、役割が構成されます。これらのアクションは、1 つ以上のユーザー・アカウントに関連付けられます。

役割ベースのアクセスを構成するには、「**アカウント**」ペインの以下のセクションを使用します。

リソース・グループ
: リソース・グループは、ユーザーが使用できるリソースを定義します。IBM Spectrum Protect Plus に追加される各リソースは、個々の IBM Spectrum Protect Plus 機能や画面と一緒に、リソース・グループに入れることができます。リソース・グループを定義すると、ユーザー・エクスペリエンスを微調整することができます。例えば、リソース・グループには、バックアップ機能やレポート作成機能のみへのアクセス権と一緒に、個々のハイパーバイザーを入れることができます。リソース・グループが役割とユーザーに関連付けられている場合、そのユーザーには、割り当てられているハイパーバイザーのバックアップとレポート作成に関連した画面のみが表示されます。

役割
: 役割は、リソース・グループで定義されるリソースで実行できるアクションを定義します。リソース・グループは、ユーザー・アカウントから使用できるリソースを定義し、役割は、リソース・グループで定義されるリソースと対話する許可を設定します。例えば、バックアップ・ジョブとリストア・ジョブを含むリソース・グループが作成される場合、役割により、ユーザーがそれらのジョブとどのように対話するかが決まります。

  リソース・グループで定義されるバックアップ・ジョブとリストア・ジョブをユーザーが作成、表示、および実行できるものの、削除はできないように、許可を設定できます。同様に、管理者アカウントを作成する許可を設定して、ユーザーが他のアカウントの作成と編集、サイトとリソースのセットアップ、および使用可能なすべての IBM Spectrum Protect Plus 機能との対話ができるようにすることもできます。

ユーザー・アカウント
: ユーザー・アカウントはリソース・グループを役割に関連付けます。ユーザーが IBM Spectrum Protect Plus にログインして、その機能を使用できるようにするには、最初に、ユーザーを個々のユーザー (ネイティブ・ユーザーと呼ばれる) として追加するか、LDAP ユーザーのインポート済みグループの一部として追加してから、リソース・グループと役割をユーザー・アカウントに割り当てる必要があります。アカウントは、リソース・グループで定義されるリソースや機能にアクセスできるだけでなく、役割で定義されるリソースや機能と対話する許可があります。

ユーザー・リソース・グループの管理

リソース・グループは、ユーザーが使用できるリソースを定義します。IBM Spectrum Protect Plus に追加される各リソースは、個々の IBM Spectrum Protect Plus 機能や画面と一緒に、リソース・グループに入れることができます。

リソース・グループの作成

ユーザーが使用できるリソースを定義するために、リソース・グループを作成します。

始める前に

アプリケーション・サーバーとしてのマシンごとに複数のアプリケーションを 1 つのリソース・グループに割り当てることはできません。例えば、SQL と Exchange が同じマシンを占有し、両方が SPP に登録さ

© Copyright IBM Corp. 2017, 2019

れている場合、そのうちの 1 つのみをアプリケーション・サーバーとして特定のリソース・グループに追加できます。

手順

リソース・グループを作成するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**リソース・グループ**」をクリックします。
2. 「**リソース・グループの作成**」をクリックします。「**リソース・グループの作成**」ペインが表示されます。
3. リソース・グループの名前を入力します。
4. 「**リソース・グループを作成する**」メニューから、以下のいずれかのオプションを選択します。

オプション	アクション
新規	a. 「**リソース・タイプを選択する**」メニューからリソース・タイプを選択します。 b. リソース・サブタイプを選択してから、「**リソースの追加**」をクリックします。リソースが「**選択されたリソース**」ビューに追加されます。
テンプレートから	a. Select a resource group from the 「**どのリソース・グループをテンプレートとして使用しますか?**」リストからリソース・グループを選択します。選択したテンプレートからのリソースが「**選択されたリソース**」ビューに追加されます。 b. 「**リソース・タイプの選択**」リストおよびその関連したリストを使用してリソースを追加できます。 使用可能なリソース・タイプおよびその使用法を確認するには、294 ページの『リソース・タイプ』を参照してください。

   グループからリソースを削除したい場合は、リソースと関連付けられている削除アイコン をクリックするか、または「**すべて削除**」をクリックしてすべてのリソースを削除します。

5. リソースの追加を終了したら、「**リソース・グループの作成**」をクリックします。

タスクの結果

そのリソース・グループは、リソース・グループ・テーブルに表示され、新規および既存のユーザー・アカウントに関連付けることができます。

次のタスク

リソース・グループを追加後に、以下のアクションを実行してください。

アクション	方法
そのリソース・グループに関連付けられたユーザー・アカウントで実行できるアクションを定義する役割を作成します。役割は、リソース・グループに定義されているリソースと対話するための許可を定義するのに使用されます。	298 ページの『役割の作成』を参照してください。

リソース・タイプ

リソース・タイプはリソース・グループの作成時に選択され、リソース・タイプにより、グループに割り当てられたユーザーが使用できるリソースが決まります。

以下のリソース・タイプとサブタイプが 使用可能です。

リソース・タイプ	サブタイプ	説明
アカウント	• 役割 • ユーザー • ID	「**アカウント**」ペインから役割とユーザーへのアクセス権を付与する場合に使用します。
アプリケーション	• Db2 • Oracle • SQL スタンドアロン/フェイルオーバー・クラスター • SQL Always On	IBM Spectrum Protect Plus でアプリケーション・サーバー上の個々のアプリケーション・データベースの表示へのアクセス権を付与する場合に使用します。
アプリケーション・サーバー	• Db2 • SQL(Q) • Oracle	個々のデータベースにアクセスすることなく、IBM Spectrum Protect Plus 内のアプリケーション・サーバーへのアクセス権を付与する場合に使用します。
ハイパーバイザー	• VMware • Hyper-V	ハイパーバイザー・リソースへのアクセス権を付与する場合に使用します。
ジョブ	なし	インベントリー・ジョブ、バックアップ・ジョブ、リストア・ジョブへのアクセス権の付与に使用します。リソースへの SLA ポリシーの割り当てを含めて、すべてのバックアップ操作とリストア操作にジョブ・リソース・グループは必須です。
報告書	• バックアップ・ストレージの使用状況 • Protection • システム • VE 環境	レポート・タイプと個々のレポートへのアクセス権の付与に使用します。
画面	なし	IBM Spectrum Protect Plus インターフェースで画面へのアクセス権を付与または拒否する場合に使用します。特定の画面がユーザーのリソース・グループに含まれていない場合、そのユーザーは、付与されている許可に関係なく、その画面で提供されている機能にアクセスできません。
SLA ポリシー	なし	バックアップ操作の SLA ポリシーへのアクセス権を付与する場合に使用します。
システム	ID	リソースへのアクセスに必要な資格情報へのアクセス権の付与に使用します。ID 機能は、「**システム**」 > 「**ID**」ペインから使用できます。

リソース・タイプ	サブタイプ	説明
システム構成	ディスク	vSnap バックアップ・ストレージ・サーバーへのアクセス権の付与に使用します。
システム構成	LDAP	ユーザー登録のために LDAP サーバーへのアクセス権を付与する場合に使用します。
システム構成	ログ	監査ログとシステム・ログの表示とダウンロードへのアクセス権の付与に使用します。
システム構成	スクリプト	アップロードされた事前スクリプトと事後スクリプトへのアクセス権の付与に使用します。
システム構成	スクリプト・サーバー	バックアップ・ジョブまたはリストア・ジョブ時にスクリプトが実行されるスクリプト・サーバーへのアクセス権の付与に使用します。
システム構成	サイト	vSnap バックアップ・ストレージ・サーバーに割り当てられるサイトへのアクセス権の付与に使用します。
システム構成	SMTP	ジョブ通知のために SMTP サーバーへのアクセス権を付与する場合に使用します。
システム構成	VADP プロキシー	VADP プロキシー・サーバーへのアクセス権の付与に使用します。

リソース・グループの編集

リソース・グループを編集して、そのグループに割り当てられているリソースおよび機能を変更できます。更新されたリソース・グループ設定は、そのリソース・グループに関連付けられているユーザー・アカウントが IBM Spectrum Protect Plus にログインした時点で有効になります。

始める前に

リソース・グループを編集する前に、以下の考慮事項を確認してください。

- ユーザー・アカウントの許可またはアクセス権限の変更時にユーザーがサインインした場合、更新された許可が有効になるためには、そのユーザーがサインアウトしてから再びサインインする 必要があります。
- 「**変更不能**」として指定されていないリソース・グループはいずれも 編集できます。

アプリケーション・サーバーとしてのマシンごとに複数のアプリケーションを 1 つのリソース・グループに割り当てることはできません。例えば、SQL と Exchange が同じマシンを占有し、両方が SPP に登録されている場合、そのうちの 1 つのみをアプリケーション・サーバーとして特定のリソース・グループに追加できます。

手順

リソース・グループを編集するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**リソース・グループ**」をクリックします。
2. リソース・グループを選択し、そのリソース・グループについてのオプション ・アイコン ••• をクリックします。「**リソースの変更**」をクリックします。

3. リソース・グループ名またはリソース、あるいはその両方を修正します。
4.「**リソース・グループの更新**」をクリックします。

リソース・グループの削除

「**変更不能**」として指定されていないリソース・グループはいずれも削除できます。

手順

リソース・グループを削除するには、次のステップを完了します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**リソース・グループ**」をクリックします。
2. リソース・グループを選択し、そのリソース・グループについてのオプション ・アイコン をクリックします。「**リソース・グループの削除**」をクリックします。
3.「**はい**」をクリックします。

役割の管理

役割は、リソース・グループで定義されるリソースに対して実行できるアクションを定義します。リソース・グループは、アカウントから使用できるリソースを定義し、役割は、リソースと対話する許可を設定します。

例えば、バックアップ・ジョブとリストア・ジョブを含むリソース・グループが作成される場合、役割により、ユーザーがそれらのジョブとどのように対話するかが決まります。リソース・グループで定義されるバックアップ・ジョブとリストア・ジョブをユーザーが作成、表示、および実行できるものの、削除はできないように、許可を設定できます。

同様に、管理者アカウントを作成する許可を設定して、ユーザーが他のアカウントの作成と編集、サイトとリソースのセットアップ、および使用可能なすべての IBM Spectrum Protect Plus 機能との対話ができるようにすることもできます。

役割の機能は、正しく構成されたリソース・グループによって異なります。事前定義された役割を選択するか、カスタム役割を構成する際に、必要な IBM Spectrum Protect Plus の操作、画面、およびリソースへのアクセス権が、役割の推奨される使用法と一致することを確認する必要があります。

以下のユーザー・アカウント役割が使用可能です。

アプリケーション管理者

「アプリケーション管理者」の役割では、ユーザーは以下のアクションを実行できます。

- 管理者が委任するアプリケーション・データベース・リソースを登録し、変更する。
- アプリケーション・データベースを、割り当てられた SLA ポリシーに関連付ける。
- バックアップ操作とリストア操作を実行する。
- ユーザーにアクセス権があるレポートを実行し、スケジュールする。

リソースへのアクセス権は、「**アカウント**」 > 「**リソース・グループ**」ペインを使用して管理者が付与する必要があります。

バックアップのみ

「バックアップのみ」の役割では、ユーザーは以下のアクションを実行できます。

- バックアップ操作を実行、編集、およびモニターする。
- ユーザーにアクセス権がある SLA ポリシーを表示、作成、および編集する。

特定のバックアップ・ジョブを含めて、リソースへのアクセス権は、「**アカウント**」 > 「**リソース・グループ**」をクリックして管理者が付与する必要があります。

リストアのみ

「リストアのみ」の役割では、ユーザーは以下のアクションを実行できます。

- リストア操作を実行、編集、およびモニターする。
- ユーザーにアクセス権がある SLA ポリシーを表示、作成、および編集する。

特定のリストア・ジョブを含めて、リソースへのアクセス権は、「**アカウント**」 > 「**リソース・グループ**」ペインを使用して管理者が付与する必要があります。

セルフサービス

「セルフサービス」の役割では、ユーザーは、管理者が委任する既存のバックアップ操作とリストア操作をモニターすることができます。

特定のジョブを含めて、リソースへのアクセス権は、「**アカウント**」 > 「**リソース・グループ**」ペインを使用して管理者が付与する必要があります。

SYSADMIN

SYSADMIN 役割は管理者役割です。この役割では、すべてのリソースと特権にアクセスできます。

この役割を持つユーザーは、ユーザーを追加でき、admin ユーザー以外のすべてのユーザーに対して以下のアクションを実行できます。

- ユーザー・アカウントを変更し、削除する。
- ユーザー・パスワードを変更する。
- ユーザーの役割を割り当てる。

また、管理者は、コンソールのログイン・ウィンドウにある「**認証タイプ**」リストから「**IBM Spectrum Protect Plus**」を選択し、管理者の資格情報を入力して、管理コンソールにアクセスすることもできます。

管理コンソールから、管理者はソフトウェア更新の適用、IBM Spectrum Protect Plus アプライアンスの再始動、およびローカル・タイム・ゾーンの設定を行うことができます。

管理コンソールの使用について詳しくは、274 ページの『管理コンソールへのログオン』を参照してください。

VM 管理者

「VM 管理者」の役割では、ユーザーは以下のアクションを実行できます。

- ユーザーにアクセス権があるハイパーバイザー・リソースを登録し、変更する。
- ハイパーバイザーを SLA ポリシーに関連付ける。
- バックアップ操作とリストア操作を実行する。
- ユーザーにアクセス権があるレポートを実行し、スケジュールする。

リソースへのアクセス権は、「**アカウント**」 > 「**リソース・グループ**」ペインを使用して管理者が付与する必要があります。

役割の作成

リソース・グループに関連付けられたアカウントのユーザーが実行できるアクションを定義する役割を作成します。役割は、リソース・グループに定義されているリソースと対話するための許可を定義するのに使用されます。

手順

ユーザー役割を作成するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**役割**」をクリックします。
2. 「**役割の作成**」をクリックします。「**役割の作成**」ペインが表示されます。
3. 「**役割を作成します**」リストから、以下のいずれかのオプションを選択します。

オプション	アクション
新規	役割に適用する許可を選択します。デフォルトでは、いずれの許可も事前選択されていません。
テンプレートから	a. 「**どの役割をテンプレートとして使用しますか?**」メニューから役割を選択します。テンプレート役割に関連付けられている許可は、デフォルトで選択されています。

オプション	アクション
	b. その役割に適用する追加の許可を選択し、必要でない許可を削除します。 使用可能な許可とその使用法を確認するには、299 ページの『許可タイプ』を参照してください。

4. 役割の名前を入力してから、「**役割の作成**」をクリックします。

タスクの結果
新しい役割は、役割テーブルに表示され、新規および既存のユーザー・アカウントに適用することができます。

許可タイプ
許可タイプはユーザー・アカウントの作成時に選択され、許可タイプにより、ユーザーが使用できる許可が決まります。

以下の許可が使用可能です。

名前	許可	説明
アプリケーション	表示	IBM Spectrum Protect Plus でアプリケーション・サーバー上の個々のアプリケーション・データベースを表示する場合に使用します。
アプリケーション・サーバー	登録、表示、編集、登録取り消し	個々のデータベースにアクセスすることなく、SQL Server や Oracle サーバーなどのアプリケーション・サーバーと対話する場合に使用します。
証明書	作成、表示、編集、削除	クラウド・サーバーにアクセスするために SSL 証明書と対話する場合に使用します。
クラウド	登録、表示、編集、登録取り消し	オフロード用のバックアップ・ストレージとして定義されるクラウド・サーバーとの対話に使用します。
ハイパーバイザー	登録、表示、編集、登録取り消し、オプション	VMware 仮想マシンまたは Hyper-V 仮想マシンなどのハイパーバイザー仮想マシンとの対話に使用します。
ID および鍵	作成、表示、編集、削除	リソースへのアクセスに必要な資格情報との対話に使用します。ID 機能は、「アカウント」>「ID」ペインから使用できます。
LDAP	登録、表示、編集、登録取り消し	ユーザー登録のために LDAP サーバーと対話する場合に使用します。
ログ	表示	監査ログとシステム・ログを表示する場合に使用します。

名前	許可	説明
ジョブ	作成、表示、編集、実行、削除	インベントリー・ジョブ、バックアップ・ジョブ、リストア・ジョブとの対話に使用します。**注:** ジョブを**実行**する許可がユーザーにある場合、そのジョブに対するカスタム・リストア・アクションの**保留**、**解除**、および**実行**を行うこともできます。
VADP プロキシー	登録、表示、編集、登録取り消し	VADP との対話に使用します。
報告書	作成、表示、編集、削除	レポートとの対話に使用します。
リソース・グループ	作成、表示、編集、削除	ユーザーが使用できる IBM Spectrum Protect Plus リソースを定義するリソース・グループとの対話に使用します。
役割	作成、表示、編集、削除	リソース・グループで定義されるリソースで実行できるアクションを定義する役割との対話に使用します。
スクリプト	アップロード、表示、置き換え、削除	IBM Spectrum Protect Plus に追加され、ジョブの前または後に実行される事前スクリプトと事後スクリプトとの対話に使用します。
サイト	作成、表示、編集、削除	vSnap バックアップ・ストレージ・サーバーに割り当てられるサイトとの対話に使用します。
SMTP	登録、表示、編集、登録取り消し	ジョブ通知のために SMTP サーバーと対話する場合に使用します。
バックアップ・ストレージ	登録、表示、編集、登録取り消し	vSnap バックアップ・ストレージ・サーバーとの対話に使用します。
SLA ポリシー	作成、表示、編集、削除	バックアップ・ジョブ用にカスタマイズされたテンプレートをユーザーが作成できるようにする SLA ポリシーとの対話に使用します。
ユーザー	作成、表示、編集、削除	リソース・グループを役割に関連付け、IBM Spectrum Protect Plus ユーザー・インターフェースにアクセスできるようにするユーザーとの対話に使用します。

役割の編集

役割を編集して、その役割に割り当てられているリソースおよび許可を変更できます。更新された役割設定は、その役割に関連付けられているユーザー・アカウントが IBM Spectrum Protect Plus にログインした時点で有効になります。

始める前に

役割を編集する前に、以下の考慮事項を確認してください。

- ユーザー・アカウントの許可またはアクセス権限の変更時にユーザーがサインインした場合、更新された許可が有効になるためには、そのユーザーがサインアウトしてから再びサインインする必要があります。
- 「**変更不能**」として指定されていない役割はいずれも編集できます。

手順

ユーザー役割を編集するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**役割**」をクリックします。
2. 役割を選択し、その役割についてのオプション・アイコン ••• をクリックします。「**役割の変更**」をクリックします。
3. 役割名または許可、あるいはその両方を修正します。
4. 「**役割の更新**」をクリックします。

役割の削除

「**変更不能**」として指定されていない役割を削除することができます。

手順

役割を削除するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**役割**」をクリックします。
2. 役割を選択し、その役割についてのオプション・アイコン ••• をクリックします。「**役割の削除**」をクリックします。
3. 「**はい**」をクリックします。

ユーザー・アカウントの管理

ユーザーが IBM Spectrum Protect Plus にログオンし、使用可能な機能を使用する前に、IBM Spectrum Protect Plus でユーザー・アカウントを作成しておく必要があります。

個別のユーザーのユーザー・アカウントの作成

IBM Spectrum Protect Plus で個別のユーザーのアカウントを追加します。10.1.1 より前のバージョンの IBM Spectrum Protect Plus からアップグレードする場合、前のバージョンでユーザーに割り当てられている許可を IBM Spectrum Protect Plus で再割り当てする必要があります。

始める前に

カスタム役割とリソース・グループを使用したい場合は、それらを作成してから、ユーザーを作成してください。293 ページの『リソース・グループの作成』および298 ページの『役割の作成』を参照してください。

手順

個別のユーザーのアカウントを作成するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ユーザー**」をクリックします。
2. 「**ユーザーの追加**」をクリックします。「**ユーザーの追加**」ペインが表示されます。
3. 「**追加するユーザーまたはグループのタイプを選択**」 > 「**個別の新規ユーザー**」をクリックします。
4. ユーザーの名前とパスワードを入力します。
5. 「**役割の割り当て**」セクションで、ユーザーに対して 1 つ以上の役割を選択します。
6. 「**許可グループ**」セクションで、ユーザーが使用できる許可とリソースを確認してから、「**続行**」をクリックします。
7. 「**ユーザーの追加 - リソースの割り当て**」セクションで、1 つ以上のリソース・グループをユーザーに割り当ててから、「**リソースの追加**」をクリックします。

リソース・グループは、「**選択されたリソース**」セクションに追加されます。

8.「**ユーザーの作成**」をクリックします。

タスクの結果

ユーザー・アカウントがユーザー・テーブルに表示されます。テーブルからユーザーを選択して、使用可能な役割、許可、およびリソース・グループを表示します。

LDAP グループのユーザー・アカウントの作成

IBM Spectrum Protect Plus への LDAP グループのユーザー・アカウントの追加

始める前に

LDAP グループのユーザー・アカウントを作成する前に、以下の手順を確認してください。

- IBM Spectrum Protect Plus に LDAP プロバイダーを登録します。270 ページの『LDAP サーバーの追加』を参照してください。
- カスタム役割とリソース・グループを使用したい場合は、それらを作成してから、ユーザーを作成してください。293 ページの『リソース・グループの作成』および 298 ページの『役割の作成』を参照してください。

手順

LDAP グループのユーザー・アカウントを作成するには、以下のステップを確認してください。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ユーザー**」をクリックします。
2.「**ユーザーの追加**」をクリックします。「**ユーザーの追加**」ペインが表示されます。
3.「**追加するユーザーまたはグループのタイプを 選択**」 > 「**LDAP グループ**」をクリックします。
4. LDAP グループを選択します。
5.「**役割の割り当て**」セクションで、ユーザーに対して 1 つ以上の役割を選択します。
6.「**許可グループ**」セクションで、ユーザーが使用できる許可とリソースを確認してから、「**続行**」をクリックします。
7.「**ユーザーの追加 - リソースの割り当て**」セクションで、1 つ以上のリソース・グループをユーザーに割り当ててから、「**リソースの追加**」をクリックします。

   リソース・グループは、「**選択されたリソース**」セクションに追加されます。
8.「**ユーザーの作成**」をクリックします。

タスクの結果

ユーザー・アカウントがユーザー・テーブルに表示されます。テーブルからユーザーを選択して、使用可能な役割、許可、およびリソース・グループを表示します。

ユーザー・アカウントの編集

ユーザー・アカウントのユーザー名、パスワード、関連したリソース・グループ、および役割を編集できます。ただし、SUPERUSER 役割に割り当てられているユーザーは例外です。ユーザーが SUPERUSER 役割のメンバーである場合、ユーザーのパスワードのみ変更できます。

始める前に

ユーザー・アカウントの許可またはアクセス権限の変更時にユーザーがサインインした場合、更新された許可が有効になるためには、そのユーザーがサインアウトしてから再びサインインする必要があります。

手順

ユーザー・アカウントの資格情報を編集するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ユーザー**」をクリックします。

2. ユーザーを 1 人以上選択します。異なる役割を持つ複数のユーザーを選択した場合、それぞれのリソースのみ変更できますが、役割は変更できません。
3. オプション・アイコン *** をクリックして、使用可能なオプションを確認します。示されるオプションは、選択したユーザー (単数または複数) によって異なります。

   設定の変更
   ユーザー名とパスワード、関連した役割、およびリソース・グループを編集します。

   リソースの変更
   関連したリソース・グループを編集します。
4. ユーザーの設定を変更してから、「**ユーザーの更新**」または「**リソースの割り当て**」をクリックします。

ユーザー・アカウントの削除

いずれのユーザー・アカウントも削除できます。ただし、SUPERUSER 役割に割り当てられているユーザーは例外です。

手順

ユーザー・アカウントを削除するには、以下のステップを実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ユーザー**」をクリックします。
2. ユーザーを選択します。
3. オプション・アイコン *** をクリックしてから、「**ユーザーの削除**」をクリックします。

ID の管理

IBM Spectrum Protect Plus の一部の機能には、リソースにアクセスするための資格情報が必要です。例えば、IBM Spectrum Protect Plus は、カタログ作成、データ保護、データ・リストアのようなタスクを実行するために、登録時に指定されたローカル・オペレーティング・システム・ユーザーとして Oracle サーバーに接続します。

リソースのユーザー名とパスワードは、「**ID**」ペインを使用して追加および編集できます。リソースへのアクセスに資格情報を必要とする IBM Spectrum Protect Plus の機能を使用する場合、「**既存のユーザーの使用**」を選択し、ドロップダウン・メニューから ID を選択します。

ID の追加

ユーザー資格情報を提供するために、ID を追加します。

手順

ID を追加するには、以下の手順を実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ID**」をクリックします。
2. 「**ID の追加**」をクリックします。
3. 「**ID のプロパティー**」ペインで、各フィールドに入力します。

   名前

   ID を識別するために役立つ分かりやすい名前を入力します。

   ユーザー名

   SQL サーバーや Oracle サーバーなどのリソースに関連付けられているユーザー名を入力します。

   パスワード

   リソースに関連付けられているパスワードを入力します。
4. 「**保存**」をクリックします。
   ID が ID テーブルに表示され、リソースにアクセスする資格情報が必要な機能を利用するときに、「**既存のユーザーの使用**」オプションから選択できるようになります。

ID の編集

ID を修正して、関連リソースへのアクセスに使用するユーザー名とパスワードを変更することができます。

手順

ID を編集するには、以下の手順を実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ID**」をクリックします。
2. ID に関連付けられている編集アイコン をクリックします。
   「**ID プロパティー**」ペインが表示されます。
3. ID 名、ユーザー名、およびパスワードを修正します。
4. 「**保存**」をクリックします。
   修正された ID が ID テーブルに表示され、リソースにアクセスする資格情報が必要な機能を利用するときに、「**既存のユーザーの使用**」オプションから選択できるようになります。

ID の削除

廃止された ID は削除できます。ID が登録済みアプリケーション・サーバーに関連付けられている場合は、まずアプリケーション・サーバーから ID を削除する必要があります。関連付けを削除するには、アプリケーション・サーバーのタイプに関連した「**バックアップ**」 > 「**アプリケーション・サーバーの管理**」ページにナビゲートし、アプリケーション・サーバーの設定を編集します。

手順

ID を削除するには、以下の手順を実行します。

1. ナビゲーション・ペインで、「**アカウント**」 > 「**ID**」をクリックします。
2. ID に関連付けられている削除アイコン をクリックします。
3. 「**はい**」をクリックして ID を削除します。

第 14 章 ライセンス交付

IBM Spectrum Protect Plus では、現在の使用法がライセンス資格レベル内にあるかどうかを判別するため、および潜在的なライセンス違反を防止するために、ライセンス監査がデフォルトで有効になります。

IBM Spectrum Protect Plus は、資格監査ログを IBM® ソフトウェア・ライセンス・メトリック・タグ (.slmtag) ファイルとして生成します。次に IBM® License Metric Tool (ILMT) を使用して、ファイルを変換し、License Consumption Reports を生成します。このセクションの情報を使用して、.slmtag ファイルを解釈してください。

ソフトウェア・ライセンス・メトリック (SLM) タグ

IBM Spectrum Protect Plus は、資格監査ログを IBM® ソフトウェア・ライセンス・メトリック・タグ (.slmtag) ファイルとして生成します。次に IBM® License Metric Tool (ILMT) を使用して、ファイルを変換し、License Consumption Reports を生成します。提供された情報を使用して、.slmtag ファイルを解釈してください。

.slmtag ファイルは、最大ファイル・サイズ 1 MB まで情報を保管できます。それを超えると、ファイルはアーカイブされ、新しいログ・ファイルが作成されます。最大 10 個のログ・ファイルが保持されます。

アップグレード要件 : 旧リリースから IBM Spectrum Protect Plus 10.1.3 にアップグレードしようとする場合は、メンテナンス・ジョブを実行して .slmtag ファイルを生成する必要があります。今後のアップグレードに備えて、メンテナンス・ジョブを実行して既存の .slmtag ファイルを更新しておく必要があります。

ログの形式

.slmtag ファイルは XML 形式で保管され、新しいメトリック・レコードがファイルの終わりに付加されます。

.slmtag のサンプル・ファイルは次のとおりです。

```
<SchemaVersion>2.1.1</SchemaVersion>
<SoftwareIdentity>
   <SoftwareIdentity name>"IBM Spectrum Protect Plus"</Name>
   <InstanceId>/opt/virgo</InstanceId>
</SoftwareIdentity>
<Metric logTime ="2018-11-05T16:05:09+00:00">
   <Type>HYPERVISOR_SERVER_COUNT</Type>
   <SubType>HYPERVISOR_SERVER_COUNT</SubType>
   <Value>0</Value>
   <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
   </Period>
</Metric>
<Metric logTime="2018-11-05T16:05:09+00:00">
   <Type>APPLICATION_INSTANCE_COUNT</Type>
   <SubType>APPLICATION_INSTANCE_COUNT</SubType>
   <Value>0</Value>
   <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
   </Period>
</Metric>
```

ここで、Value エレメントは、EndTime エレメント内の指定された時刻に、インスタンス・グループ用にパッケージがデプロイされたすべてのリソース・グループ内のホスト数を示します。

時間の経過につれてファイルが大きくなると、古いメトリック・エレメントを削除するためにファイルを編集することができます。必ず、ILMT のスキャンに十分な時間の間、エレメントを保持してください。ス

© Copyright IBM Corp. 2017, 2019

キャン頻度は ILMT 管理者によって決定されますが、通常、エレメントを保持するのに十分な時間は 1 カ月です。

ログのロケーション

`.slmtag` ファイルは /data/slmtag ディレクトリーにあります。

関連概念

247 ページの『ジョブ・タイプ』
IBM Spectrum Protect Plus におけるバックアップ操作、リストア操作、メンテナンス操作、およびインベントリー操作の実行に、ジョブを使用します。

関連タスク

248 ページの『ジョブの開始』
いずれのジョブも、スケジュールで実行するよう設定されている場合でも、オンデマンドで実行できます。

IBM License Metric Tool (ILMT) の組み込み

License Metric Tool (ILMT) を使用すると、システム環境がライセンス要件に準拠しているかどうかの確認に役立ちます。

ILMT は、仮想化環境の管理およびライセンス使用状況の計測のための有用な機能を備えています。ILMT は、ユーザーのインフラストラクチャーにインストールされたソフトウェアを 検出し、使用量データの分析を支援し、監査レポートの生成を可能にします。各レポートでは、コンピューター・グループ、ソフトウェア・インストール、ソフトウェア・カタログのコンテンツなど、インフラストラクチャーに関する各種情報が提供されます。

デフォルトでは、すべての ILMT 監査レポートで直近 90 日間のデータが示されます。レポートに表示される情報のタイプと量をフィルターを使用してカスタマイズでき、将来の使用のために個人用設定を保存することができます。レポートを .csv または .pdf 形式にエクスポートすることもでき、また、重要なイベントが発生したときに指定の受信者に通知されるようにレポートの E メール送信をスケジュールすることもできます。

詳しくは、IBM License Metric Tool 製品資料を参照してください。

第 15 章 トラブルシューティング

問題を診断して解決するために、トラブルシューティングの 手順もご利用いただけます。

IBM Spectrum Protect Plus リリースごとの既知の問題や制約事項のリストについては、技術情報 2014120 を参照してください。

トラブルシューティング用のログ・ファイルの収集

IBM Spectrum Protect Plus アプリケーションのトラブルシューティングを 行うために、IBM Spectrum Protect Plus によって生成されたログ・ファイルのアーカイブをダウンロードできます。

手順

トラブルシューティングのためにログ・ファイルを収集するには、以下のステップを実行します。

1. ユーザー・メニューをクリックしてから、**[システム・ログのダウンロード**」をクリックします。
   ダウンロード・プロセスは、完了するまでに少し時間がかかる場合があります。
2. ファイル・ログの zip ファイルを開くか、保存します。このファイルには、各種 IBM Spectrum Protect Plus コンポーネントの個別のログ・ファイルが含まれています。

   ログ・ファイルについては、アプリケーションの保護またはハイパーバイザー・バックアップの保護のセクションを参照してください。

次のタスク

問題のトラブルシューティングを 行うには、以下のステップを実行します。

1. ログ・ファイルを分析し、問題を解決するのに適切なアクションを行います。
2. 問題を解決できない場合は、ログ・ファイルを IBM ソフトウェア・サポートに送信して、支援を求めます。

© Copyright IBM Corp. 2017, 2019

第 16 章 製品メッセージ

IBM Spectrum Protect Plus コンポーネントは、発行元のコンポーネントの識別に役立つ接頭部を付けてメッセージを送信します。固有 ID を使用して特定のメッセージを見つけるには、検索オプションを使用してください。

メッセージは以下の要素で構成されています。

- 5 文字の接頭部。
- メッセージを識別する番号。
- 画面に表示され、メッセージ・ログに書き込まれる、メッセージ・テキスト。

ヒント: 探しているメッセージ・コードを見つけるには、Ctrl+F を押してブラウザーの検索機能を使用してください。

以下に、Db2 エージェントの接頭部が付加されたメッセージの例を示します。「More」をクリックすると、メッセージの理由を説明する追加の詳細が表示されます。

```
警告
Apr 16, 2019
9:14:37 AM
GTGGH0098
[myserver1.myplace.irl.ibm.com]
Database AC7 will not be backed up as it is ineligible for the backup operation. More
```

IBM Spectrum Protect Plus メッセージ接頭語

メッセージには異なる接頭部が付いており、そのメッセージを出すコンポーネントを特定する上で役立ちます。

以下の表は、各コンポーネントと関連する接頭語を示しています。

表 *24.* コンポーネント別のメッセージ接頭語

接頭部	**コンポーネント**
CTGGA	IBM Spectrum Protect Plus
CTGGE	IBM Spectrum Protect Plus for Microsoft SQL Server
CTGGF	IBM Spectrum Protect Plus for Oracle
CTGGG	IBM Spectrum Protect Plus for Microsoft Exchange Server
CTGGH	IBM Spectrum Protect Plus for IBM Db2
CTGGI	IBM Spectrum Protect Plus for MongoDB

すべてのメッセージのリストについては、IBM Knowledge Centre (ここをクリック) 参照してください。

© Copyright IBM Corp. 2017, 2019

付録 A 検索ガイドライン

ファイルやリストア・ポイントなどのエンティティーの 検索には、フィルターを 使用します。

文字ストリングを入力して、その文字ストリングと正確に一致する名前を持つオブジェクトを検索できます。例えば、`string.txt` という用語を検索すると、完全一致突き合わせ `string.txt` が戻されます。

正規表現検索項目もサポートされます。詳しくは、正規表現によるテキストの検索を参照してください。

また、検索には以下の特殊文字も含むことができます。特殊文字の前に円記号 (¥) エスケープ文字を使用する必要があります。

```
+ - & | ! ( ) { } [ ] ^ " ~ * ? : \
```

例えば、`string[2].txt` ファイルを検索するには、`string¥[2¥].txt` と入力します。

ワイルドカードを使用した検索

ストリングの先頭、中央、または終わりにワイルドカードを配置し、ストリング内でワイルドカードを組み合わせることができます。

アスタリスクと文字ストリングを突き合わせる

次の例では、アスタリスクを使用する検索テキストを示します。

- `string*` は、string、strings、または stringency のような用語を検索します
- `str*ing` は、string、straying、または straightening のような用語を検索します
- `*string` は string または shoestring のような用語を検索します

単一のテキスト・ストリングで複数のアスタリスク・ワイルドカードを使用できますが、複数のワイルドカードを使用すると大規模な検索の速度が大幅に低下する場合があります。

疑問符と単一文字を突き合わせる

次の例では、疑問符を使用する検索テキストを示します。

- `string?` は、strings、stringy、または string1 のような用語を検索します
- `st??ring` は、starring または steering のような用語を検索します
- `???string` は、hamstring または bowstring のような用語を検索します

© Copyright IBM Corp. 2017, 2019

付録 B IBM Spectrum Protect 製品ファミリーのアクセシビリティー機能

アクセシビリティー機能は、運動障害または視覚障害などの障害を持つユーザーが情報技術コンテンツを快適に使用できるように支援します。

概説

IBM Spectrum Protect ファミリーの製品は、以下の主なアクセシビリティー機能を提供します。

- キーボードのみによる操作
- スクリーン・リーダー (読み上げソフトウェア) に使用する操作

IBM Spectrum Protect ファミリー製品は、最新の W3C 標準 WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/) が、US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) および Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) に準拠するように使用されています。 アクセシビリティー機能を利用するには、最新リリースのスクリーン・リーダーと、この製品によってサポートされる最新の Web ブラウザーを使用してください

IBM Knowledge Center の製品資料は、アクセシビリティーに対応しています。 IBM Knowledge Center のアクセシビリティー機能については、 the IBM Knowledge Center ヘルプの「Accessibility」セクション (www.ibm.com/support/knowledgecenter/about/releasenotes.html#accessibility) に記載されています。

キーボード・ナビゲーション

この製品は、標準のナビゲーション・キーを使用します。

インターフェース情報

ユーザー・インターフェースには、1 秒当たり 2 回から 55 回の点滅を行うコンテンツはありません。

Web ユーザー・インターフェースでは、コンテンツを正しくレンダリングするために、また使いやすさを実現するために、カスケーディング・スタイル・シートが使用されています。このアプリケーションには、視覚に障害のあるユーザーがシステム 表示設定を使用するための、同等の方式 (ハイコントラスト・モードなど) が用意されています。 フォント・サイズの制御は、デバイスまたは Web ブラウザーの設定を使用して行うことができます。

Web ユーザー・インターフェースには、アプリケーションの機能領域に素早くナビゲートできる WAI-ARIA ナビゲーション・ランドマークが含まれています。

ベンダー・ソフトウェア

IBM Spectrum Protect 製品ファミリーには、IBM の使用許諾契約書の対象とならないベンダー・ソフトウェアが含まれます。IBM は、それらの製品のアクセシビリティー機能を保証するものではありません。ベンダーの製品のアクセシビリティー機能については、ベンダーにお問い合わせください。

関連アクセシビリティー情報

IBM では、標準の IBM ヘルプ・デスクとサポート Web サイトに加えて、聴覚に障害のあるお客様が営業担当者やサポート・サービスに連絡が取れるように TTY 電話サービスを開設しています。

TTY サービス
800-IBM-3383 (800-426-3383)
(北アメリカ内)

IBM のアクセシビリティーに対する取り組みについて詳しくは、IBM Accessibility (www.ibm.com/able) を参照してください。

© Copyright IBM Corp. 2017, 2019

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。 この資料は、IBM から他の言語でも提供されている可能性があります。ただし、これを入手するには、本製品または当該言語版製品を所有している必要がある場合があります。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。 本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。 これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。 ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について 実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 *103-8510*
東京都中央区日本橋箱崎町 *19* 番 *21* 号
日本アイ ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するま まの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕 疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとし ます。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。 本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部では ありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。 実際の結果は、異なる可能性があります。

© Copyright IBM Corp. 2017, 2019

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。 より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、 名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。 お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション ・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。 このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。 従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性が あることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物には、 次のように、著作権表示を入れていただく必要があります。「© (お客様の会社名) (西暦年).このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_.

商標

IBM、IBM ロゴ、および ibm.com® は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、 www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe は、Adobe Systems Incorporated の米国およびその他の国における登録商標です。

Linear Tape-Open、LTO、および Ultrium は、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

Intel および Itanium は、Intel Corporation または子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。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、および Windows NT は、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその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。

UNIX は The Open Group の米国およびその他の国における登録商標です。

VMware、VMware vCenter Server、および VMware vSphere は VMware, Inc. または子会社の米国およびその他の国における登録商標または商標です。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用条件

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、 二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することは できません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示を していただくことを条件に、お客様の企業内に限り、複製、配布、および表示することが できます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、 お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権利

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと 判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。 これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも 含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。 IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。 ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項をご確認ください。

この「ソフトウェア・オファリング」は、Cookie もしくはその他のテクノロジーを使用して個人情報を収集することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie などの各種テクノロジーの使用について詳しくは、「IBM オンラインでのプライバシー・ステートメントのハイライト」(http://www.ibm.com/privacy/jp/ja/)、「IBM オンラインでのプライバシー・ステートメント」(http://www.ibm.com/privacy/details/jp/ja) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』というタイトルのセクション、および「IBM Software Products and Software-as-a-Service Privacy Statement」(http://www.ibm.com/software/info/product-privacy) を参照してください。

用語集

この用語集には、IBM Spectrum Protect 製品ファミリーの用語および定義が記載されています。

IBM Spectrum Protect 用語集 を参照してください。

© Copyright IBM Corp. 2017, 2019

Printed in Japan