

IBM Spectrum Protect Plus
バージョン 10.1.6

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、[541 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 6、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 10.1.6
Installation and User's Guide
Third edition (26th June 2020)

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, 2020.

目次

本書について.....	ix
本書の対象読者.....	ix
資料.....	ix
バージョン 10.1.6 の新機能.....	xi
製品開発への参加.....	xiii
スポンサー・ユーザー・プログラム.....	xiii
ベータ・プログラム.....	xiii
第 1 章製品の概要.....	1
デプロイメント・ストーリーボード.....	1
製品のコンポーネント.....	5
製品ダッシュボード.....	8
アラート.....	9
役割ベースのアクセス制御.....	10
バックアップ・ストレージ・データの複製.....	10
2 次バックアップ・ストレージへのコピー・スナップショット.....	11
IBM Spectrum Protect Plus on IBM Cloud.....	14
IBM Spectrum Protect Plus on AWS.....	15
IBM Spectrum Protect との統合.....	15
Operations Center への IBM Spectrum Protect Plus の追加.....	16
Operations Center の URL の入力.....	18
Operations Center へのアクセス.....	19
第 2 章 IBM Spectrum Protect Plus のインストール.....	21
製品デプロイメントのロードマップ.....	21
システム要件.....	21
コンポーネントの要件.....	21
ハイパーバイザーとクラウド・インスタンスの要件.....	37
ファイル索引付けおよびリストア要件.....	40
ファイル・システムの要件.....	47
Kubernetes Backup Support の要件.....	51
Db2 の要件.....	56
Microsoft Exchange Server の要件.....	62
MongoDB の要件.....	68
Office 365 の要件.....	74
Oracle 要件.....	78
Microsoft SQL Server の要件.....	85
IBM Spectrum Protect Plus インストール・パッケージの入手.....	93
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.....	94
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.....	96
静的 IP アドレスの割り当て.....	98
製品キーのアップロード.....	99
ファイアウォール・ポートの編集.....	99
iSCSI イニシエーター・ユーティリティのインストール.....	101
第 3 章 vSnap サーバーのインストール.....	103
vSnap サーバーのインストール.....	103
物理 vSnap サーバーのインストール.....	103

VMware 環境での仮想 vSnap サーバーのインストール.....	104
Hyper-V 環境での仮想 vSnap サーバーのインストール.....	106
vSnap サーバーのアンインストール.....	107
第 4 章 vSnap サーバーの管理.....	109
vSnap サーバーの登録.....	109
vSnap サーバーの設定の編集.....	110
バックアップ・ストレージ・オプションの構成.....	111
vSnap ストレージ・プールの削除および再作成の方法.....	117
vSnap サーバーの初期化.....	120
簡単な初期化の実行.....	120
高度な初期化の実行.....	120
vSnap ストレージ・プールの拡張.....	121
スループット率の変更.....	122
障害が起きた vSnap サーバーの置き換え.....	122
vSnap サーバー管理の解説.....	123
ユーザー管理.....	124
ストレージ管理.....	125
ネットワーク管理.....	127
カーネル・ヘッダーとカーネル・ツール.....	128
vSnap サーバーのトラブルシューティング.....	129
vSnap パスワードの同期化.....	129
vSnap サーバーがまだオフラインになっているのはなぜですか?.....	129
IBM Spectrum Protect Plus 環境で障害を起こした vSnap サーバーを修復できますか?.....	130
IBM Spectrum Protect Plus 環境で障害を起こした vSnap サーバーを修復するにはどうすれば よいですか?.....	130
IBM Spectrum Protect Plus 環境で障害を起こしたターゲット vSnap を修復するにはどうすれ ばよいですか?.....	134
IBM Spectrum Protect Plus 環境で障害を起こした二重役割の vSnap サーバーを修復するには どうすればよいですか?.....	138
第 5 章 Kubernetes Backup Support のインストール.....	143
前提条件.....	143
Kubernetes でのイメージのインストールとデプロイメント.....	146
Kubernetes Backup Support のアンインストール.....	151
第 6 章 クイック・スタート.....	153
IBM Spectrum Protect Plus の始動.....	155
管理サイト.....	156
バックアップ・ポリシーの作成.....	157
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.....	159
保護するリソースの追加.....	161
ジョブ定義へのリソースの追加.....	163
バックアップ・ジョブの開始.....	164
レポートを実行する.....	165
第 7 章 IBM Spectrum Protect Plus コンポーネントの更新.....	167
更新の管理.....	167
vSnap サーバーの更新.....	170
物理 vSnap サーバー用のオペレーティング・システムの更新.....	171
仮想 vSnap サーバー用のオペレーティング・システムの更新.....	171
vSnap サーバーの更新.....	172
IBM Spectrum Protect Plus 仮想アプライアンスの更新.....	173
Hyper-V Replica 環境で仮想マシンを更新するための追加のステップ.....	174
VADP プロキシの更新.....	175
早期可用性更新の適用.....	176

第 8 章システム環境の構成	177
2 次バックアップ・ストレージの管理	177
クラウド・ストレージの管理	177
リポジトリ・サーバー・ストレージの管理	184
サイトの管理	198
サイトの追加	198
サイトの編集	199
サイトの削除	200
LDAP サーバーと SMTP サーバーの管理	201
LDAP サーバーの追加	201
SMTP サーバーの追加	202
LDAP サーバーまたは SMTP サーバーの設定の編集	203
LDAP サーバーまたは SMTP サーバーの削除	204
管理コンソールへのログイン	204
鍵と証明書の管理	205
アクセス・キーの追加	205
アクセス・キーの削除	205
証明書の追加	206
証明書の削除	206
SSH 鍵の追加	206
SSH 鍵の削除	208
管理コンソールからの SSL 証明書のアップロード	208
タイム・ゾーンの設定	209
仮想アプライアンスへのログイン	210
VMware での仮想アプライアンスへのアクセス	210
Hyper-V での仮想アプライアンスへのアクセス	210
ネットワーク接続のテスト	211
コマンド・ラインからのサービス・ツールの実行	211
リモートでのサービス・ツールの実行	212
仮想ディスクの追加	213
仮想アプライアンスへのディスクの追加	213
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	214
グローバル設定の構成	216
デモ環境の削除	222
 第 9 章バックアップ操作の SLA ポリシーの管理	 225
保護の要約	225
ハイパーバイザー、データベース、およびファイル・システムの SLA ポリシーの作成	228
Amazon EC2 インスタンスの SLA ポリシーの作成	232
Kubernetes クラスター用の SLA ポリシーの作成	234
SLA ポリシーの編集	239
SLA ポリシーの削除	239
 第 10 章仮想化システムの保護	 241
VMware	241
vCenter Server インスタンスの追加	241
VMware データのバックアップ	245
VADP バックアップ・プロキシの管理	251
VMware データのリストア	256
Hyper-V	266
Hyper-V サーバーの追加	266
Hyper-V データのバックアップ	269
Hyper-V データのリストア	273
Amazon EC2	279
AWS IAM ユーザーの作成	280
Amazon EC2 アカウントの追加	281

Amazon EC2 データのバックアップ.....	282
Amazon EC2 データのリストア.....	284
ファイルのリストア.....	287
第 11 章ファイル・システムの保護.....	291
Windows ファイル・システム.....	291
ファイル・システム の前提条件.....	291
ファイル・システムの追加.....	292
ファイル・システム・データのバックアップ.....	296
ファイル・システム データのリストア.....	302
第 12 章コンテナの保護.....	309
概説.....	309
バックアップおよびリストアのタイプ.....	310
SLA ポリシー.....	311
ユーザー役割.....	312
セキュリティ機能.....	313
ユーザー・インターフェースを使用した Kubernetes クラスターの保護.....	314
Kubernetes クラスターの登録.....	314
SLA バックアップ・ジョブの定義.....	317
コンテナ・データのリストア.....	320
Kubernetes ジョブ・セッションの有効期限切れ.....	323
ジョブの表示およびレポートの実行.....	324
コマンドを使用したコンテナの保護.....	327
Kubernetes Backup Support 要求.....	327
コマンド・ラインを使用したコンテナのバックアップ.....	329
コマンド・ラインを使用したコンテナ・データのリストア.....	339
コンテナのバックアップ・ジョブとリストア・ジョブの管理.....	342
第 13 章クラウド管理システムの保護.....	347
Microsoft Office 365.....	347
Azure Active Directory への登録.....	347
IBM Spectrum Protect Plus への Office 365 テナントの登録.....	348
詳細なプロセス・ログ.....	349
Office 365 データのバックアップ.....	350
Office 365 データのリストア.....	351
第 14 章データベースの保護.....	353
Db2.....	353
Db2 の前提条件.....	353
Db2 アプリケーション・サーバーの追加.....	356
Db2 データのバックアップ.....	360
Db2 データのリストア.....	367
Exchange Server.....	379
前提条件.....	379
特権.....	380
Exchange アプリケーション・サーバーの追加.....	381
Exchange データベースのバックアップ.....	383
永久差分バックアップ戦略.....	386
Exchange データベースのリストア.....	387
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..	417
MongoDB.....	420
MongoDB の前提条件.....	420
MongoDB アプリケーション・サーバーの追加.....	423
MongoDB データのバックアップ.....	427
MongoDB データのリストア.....	432
Oracle.....	448

Oracle アプリケーション・サーバーの追加.....	448
Oracle データのバックアップ.....	450
Oracle データのリストア.....	453
SQL Server.....	460
SQL Server アプリケーション・サーバーの追加.....	461
SQL Server データのバックアップ.....	463
SQL Server データのリストア.....	467
第 15 章 IBM Spectrum Protect Plus の保護.....	475
アプリケーションのバックアップ.....	475
アプリケーションのリストア.....	475
リストア・ポイントの管理.....	476
ジョブ・セッションを期限切れに設定.....	476
カタログからのリソース・メタデータの削除.....	477
第 16 章ジョブと操作の管理.....	479
ジョブ・タイプ.....	479
ジョブおよびジョブ・スケジュールの作成.....	480
オンデマンドでのジョブの開始.....	481
ジョブの表示.....	482
リソース・レベルでのバックアップ・ジョブ進行状況の表示.....	483
ジョブ・ログの表示.....	484
同時ジョブの表示.....	484
ジョブの一時停止と再開.....	484
ジョブとジョブ・スケジュールの編集.....	485
ジョブのキャンセル.....	485
ジョブの削除.....	486
部分的に完了したバックアップ・ジョブの再実行.....	486
アドホック・バックアップ・ジョブの実行.....	487
バックアップ操作とリストア操作のスクリプトの構成.....	487
スクリプトのアップロード.....	488
サーバーへのスクリプトの追加.....	488
第 17 章レポートおよびログの管理.....	491
レポートのタイプ.....	491
バックアップ・ストレージの使用状況レポート.....	491
保護レポート.....	492
システム・レポート.....	495
VM 環境レポートの実行.....	496
レポートのアクション.....	498
レポートの実行.....	498
カスタム・レポートの作成.....	499
レポートのスケジューリング.....	500
アクションのための監査ログの収集および確認.....	500
第 18 章ユーザー・アクセスの管理.....	503
ユーザー・リソース・グループの管理.....	504
リソース・グループの作成.....	504
リソース・グループの編集.....	507
リソース・グループの削除.....	507
役割の管理.....	507
役割の作成.....	509
役割の編集.....	511
役割の削除.....	511
ユーザー・アカウントの管理.....	512
個別のユーザーのユーザー・アカウントの作成.....	512
LDAP グループのユーザー・アカウントの作成.....	512

ユーザー・アカウント資格情報の編集.....	513
ユーザー・アカウントの削除.....	514
ID の管理.....	514
ID の追加.....	514
ID の編集.....	514
ID の削除.....	515
第 19 章ライセンス交付の概要.....	517
ソフトウェア・ライセンス・メトリック (SLM) タグ.....	517
IBM License Metric Tool (ILMT) の組み込み.....	518
第 20 章トラブルシューティング.....	519
トラブルシューティング用のログ・ファイルの収集.....	519
テープまたはクラウド・ストレージにデータを階層化するにはどうすればよいですか?.....	519
Kubernetes Backup Support のトラブルシューティング.....	520
Kubernetes Backup Support ログ・ファイルの収集.....	520
ログ・ファイルのトレース・レベルの設定.....	521
Kubernetes Backup Support のトレース・ログの表示.....	522
クイック・リファレンス.....	523
バックアップとリストアのトラブルシューティング.....	527
第 21 章製品メッセージ.....	535
メッセージ接頭語.....	535
付録 A 検索ガイドライン.....	537
付録 B アクセシビリティー.....	539
特記事項.....	541
用語集.....	545
索引.....	547

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 (21 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。

バージョン 10.1.6 の新機能

IBM Spectrum Protect Plus バージョン 10.1.6 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。

資料に変更が加えられた場合、余白に垂直バー (|) を付けて表示しています。

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。

連絡先と情報の登録

[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、長期データ・ストレージのためにクラウド・ストレージまたはリポジトリ・サーバー (IBM Spectrum Protect サーバーなど) と統合することができます。

IBM Spectrum Protect Plus のデプロイメント・ストーリーボード

このストーリーボードは、製品をデプロイするのに必要なタスクを順に進める上で役立ちます。デプロイメント・ストーリーボードは、IBM Spectrum Protect Plus を実稼働環境に正常にデプロイする上で助けとなるように設計されています。このストーリーボードには、各タスクが必要な順序でリストされていて、IBM Spectrum Protect Plus Blueprints のタスクの説明、ビデオ、およびガイドラインへのリンクが掲載されています。ストーリーボードでは、製品をデプロイする際に進行状況を確認できるように、タスクの期待される成果を説明しています。

開始する前に、環境のシステム要件を確認してください。詳しくは、[21 ページの『システム要件』](#)を参照してください。

表 1 の各ステップでは、Blueprints の情報と Sizer ツールの機能を利用します。これらのタスクを実行する上で役立つビデオのリンクが表 2 に示されています。

表 1. デプロイメント・ストーリーボード		
ストーリー	手順	期待される成果
Blueprints と Sizer ツールのスプレッドシートをダウンロードして、容量要件のサイジングを準備します。	サイジングのガイドラインについては、IBM Spectrum Protect Plus Blueprints の第 1 章から第 3 章を参照してください。 サイジング・スプレッドシートについてのヘルプは、 表 2 のビデオへのリンクを参照してください。 サイジング・スプレッドシートの Sizer ツール を次のページからダウンロードして、下記のステップを実行します。 Blueprints	IBM Spectrum Protect Plus の容量要件のサイジングに必要な Sizer ツールのスプレッドシートと情報を入手しました。

表 1. デプロイメント・ストーリーボード (続き)

ストーリー	手順	期待される成果
ご使用の環境の 1 次ストレージに必要な容量をサイジングします。	<p>Sizer を使用して、1 次ストレージをサイジングします。</p> <ol style="list-style-type: none"> 1. ダウンロードした Sizer ツールのスプレッドシートを開き、マクロを有効にします。スプレッドシートのコピーを 1 次ストレージ用にローカル・ドライブに保存します。 2. 「ここから開始 (Start Here)」シートで 1 次ストレージのグローバル・オプションの選択内容を指定します。 3. 「VMware」タブを開き、日次変更率と年間増加率など、vCenter の容量に関するデータを入力します。 4. 「HyperV」タブを開き、HyperV の容量に関するデータを入力します。 5. 使用する予定のアプリケーションごとに、アプリケーションのタブを開き、容量のニーズに関するデータを入力します。 6. すべてのデータを入力したら、「サイジングの結果 (Sizing Results)」タブをクリックして、計算結果を確認します。 7. 推奨される vSnap サーバーのサイズを設定します。 vSnap ストレージ・プールのサイズの値を自動的に指定するには、「自動 (Automatic)」をクリックします。 8. 必要な vSnap サーバーの予約のパーセンテージを入力します。この予約は、使用、リストア操作、再利用のために予約される vSnap サーバー・ストレージのパーセンテージです。 9. IBM Spectrum Protect Plus を開き、「システム構成」 > 「グローバル設定」にナビゲートします。Sizer ツールで示されているように、グローバル設定のパーセンテージを入力します。これらのパーセンテージを使用して、以下のオプションを設定します。 <ul style="list-style-type: none"> ・ターゲットのフリー・スペース・エラー (パーセンテージ) ・ターゲットのフリー・スペース警告 (パーセンテージ) 10. 1 次ストレージに関する Sizer の結果を確認します。Sizer を保存します。ただし、2 次ストレージに必要な設定を入力するために開いたままにしておいてください。 	<p>Sizer ツールのスプレッドシートは、1 次ストレージのサイジング情報を計算するのに役立ちます。</p> <p>Sizer のサイジング・スプレッドシートのコピーを保存しました。容量要件が変化した場合は、このスプレッドシートを適宜に更新できます。</p> <p>また、vSnap サーバーの必要な数とサイズのほか、オプションで必要な VMware vStorage API for Data Protection プロキシの数に関する詳細も得られました。</p> <p>スプレッドシートへの入力内容に基づいて、8 年間の増加に関する詳細な見通しを得られました。使用率に基づいて指定のしきい値に達したときに vSnap から警告とエラーをトリガーするためのグローバル設定を設定しました。</p>

表 1. デプロイメント・ストーリーボード (続き)		
ストーリー	手順	期待される成果
ご使用の環境の 2 次ストレージに必要な容量をサイジングします。	<p>Sizer を使用して、次のステップを実行し、2 次ストレージをサイジングします。Blueprints の第 5 章を参照してください。</p> <ol style="list-style-type: none"> Blueprints ページからサイジング・スプレッドシートをダウンロードして、マクロを有効にします。Sizer シートのコピーを 2 次ストレージ用にローカル・ドライブに保存します。 値が入力されている場合は、「クリックしてリセット (Click to reset)」をクリックして Sizer ツールのスプレッドシートをリセットします。 「ここから開始 (Start Here)」シートで 2 次ストレージのグローバル・オプションの選択内容を指定します。 先ほど保存した 1 次ストレージ用の Sizer ツールのスプレッドシートの「結果 (Results)」タブに移動します。「複製のワークロード (Replication workload)」テーブルにリストされている結果をコピーして、2 次ストレージ用の Sizer ツールのスプレッドシートの「ここから開始 (Start Here)」タブの「オプションの複製の入力ワークロード (Optional Replication Input Workload)」テーブルに値を入力します。 アプリケーション・データを保護する予定の場合は、アプリケーションのタブに入力します。例えば、オブジェクト・ストレージへのデータのコピーや複製ポリシーに関するオプションを指定できます。 2 次ストレージに関するサイジングの結果を確認します。両方の Sizer ツールのスプレッドシートを保存して閉じます。 	<p>IBM Spectrum Protect Plus 環境の 2 次ストレージの容量のサイジングを得られました。</p> <p>ご使用の環境の 2 次ストレージに関する Sizer のコピーを保存しました。何らかの変更がある場合は、Sizer を変更して、必要な変更を行うことができます。</p> <p>また、毎年 vSnap サーバーの数量、VADP プロキシの数量、および各 vSnap サーバーのサイズに関する詳細も得られました。</p> <p>Sizer への入力内容に基づいて、8 年間の増加に関する詳細な見通しを得られました。使用率に達したときに vSnap から警告とエラーをトリガーするためのグローバル設定を設定しました。</p>
必要なバージョンの ISO イメージを使用して、IBM Spectrum Protect Plus のインストールまたはアップグレードを行います。システム環境を更新する場合、新規カーネルがインストールされ、再始動が必要になります。	<p>IBM Spectrum Protect Plus をインストールして、94 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』または 96 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』の説明に従います。</p>	<p>IBM Spectrum Protect Plus がインストールされました。</p>
必要なバージョンの ISO イメージを使用して、vSnap サーバーのインストールまたはアップグレードを行います。データ重複排除を使用する場合は、vSnap サーバーの再始動には最大 15 分かかります。	<p>vSnap サーバーをインストールして、103 ページの『物理 vSnap サーバーのインストール』の説明に従います。仮想 vSnap サーバーをインストールする場合は、106 ページの『Hyper-V 環境での仮想 vSnap サーバーのインストール』の説明に従います。</p>	<p>vSnap サーバーがインストールされます。vSnap サーバーがインストールされたことを確認するには、<code>vsnap show</code> コマンドを実行します。</p>

表 1. デプロイメント・ストーリーボード (続き)		
ストーリー	手順	期待される成果
Blueprints とサイジング・ツールを使用したサイジングから得られた容量を指定して vSnap サーバーをビルドします。	<ol style="list-style-type: none"> 1. ボリュームを作成して、vSnap 装置をマップします。 2. ボリュームを VM クラスターにマップします。 3. Blueprints で、Blueprints で仮想または物理の vSnap サーバーをセットアップするためのステップを参照してください。 	vSnap サーバーがビルドされます。
ログ・スペースを追加します。	<p>vSnap サーバー・ストレージ・キャッシュ、クラウド・キャッシュ、およびログ・ファイルを保管するための 3 つの区画を使用して、Linux® Multiple Device ドライバーを作成します。クラウド・キャッシュについては、容量はデフォルトで 128 GB に設定されています。クラウドにデータをコピーする予定の場合は、この容量を増やす必要があります。クラウド・ストレージへの物理 vSnap サーバーのコピー・データについては、必要な容量を指定して /opt/vsnap-data ファイル・システムを作成する必要があります。</p> <p>このステップについて詳しくは、Blueprints の <i>Configuring a physical vSnap server using storage software provided RAID</i> および <i>Chapter 7 Configuring Cloud Object Storage</i> を参照してください。</p>	仮想または物理の vSnap サーバーのログ・スペースをセットアップしました。
vSnap サーバーを登録します。	vSnap サーバーを登録します。詳細情報とステップについては、 109 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 vSnap サーバーの登録』 を参照してください。	vSnap サーバーが登録され、IBM Spectrum Protect Plus に追加されます。
vSnap サーバーを初期化します。	IBM Spectrum Protect Plus のインストールまたはアップグレードを行い、vSnap サーバーを追加した後、vSnap サーバーを初期化する必要があります。詳細情報とステップについては、 120 ページの『簡単な初期化の実行』 を参照してください。	選択内容に応じて、vSnap サーバーは、暗号化を有効にして初期化されるか、暗号化を有効にせずに初期化されます。
vSnap サーバーを構成します。	複製パートナーの追加など、vSnap サーバー・ストレージのオプションを構成するには、 111 ページの『バックアップ・ストレージ・オプションの構成』 を参照してください。	データ複製機能を構成した場合は、複製パートナーがセットアップされています。
(オプション) vSnap サーバーを VADP プロキシとして構成します。	vSnap サーバーとの間のデータの移動を最適化するために VADP プロキシを使用する場合は、vSnap サーバーを VADP プロキシとして登録する必要があります。詳しい手順については、 254 ページの『vSnap サーバーでの VADP プロキシの登録』 を参照してください。	vSnap サーバーが VADP プロキシとして構成されます。
vCenter の作成やハイパーバイザーの登録など、VMware 環境のセットアップを行います。	VMware データを保護するには、最初に vCenter Server をセットアップする必要があります。手順については、 241 ページの『VMware データのバックアップとリストア』 を参照してください。必要な vCenter Server の特権が有効になっていることを確認してください。必要な特権について詳しくは、 242 ページの『仮想マシンの特権』 を参照してください。	vCenter が必要な権限でセットアップされるため、VMware データの保護を開始できます。
ユーザーを追加します。	IBM Spectrum Protect Plus を使用する必要があるユーザーを追加します。詳しくは、ページで「ユーザーの追加」フォームを使用した 512 ページの『個別のユーザーのユーザー・アカウントの作成』 を参照してください。	ユーザーが追加され、IBM Spectrum Protect Plus を操作するための権限が付与されます。

表 1. デプロイメント・ストーリーボード (続き)		
ストーリー	手順	期待される成果
SLA ポリシーを作成します。	IBM Spectrum Protect Plus ワークロード用の SLA ポリシーをセットアップします。SLA ポリシーについて詳しくは、 225 ページの『第 9 章 バックアップ操作の SLA ポリシーの管理』 を参照してください。	IBM Spectrum Protect Plus ワークロード用の SLA ポリシーがセットアップされ、バックアップ・ジョブを実行する準備ができました。
グローバル設定を更新します。	管理者は、重複排除や暗号化など、すべての操作のグローバル設定を編集できます。グローバル設定について詳しくは、 216 ページの『グローバル設定の構成』 を参照してください。	グローバル設定は、設定される場合、IBM Spectrum Protect Plus 環境全体に適用されます。

リソースとビデオ・ライブラリー

ご使用の IBM Spectrum Protect Plus 環境のサイジングには Blueprints を使用する必要があります。次の表にリストされているビデオは、このプロセスに役立ちます。

表 2. Blueprints とサイジング	
タスクまたはトピック	ビデオのリンク
Sizer ツールの概要	IBM Spectrum Protect Plus Sizer and Blueprints: 1. Sizer introduction - Demo
Sizer ワークシートの概要	IBM Spectrum Protect Plus Sizer & Blueprints: 2. Sizer Worksheet Overview – Demo
Sizer のグローバル値	IBM Spectrum Protect Plus Sizer & Blueprints: 3. Sizer Global Values – Demo
ハイパーバイザーの追加	IBM Spectrum Protect Plus Sizer & Blueprints: 4. Adding a Hypervisor workload to the sizer – Demo
アプリケーションの追加	IBM Spectrum Protect Plus Sizer & Blueprints: 5. Adding Application workload to the sizer– Demo
結果の評価	IBM Spectrum Protect Plus Sizer & Blueprints: 6. Evaluating the sizer’s results – Demo
2 次ストレージの追加	IBM Spectrum Protect Plus Sizer & Blueprints: 7. Adding a secondary site to sizer – Demo
What if シナリオ	IBM Spectrum Protect Plus Sizer & Blueprints: 8. What if sizing scenarios – Demo
Blueprints の新機能	IBM Spectrum Protect Plus Sizer & Blueprints: 9. What’s new in 10.1.5 sizer – Presentation
デプロイメントでの Sizer の結果の使用	IBM Spectrum Protect Plus Sizer & Blueprint: 10. Tying the blueprints, sizer and install together - Demo

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 サービスがあります。

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・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。

VADP プロキシ (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、[8 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。

項目	説明
IBM Spectrum Protect アイコン 	このアイコンをクリックすると、拡張データ保護を提供するために IBM Spectrum Protect Operations Center が開きます。このアイコンがアクティブになるのは、「 グローバル設定 」ページで「 IBM Spectrum Protect Operations Center URL 」設定フィールドに URL が入力されている場合のみです。この設定については、 216 ページの『グローバル設定の構成』 を参照してください。
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、 9 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。

制約事項： IBM Spectrum Protect Plus 製品は、メニューの ICU 照合ソートに従わないため、メニューはコード・ポイントの順序で表示されます。例えば、一部の言語では、コード・ポイントとは異なる順序で文字がソートされます。そのため、そのような言語の使用時に文字および単語がメニューに表示されるソート順は、予期しない順序になります。

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、セキュリティ証明書管理、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 Server 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。

$$100 \times \text{成功したジョブ数} / \text{ジョブの総数} = \text{成功率}$$

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、圧縮の比率に加えて達成された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。

ジョブが部分的に成功

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。

コピー・ストレージ・スナップショットのロック状態例外

最新のコピー・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。コピーの保存設定を増やすか、ポリシーのコピー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。

ストレージで重複排除が無効に設定された

重複排除が無効になった場合に表示され、ストレージ・サーバーの IP が表示されます。この状況は、vSnap の重複排除自動無効化テーブル (DDT) オプションが有効になっていて、定義済みのサイズまたはパーセンテージのしきい値を超過した場合に起こります。

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、503 ページの『[第 18 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、[225 ページの『第 9 章 バックアップ操作の 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。

- 複数の vSnap サーバーがある環境では、すべての vSnap サーバーでパートナーシップが確立されている必要があります。
- 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・ストレージへのコピー・スナップショット

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・ストレージにコピーできます。

用語の変更: 以前のリリースでは、IBM Spectrum Protect Plus から 2 次バックアップ・ストレージにデータをコピーするプロセスは、データのオフロードと呼ばれていました。IBM Spectrum Protect Plus バージョン 10.1.5 以降では、このプロセスは、データのコピーと呼ばれます。

以下の 2 次バックアップ・ストレージ・ターゲットが、コピー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・サーバー (現行リリースの IBM Spectrum Protect Plus の場合、リポジトリ・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目標などの要因によって異なります。

標準オブジェクト・ストレージ

標準オブジェクト・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。

標準オブジェクト・ストレージは、スナップショット・データを IBM Spectrum Protect サーバーまたはクラウド・ストレージ・システムにコピーする場合のオプションです。標準オブジェクト・ストレージにスナップショット・データがコピーされると、最初のコピー操作中にフルコピーが作成されます。後続のコピーは差分コピーで、前回のコピー操作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上のメリットは必要でない場合は、スナップショットを標準オブジェクト・ストレージにコピーすると便利です。

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 (VTL) 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、スナップショット・データを IBM Spectrum Protect サーバー にコピーするときのオプションです。

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。

スナップショット・データを磁気テープまたはクラウド・ストレージ・システムにコピーすると、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・オブジェクト・アーカイブ・ストレージにコピーすると、追加のコストとセキュリティ上のメリットが得られます。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。ただし、これらのストレージ・タイプへのコピーには完全なデータ・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。

IBM Spectrum Protect Plus から IBM Spectrum Protect サーバーにデータをテープにコピーする場合、IBM Spectrum Protect の階層化機能を使用することはお勧めしません。テープにデータをアーカイブする場合は、コールド・キャッシュ・ストレージ・プールを使用する必要があります。階層化については、[519 ページの『テープまたはクラウド・ストレージにデータを階層化するにはどうすればよいですか?』](#)を参照してください。ストレージのセットアップのさまざまなシナリオおよび詳細については、[184 ページの『IBM Spectrum Protect にデータをコピーまたはアーカイブするための構成』](#)を参照してください。

各クラウド・ストレージ・システムの標準オブジェクト・ストレージおよびアーカイブ・オブジェクト・ストレージにスナップショット・データがコピーされる方法については、[34 ページの『クラウド・ストレージ要件』](#)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

スナップショットを 2 次ストレージにコピーするには、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・サーバーにスナップショットをコピーします <ul style="list-style-type: none">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。	184 ページの『IBM Spectrum Protect にデータをコピーまたはアーカイブするための構成』 および 196 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・サーバーの登録』 を参照してください。
クラウド・ストレージにスナップショットをコピーするために、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。 <ul style="list-style-type: none">178 ページの『Amazon S3 オブジェクト・ストレージの追加』179 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』181 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』196 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・サーバーの登録』

アクション	方法
ストレージを含むバックアップ・ポリシーを作成します。	157 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 Server 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・ストレージにコピーされます。

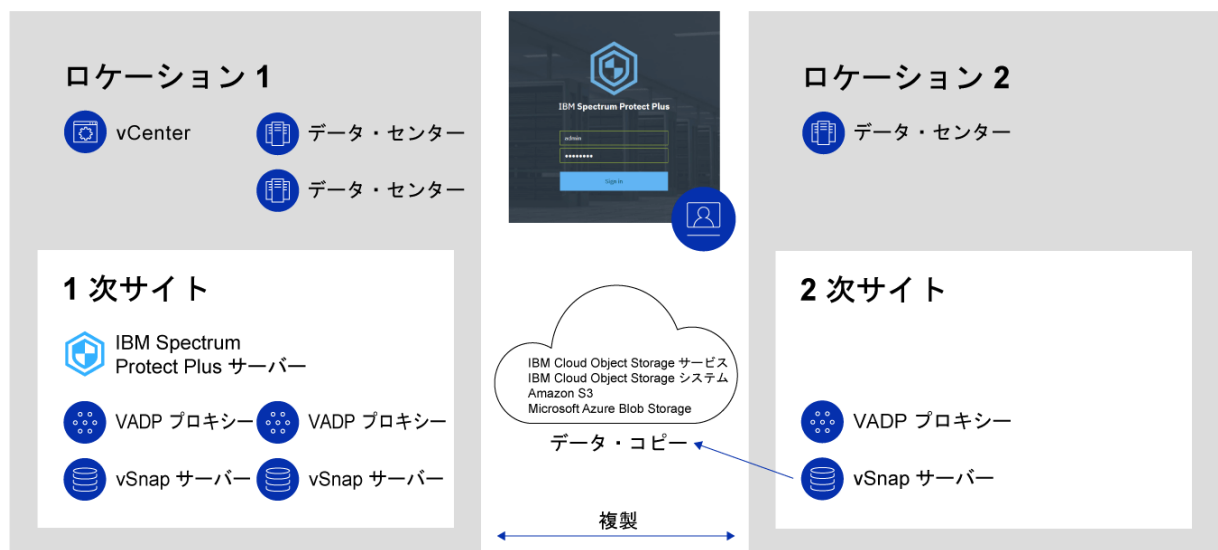


図 2. クラウド・ストレージにコピーする、2つの地理的ロケーションにおける IBM Spectrum Protect Plus デプロイメント

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 にコピーされます。



図 3. IBM Spectrum Protect にコピーする、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、AWS で実行中のデータベースを保護するユーザー向けのデータ保護ソリューションです。さらに、ユーザーは、IBM Spectrum Protect Plus サーバーを VMC にインストールして、vSnap サーバーを AWS Virtual Private Cloud (VPC) にインストールしながら、VMware Cloud (VMC) on AWS によって管理されている仮想マシンを保護することができます。

IBM Spectrum Protect Plus on AWS を以下のいずれかの構成でデプロイすることができます。VMC on AWS に対するサポートは、ハイブリッド環境でのみ利用できます。VMC on AWS に対するサポートについて詳しくは、[IBM Spectrum Protect Plus for VMware Cloud on AWS](#) を参照してください。

オールクラウド環境

この構成では、IBM Spectrum Protect Plus サーバーと vSnap サーバーの両方が既存または新規の VPC 上の AWS にデプロイされます。オンプレミスの IBM Spectrum Protect Plus サーバーおよび VMware または Microsoft Hyper-V インフラストラクチャーは不要です。

このオプションは、AWS 上のデータベースを保護したいものの、IBM Spectrum Protect Plus をオンプレミス環境で稼働したくない新規の IBM Spectrum Protect Plus ユーザーのメリットとなる場合があります。

ハイブリッド環境

この構成では、vSnap サーバーのみが既存または新規の VPC 上の AWS にデプロイされます。IBM Spectrum Protect Plus サーバーは、オンプレミスまたは別のロケーションでインストールされ、保守されます。このオプションは、オンプレミスとクラウド環境で実行されているワークロードを引き続き保護したい既存の IBM Spectrum Protect Plus ユーザーのメリットとなる場合があります。

バックアップ操作とリカバリー操作のほか、ハイブリッド環境を使用して、オンプレミスのロケーションと AWS の間でデータを複製して再利用し、データ保護を強化することもできます。例えば、DevOps、品質保証、テスト、災害復旧の目的で、オンプレミスのサイトで保護されているデータを AWS で使用することができます。

AWS への IBM Spectrum Protect Plus のデプロイ

AWS Marketplace の [IBM Spectrum Protect Plus ページ](#) は、IBM Spectrum Protect Plus サーバーと 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、使用方法、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 との統合

IBM Spectrum Protect Plus 環境を IBM Spectrum Protect Operations Center からモニターすることができます。利便性のために、Operations Center に IBM Spectrum Protect Plus から直接アクセスすることもできます。

Operations Center からの IBM Spectrum Protect Plus のモニター


Operations Center には、以下の情報を提供する IBM Spectrum Protect Plus 用のダッシュボードが組み込まれています。

- 選択した期間のジョブ・アクティビティの要約。バックアップ・ジョブ、リストア・ジョブ、およびその他のジョブの成功と失敗のパーセンテージを表示できます。この要約情報から、各ジョブ・タイプの詳細な情報に移動できます。
- vSnap サーバーの容量と可用性の要約。すべての vSnap サーバーを介して IBM Spectrum Protect Plus サーバーで利用できる合計ディスク容量を表示できます。各 vSnap サーバーの使用可能容量も表示できます。
- IBM Spectrum Protect Plus サーバーで定義されている SLA ポリシーの要約。バックアップ・ジョブが関連付けられているポリシーの数を表示できます。バックアップ・ジョブによって保護されているリソースのパーセンテージと、保護されていないリソースの数も表示できます。この要約情報から、詳細なポリシー情報に移動できます。

この機能を有効にするには、システム管理者が IBM Spectrum Protect Plus サーバーを Operations Center に追加する必要があります。

IBM Spectrum Protect Plus GUI からの Operations Center へのアクセス

IBM Spectrum Protect Plus から Operations Center にアクセスするには、システム管理者は、IBM Spectrum Protect Plus GUI の「グローバル設定」ページで Operations Center の URL を追加する必要があります。

その後、メニュー・バーの IBM Spectrum Protect アイコン  から Operations Center にアクセスできます。

Operations Center への IBM Spectrum Protect Plus の追加

IBM Spectrum Protect Plus サーバーを Operations Center に追加する場合、サーバーと Operations Center 間に接続を確立します。この接続が確立されると、Operations Center を使用して IBM Spectrum Protect Plus 環境をモニターできます。

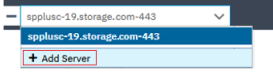
始める前に

Operations Center の URL と、ログオンするためのユーザー資格情報があることを確認してください。

手順

IBM Spectrum Protect Plus サーバーを Operations Center に追加するには、以下のステップを実行します。

1. Operations Center メニュー・バーで、「概要」 > 「**Protect Plus**」をクリックして、以下のアクションのいずれかを実行して「サーバーの追加」ウィザードを開きます。

現在の構成	アクション
Operations Center に接続されている IBM Spectrum Protect Plus サーバーがない。	構成されている IBM Spectrum Protect Plus サーバーがないことを示すメッセージが表示されます。「+サーバーの追加」をクリックします。
1 つ以上の IBM Spectrum Protect Plus サーバーが Operations Center に接続されている。	IBM Spectrum Protect Plus ダッシュボードが表示されます。モニター・ダッシュボードのサーバー・リストから、「+サーバーの追加」  を選択します。

2. IBM Spectrum Protect Plus サーバーを追加するには、ウィザードの指示に従います。

ウィザードの「許可」ページでは、IBM Spectrum Protect Plus サーバーにアクセスしてモニターするためのユーザー資格情報を指定するように求めるプロンプトが表示されます。お持ちの IBM Spectrum Protect Plus アカountの資格情報が、Operations Center 資格情報と一致する場合、そのアカウントを使用できます。一致している資格情報がない場合は、アカウントを作成する必要があります。

Operations Center 資格情報を使用する

Operations Center へのログオンに使用した管理者アカウントのユーザー名とパスワードに一致する、既存の IBM Spectrum Protect Plus ユーザー・アカウントを使用する場合は、このオプションを選択します。

モニター・ユーザー・アカウントの作成

ウィザードで IBM Spectrum Protect Plus ユーザー・アカウントを作成する場合、このオプションを選択します。

Operations Center の IBM Spectrum Protect Plus へのアクセスを有効にし、アカウントを作成するには、SYSADMIN 役割に割り当てられている IBM Spectrum Protect Plus ユーザー・アカウントの資格情報を指定します。次の図に示すように、「ユーザー名」と「パスワード」の各フィールドに資格情報を入力します。

Add Server

Authorization

Identify or create a user account on the IBM Spectrum Protect Plus server for monitoring. [Learn more](#)

☐ Use Operations Center credentials (User account with the same credentials must already be defined on server)

☒ Create a monitoring administrator

Specify IBM Spectrum Protect Plus login credentials for a user account that can create custom user roles and user accounts. This user account is used only during configuration. During configuration, a new user role and account for monitoring are created.

User name

Password

Back Add Server Cancel

図 4. IBM Spectrum Protect Plus 資格情報の入力

ここに入力した資格情報は保存されません。Operations Center は、これらのアカウント資格情報を使用して IBM Spectrum Protect Plus サーバーにログオンし、ユーザー・アカウント OC_MONITOR_ *number* を作成します。ここで *number* は、乱数の ID です。Operations Center は新規アカウントを使用して IBM Spectrum Protect Plus 環境に接続します。

3. 「サーバーの追加」をクリックします。

操作が正常に実行されると、以下の図に示すような結果が表示されます。

Add Server

✓ Succeeded

10:19 PM Adding IBM Spectrum Protect Plus server...
Connecting to the IBM Spectrum Protect Plus server.
Creating monitor role.
Creating monitor user.
Saving server.
Establishing session.

✓
✓
✓
✓
✓

Close


図 5. IBM Spectrum Protect Plus が正常に追加

Operations Center の URL の入力

Operations Center に IBM Spectrum Protect Plus からアクセスするには、IBM Spectrum Protect Plus グローバル設定から Operations Center の URL を入力します。

このタスクについて

グローバル設定を構成するには、IBM Spectrum Protect Plus 管理者資格情報が必要です。

この設定に入力すると、IBM Spectrum Protect アイコン  が IBM Spectrum Protect Plus メニュー・バーでアクティブになります。

手順

Operations Center URL を入力するには、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」 > 「グローバル設定」をクリックします。
2. 「**IBM Spectrum Protect Operations Center URL**」フィールドで Operations Center の URL を入力します。

Global Preferences

Register system preferences for your IBM Spectrum Protect Plus environment.

Integration with other storage products

IBM Spectrum Protect Operations Center



<https://tapsrv09.storage.tucson.il>



URL

図 6. Operations Center の URL の入力

3. IBM Spectrum Protect Plus メニュー・バー上の IBM Spectrum Protect アイコンをアクティブにするには、IBM Spectrum Protect Plus をログオフしてから再度ログオンします。

Operations Center へのアクセス

IBM Spectrum Protect Plus 環境をモニターするために Operations Center を開始します。


始める前に

以下のタスクが完了していることを確認します。

- 16 ページの『Operations Center への IBM Spectrum Protect Plus の追加』
- 18 ページの『Operations Center の URL の入力』

手順

Operations Center にアクセスして IBM Spectrum Protect Plus 環境をモニターするには、以下のステップを実行します。

1. IBM Spectrum Protect Plus メニュー・バーで、IBM Spectrum Protect アイコン  をクリックします。
2. Operations Center にログオンします。
3. Operations Center メニュー・バーで、「概要」 > 「Protect Plus」をクリックします。

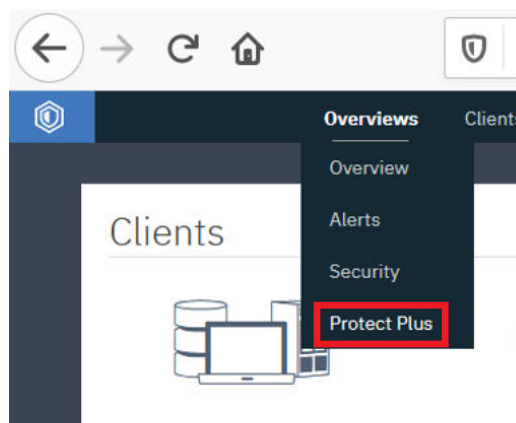


図 7. Operations Center での IBM Spectrum Protect Plus の選択

4. 以下の図のように IBM Spectrum Protect Plus モニター・ダッシュボードで IBM Spectrum Protect Plus 環境の状況を確認します。

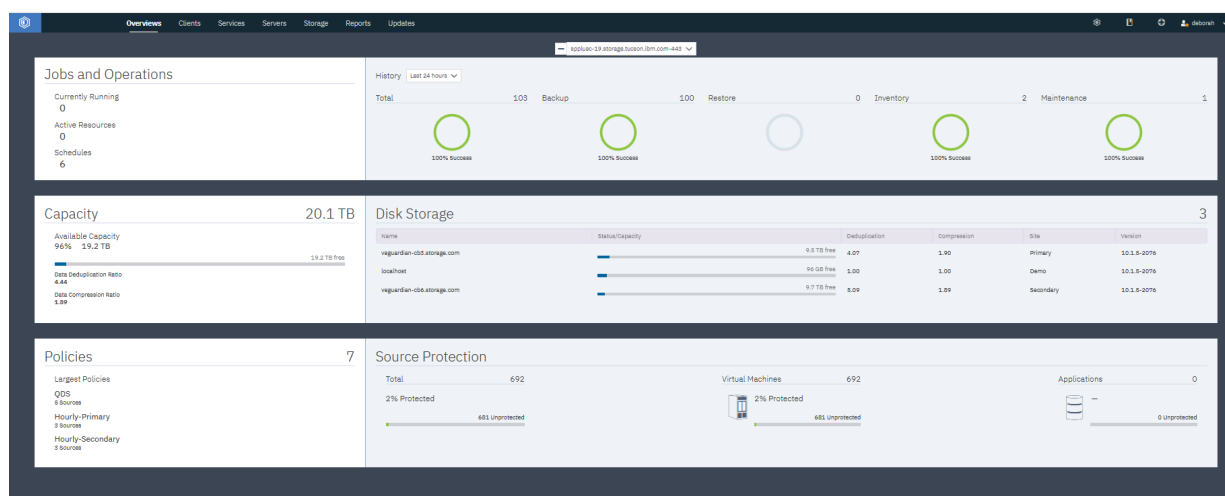


図 8. IBM Spectrum Protect Plus ダッシュボードの表示

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。	21 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。	21 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。	103 ページの『第 3 章 vSnap サーバーのインストール』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 VMware vStorage API for Data Protection (VADP) プロキシが必要な場合は、それらのプロキシを作成し、構成します。	251 ページの『VADP バックアップ・プロキシの管理』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。	153 ページの『第 6 章 クイック・スタート』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 304861](#) 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 304861](#) 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・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・ベンダーによって異なります。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、ベンダーと同じレベルの製品またはバージョンをサポートします。

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、以下のいずれかの要件が満たされていることを確認してください。

- 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) (IBM Spectrum Protect Plus V10.1.2 以降)
- vSphere 7.0 (すべての更新およびパッチ・レベルを含む) (IBM Spectrum Protect Plus V10.1.6 以降)
- Microsoft® Hyper-V 2016
- Microsoft Hyper-V 2019 (IBM Spectrum Protect Plus V10.1.3 以降)

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・サーバー
- 48 GB のメモリー
- 仮想マシン (VM) 用の 548 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atalog作成、インベントリー操作、バックアップ・ジョブ、またはファイル・リストア・ジョブでエラーが発生す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および検証が行われています。

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

画面解像度が 1024 x 768 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・ウィンドウを有効にしてください。

仮想アプライアンス・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。

表 3. ターゲットが IBM Spectrum Protect Plus 仮想アプライアンスである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
22	伝送制御プロトコル (TCP)	vSnap サーバー (vSnap server)	IBM Spectrum Protect Plus 仮想アプライアンス	<p>SSH プロトコルを使用した IBM Spectrum Protect Plus 仮想アプライアンスでのトラブルシューティングとメンテナンスのタスクのためのアクセスを提供します。</p> <p>SSH プロトコルを使用した IBM Spectrum Protect Plus 仮想アプライアンスへの vSnap データ複製にも使用されます。</p>
443	TCP	IBM Spectrum Protect Plus ユーザー・インターフェース	IBM Spectrum Protect Plus 仮想アプライアンス	<p>HTTPS を使用する Web アクセスを提供します。このポートは、SSL プロトコルを使用するクライアント接続のメインエントリー・ポイントです。このポートは、Representational State Transfer アプリケーション・プログラミング・インターフェース (REST API) 照会のみ使用されます。</p>
5671	TCP および Advanced Message Queuing Protocol (AMQP)	VMware vStorage API for Data Protection プロキシ (VADP プロキシ) ホスト	IBM Spectrum Protect Plus 仮想アプライアンス	<p>VADP プロキシおよび VMware ジョブ管理ワーカーによって作成および使用されるメッセージの管理に使用されます。このポートは、RabbitMQ メッセージ・フレームワークであり、ジョブ・ログ管理も容易にします。</p>

表 3. ターゲットが IBM Spectrum Protect Plus 仮想アプライアンスである場合の通信ポート (続き)

ポート	プロトコル	イニシエーター	ターゲット	説明
8090	TCP	管理コンソール	IBM Spectrum Protect Plus 仮想アプライアンス	システム管理用のアクセスを提供します。この拡張可能なフレームワークは、システム更新やネットワーク更新などの操作を実行するプラグインをサポートします。
111	TCP	ネットワーク・ファイル・システム (NFS) クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	IBM Spectrum Protect Plus 仮想アプライアンス: オンボード vSnap サーバー	Open Network Computing (ONC) クライアントが ONC サーバーと通信するためのポートを検出できるようにします。
2049	TCP	NFS クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	IBM Spectrum Protect Plus 仮想アプライアンス: オンボード vSnap サーバー	vSnap サーバーによる NFS ファイル共有の転送に使用されます。
3260	TCP	Internet Small Computer System Interface (iSCSI) クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	IBM Spectrum Protect Plus 仮想アプライアンス: オンボード vSnap サーバー	vSnap サーバーによる iSCSI データ転送に使用されます。
20048	TCP	NFS クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	IBM Spectrum Protect Plus 仮想アプライアンス: オンボード vSnap サーバー	vSnap サーバーによる NFS データ転送に使用されます。

ポートの更新:

- ポート 9090: 以前のバージョンでは、ポート 9090 がオンライン・ヘルプに使用されていました。V10.1.4 以降、オンライン・ヘルプにこのポートは必要でなくなっています。これ以上のアクションは不要です。
- ポート 8761: 以前のバージョンでは、VADP プロキシの自動ディスカバリーおよび IBM Spectrum Protect Plus 仮想マシン (VM) のバックアップ操作にポート 8761 が使用されていました。IBM Spectrum Protect Plus V10.1.6 以降では、VADP プロキシ・アーキテクチャが変更され、ポート 8761 を開く必要はなくなっています。IBM Spectrum Protect Plus が V10.1.6 に更新されると、環境の関連する VADP プロキシもアップグレードされます。

表 4. イニシエーターが IBM Spectrum Protect Plus 仮想アプライアンスである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
22	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	vSnap サーバーまたは VADP プロキシ・ホスト	SSH プロトコルを使用したリモートの vSnap サーバーおよび VADP プロキシでのトラブルシューティングとメンテナンスのタスクのためのアクセスを提供します。SSH プロトコルを使用した IBM Spectrum Protect Plus 仮想アプライアンスからの vSnap データ複製にも使用されます。
25	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	Simple Mail Transfer Protocol (SMTP) を使用してアクセスできる E メール・サーバー	E メール・サービスへのアクセスを提供します。
389	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	Lightweight Directory Access Protocol (LDAP) サーバー	Active Directory サービスへのアクセスを提供します。
443	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	ハイパーバイザー: VMware Elastic Sky X Integrated (ESXi) ホストおよび vCenter	操作を管理するための ESXi および vCenter へのアクセスを提供します。
636	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	LDAP サーバー	SSL プロトコルを使用した Active Directory サービスへのアクセスを提供します。
902	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	ハイパーバイザー: VMware ESXi ホスト	vSphere コンポーネントに対するファイル・タイプ認識ファイル転送プロトコル (FTP) サービスを提供する Network File Copy (NFC) プロトコルに使用されます。 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。

表 4. イニシエーターが IBM Spectrum Protect Plus 仮想アプライアンスである場合の通信ポート (続き)

ポート	プロトコル	イニシエーター	ターゲット	説明
5985	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	ハイパーバイザー: iSCSI イニシエーターを使用する Hyper-V またはエージェント	Windows ベースのサーバーに Microsoft Windows Remote Management (WinRM) サービスへのアクセスを提供します。
5986	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	ハイパーバイザー: iSCSI イニシエーターを使用する Hyper-V またはエージェント	Windows ベースのサーバーに Microsoft Windows Remote Management (WinRM) サービスへのアクセスを提供します。
8098	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	VADP プロキシ・ホスト	Transport Layer Security (TLS) プロトコルを使用した IBM Spectrum Protect Plus 仮想アプライアンスと VADP プロキシの間の REST API 通信をサポートします。
8900	TCP	IBM Spectrum Protect Plus アプライアンス	vSnap サーバー (vSnap server)	TLS プロトコルを使用した IBM Spectrum Protect Plus 仮想アプライアンスと vSnap サーバーの間の REST API 通信をサポートします。

IBM Spectrum Protect Plus の通信パスの図

次の図は、IBM Spectrum Protect Plus によって管理される通信パスの概要です。この図は、デプロイメント・シナリオのトラブルシューティングとネットワーク構成に役立ちます。

- 背景がグレイでラベルが付いたリソースは、IBM Spectrum Protect Plus 仮想アプライアンスのコア・サービスを表します。
- 各種モジュールの色は、鍵で定義される各種タイプのサービスを表します。
- 「ファイアウォール」のラベルが付いたエリアは、ネットワーク・ファイアウォールを表します。
- 「ファイアウォール」エリアに示されているサービスは、ファイアウォールで開いているポートを示します。
- 破線の矢印は、リソースとサービス間の通信を表します。
- 矢印は、listen ポートに向かっています。
- 開く必要があるポート番号は、listen ポートで示されています。

例えば次のとおりです。

- vSnap サービスは、IBM Spectrum Protect Plus 仮想アプライアンスの外部として表されます。vSnap サービスは、ポート 8900 とその他のポートで listen します。
- 仮想アプライアンス内のコンポーネントは、ポート 8900 で vSnap サービスとの接続を使用して通信パスを確立します。

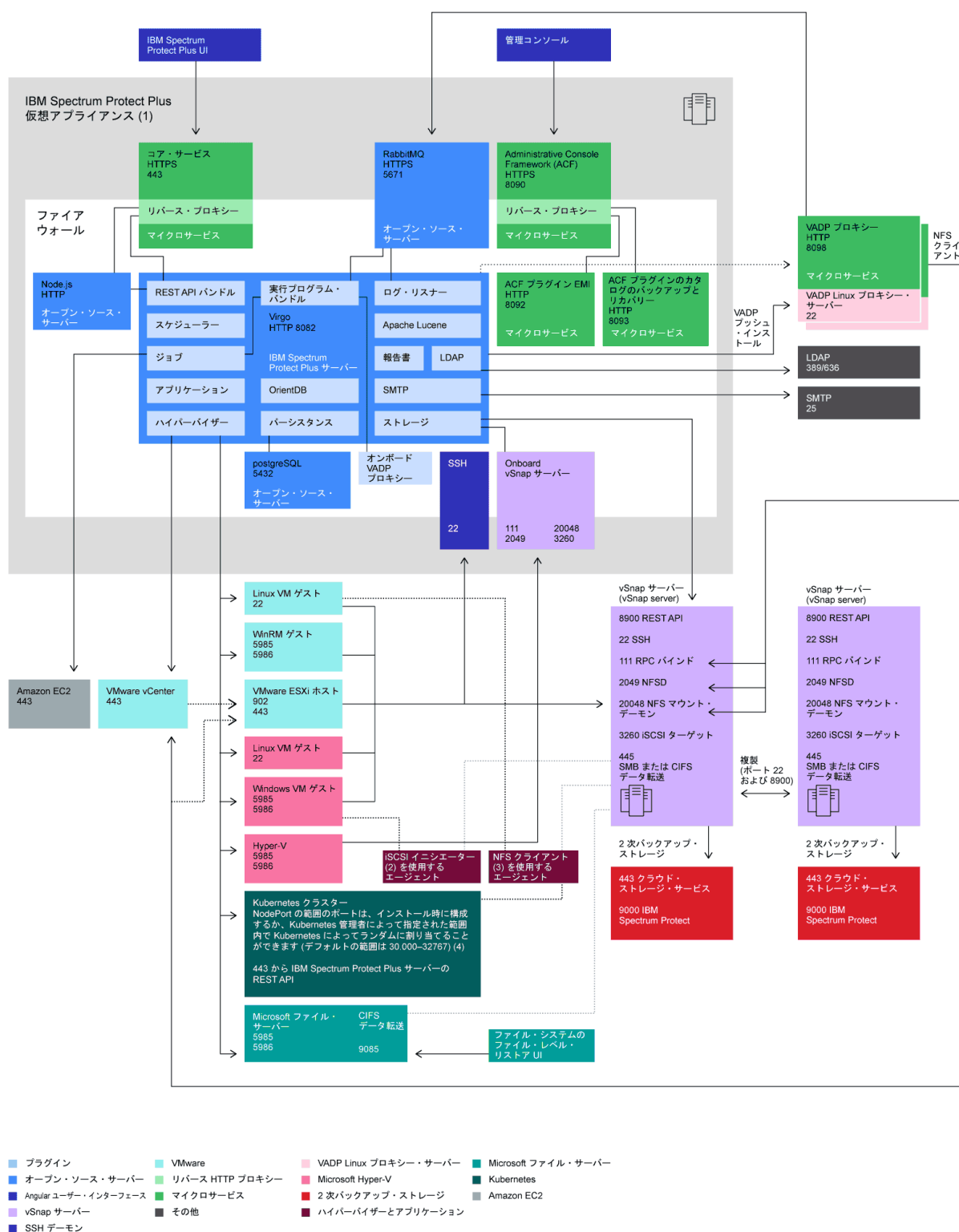


図 9. IBM Spectrum Protect Plus の通信パスの図

¹ IBM Spectrum Protect Plus 仮想アプライアンスには以下の基本コンポーネントが組み込まれています。IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシ。詳しくは、[5 ページの『製品のコンポーネント』](#)を参照してください。

² 以下のエージェントは iSCSI イニシエーターを使用します。Microsoft Hyper-V、Microsoft SQL Server、および Microsoft Exchange。

³ 以下のエージェントは NFS クライアントを使用します。VMware、Oracle、IBM Db2[®]、MongoDB、Kubernetes、および Microsoft Office 365。

⁴ SSH ポートは、IBM Spectrum Protect Plus サーバーを Kubernetes Backup Support エージェントに接続します。ポートを選択しない場合、NodePort サービスによってデフォルトの範囲内のランダムなポート番号が選択されます。このポートに値を指定する場合は、Kubernetes 管理者によって設定された NodePort の範囲内でまだ使用されていないポート番号を使用してください。

vSnap サーバーの要件

vSnap サーバーのインストール

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。localhost vSnap サーバーは、デモンストレーションやテストの目的に適しています。実稼働環境で使用するには、1 つ以上の外部 vSnap サーバーをインストールする必要があります。

効率的なデータ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。IBM Spectrum Protect Plus ソリューションの作成方法について詳しくは、[IBM Spectrum Protect Plus Blueprints](#) を参照してください。

vSnap サーバーの初期デプロイメント

初期のデプロイメントの場合、VM または物理的な Linux[®] サーバー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・サーバー
- 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。

オプションで、バックアップとリストアのパフォーマンスを向上させるためにソリッド・ステート・ドライブ (SSD) を使用します。

- バックアップのパフォーマンスを向上させるために、SSD にバックアップされる 1 つ以上のログ装置を使用するようにストレージ・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 にバックアップされるキャッシュ装置を使用するようにストレージ・プールを構成します。

vSnap サーバーの VM インストール

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

- 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) (IBM Spectrum Protect Plus V10.1.2 以降)
- vSphere 7.0 (すべての更新およびパッチ・レベルを含む) (IBM Spectrum Protect Plus V10.1.6 以降)
- Microsoft Hyper-V 2016
- Microsoft Hyper-V 2019 (IBM Spectrum Protect Plus V10.1.3 以降)

vSnap サーバーの物理インストール

V10.1.3 以降の IBM Spectrum Protect Plus が提供する新機能には、Red Hat Enterprise Linux (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 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 V10.1.6 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) (IBM Spectrum Protect Plus V10.1.2 以降)
- CentOS 7.1810 (7.6) (x86_64) (IBM Spectrum Protect Plus V10.1.3 パッチ 1 以降)
- CentOS 7.1908 (7.7) (x86_64) (IBM Spectrum Protect Plus V10.1.3 パッチ 1 以降)
- RHEL 7.5 (x86_64) (IBM Spectrum Protect Plus V10.1.2 以降)
- RHEL 7.6 (x86_64) (IBM Spectrum Protect Plus V10.1.3 パッチ 1 以降)
- RHEL 7.7 (x86_64) (IBM Spectrum Protect Plus V10.1.5 パッチ 1 以降)

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 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 7.3.1611 (x86_64)
- CentOS 7.4.1708 (x86_64)
- RHEL 7.3 (x86_64)
- RHEL 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。

表 5. ターゲットが vSnap サーバーである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
22	TCP	NFS クライアントを使用する IBM Spectrum Protect Plus 仮想アプライアンス、ハイパーバイザー、またはエージェント	vSnap サーバー (vSnap server)	SSH プロトコルを使用した vSnap サーバーでのトラブルシューティングとメンテナンスのタスクのためのアクセスを提供します。
111	TCP	NFS クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	vSnap サーバー (vSnap server)	ONC クライアントが ONC サーバーと通信するためのポートを検出できるようにします。

表 5. ターゲットが vSnap サーバーである場合の通信ポート (続き)

ポート	プロトコル	イニシエーター	ターゲット	説明
445	TCP	Server Message Block (SMB) プロトコルまたは Common Internet File System (CIFS) プロトコルを使用するアプリケーション・エージェント	vSnap サーバー (vSnap server)	トランザクション・ログのバックアップ操作とリカバリ操作作用にファイル・システム共有をマウントするために vSnap サーバーによって SMB プロトコルまたは CIFS プロトコルを介して使用されるターゲット・ポートを提供します。
2049	TCP	NFS クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	vSnap サーバー (vSnap server)	vSnap サーバーによる NFS ファイル共有に使用されます。
3260	TCP	iSCSI クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	vSnap サーバー (vSnap server)	vSnap サーバーによる iSCSI データ転送に使用されます。
8900	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	vSnap サーバー (vSnap server)	TLS プロトコルを使用した IBM Spectrum Protect Plus 仮想アプライアンスと vSnap サーバーの間の REST API 通信をサポートします。
20048	TCP	NFS クライアントを使用するハイパーバイザー、VADP プロキシ、またはエージェント	vSnap サーバー (vSnap server)	VADP プロキシ、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。このポートは、vSnap サーバーへの NFS データ転送にも使用されます。

重要なセキュリティ情報: 要求が内部ネットワーク内のノードから出される場合にのみ、vSnap データ・ポート (NFS、SMB、および iSCSI) への要求を処理します。外部 (専用でない) ネットワーク・ノードからの要求はブロックする必要があります。適切なセキュリティ・プラクティスに従っていることを確認するには、ネットワーク・セキュリティ管理者と協力してください。

ポートの更新: 以前のバージョンでは、vSnap サーバーのポート 137、138、および 139 が、SMBv1 を使用するアプリケーション・エージェントによって使用されていました。IBM Spectrum Protect Plus

V10.1.6 以降では、SMBv1 プロトコルは使用されません。すべてのエージェントが SMBv2 以降を使用するため、ポート 137、138、および 139 は不要です。

VADP プロキシ要件

VADP プロキシのインストール

IBM Spectrum Protect Plus では、VADP を使用して VM のバックアップ・ジョブを実行する際、非常に多くのシステム・リソースが必要になります。VADP バックアップ・ジョブ・プロキシを作成することにより、IBM Spectrum Protect Plus のバックアップ・ジョブのロード・シェアリングとロード・バランシングが可能になります。プロキシが存在する場合、処理中の負荷全体が IBM Spectrum Protect Plus 仮想アプリケーションからプロキシにシフトされます。

VADP プロキシは、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 環境で最小カーネル・バージョン v2.6.32 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。

- 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 (IBM Spectrum Protect Plus V10.1.1 パッチ 1 以降)
- 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 (IBM Spectrum Protect Plus V10.1.1 パッチ 1 以降)
- RHEL 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 (IBM Spectrum Protect Plus V10.1.1 以降)
- RHEL 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 (IBM Spectrum Protect Plus V10.1.1 以降)
- SUSE Linux Enterprise Server (SLES) 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 (IBM Spectrum Protect Plus V10.1.1 以降)

IBM Spectrum Protect Plus ソリューションの作成方法について詳しくは、[IBM Spectrum Protect Plus Blueprints](#) を参照してください。

VADP プロキシ・サーバーの初期のデプロイメントの場合、Linux サーバー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
- 8 GB のランダム・アクセス・メモリー (RAM) (必須)、16 GB (推奨 9)
- 60 GB の空きディスク・スペース

VADP プロキシ・サーバーでプロセッサの使用量と並行性が高くなっているため、プロキシ・サーバーに割り振られるメモリーを増やす必要があります。

プロキシは 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。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から接続可能でなければなりません。

VADP プロキシ・サーバー上のポート 8098 は、プロキシ・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 プロキシを作成するには、SYSADMIN 役割が割り当てられたユーザー ID が必要です。役割について詳しくは、507 ページの『[役割の管理](#)』を参照してください。

VADP プロキシ・ポート

VADP プロキシは、以下のポートを使用します。

表 6. ターゲットが VADP プロキシ・ホストである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
22	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	VADP プロキシ・ホスト	SSH プロトコルを使用した VADP プロキシ・ホストでのトラブルシューティングとメンテナンスのタスクのためのアクセスを提供します。
8098	TCP	IBM Spectrum Protect Plus 仮想アプライアンス	VADP プロキシ・ホスト	TLS プロトコルを使用した IBM Spectrum Protect Plus 仮想アプライアンスと VADP プロキシの間の REST API 通信をサポートします。

表 7. イニシエーターが VADP プロキシ・ホストである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
111	TCP	VADP プロキシ・ホスト	vSnap サーバー (vSnap server)	ONC クライアントが ONC サーバーと通信するためのポートを検出できるようにします。
443	TCP	VADP プロキシ・ホスト	ハイパーバイザー: VMware ESXi ホストおよび vCenter	操作を管理するための ESXi および vCenter へのアクセスを提供します。
902	TCP	VADP プロキシ・ホスト	ハイパーバイザー: VMware ESXi ホスト	vSphere コンポーネントに対するファイル・タイプ認識ファイル転送プロトコル (FTP) サービスを提供する Network File Copy (NFC) プロトコルに使用されます。 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。
2049	TCP	VADP プロキシ・ホスト	vSnap サーバー (vSnap server)	vSnap サーバーによる NFS ファイル共有の転送に使用されます。

表 7. イニシエーターが VADP プロキシ・ホストである場合の通信ポート (続き)

ポート	プロトコル	イニシエーター	ターゲット	説明
5671	TCP および AMQP	VADP プロキシ・ホスト	IBM Spectrum Protect Plus 仮想アプライアンス	VADP プロキシおよび VMware ジョブ管理ワーカーによって作成および使用されるメッセージの管理に使用されます。このポートは、RabbitMQ メッセージ・フレームワークであり、ジョブ・ログ管理も容易にします。
20048	TCP	VADP プロキシ・ホスト	vSnap サーバー (vSnap server)	VADP プロキシ、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。このポートは、vSnap サーバーへの NFS データ転送にも使用されます。

VADP プロキシは、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。

ポートの更新: 以前のバージョンでは、VADP プロキシの自動ディスカバリーおよび IBM Spectrum Protect Plus 仮想マシン (VM) のバックアップ操作にポート 8761 が使用されていました。IBM Spectrum Protect Plus V10.1.6n 以降では、VADP プロキシ・アーキテクチャーが変更され、ポート 8761 を開く必要はなくなっています。IBM Spectrum Protect Plus が V10.1.6 に更新されると、環境の関連する VADP プロキシも更新されます。

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開くか閉じて、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・ポートの編集手順については、[99 ページの『ファイアウォール・ポートの編集』](#)を参照してください。

vSnap サーバー上の VADP プロキシ

VADP プロキシは、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検討して、コアと RAM の要件を一緒に追加し、VADP プロキシと 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 プロキシが仮想 vSnap サーバーにインストールされている場合は、以下の要件が満たされている必要があります。

- 64 ビット 8 コア・プロセッサ
- 48 GB RAM

VADP プロキシと vSnap サーバーの組み合わせで、必要な [31 ページの『VADP プロキシ・ポート』](#)と [29 ページの『vSnap サーバーのポート』](#)のすべてが開いていなければなりません。

接続要件

- IBM Spectrum Protect Plus は、ネットワーク・ファイル・システム (NFS) を使用して、バックアップ操作とリストア操作のストレージ・ボリュームをマウントします。Linux では、ネイティブ Linux NFS クライアントが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 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録できます。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスによって解決可能で、vSnap サーバーから解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で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 仮想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。

リポジトリ・サーバーのストレージ要件

クラウド・ストレージにデータをコピーするためのリポジトリ・サーバーとして IBM Spectrum Protect を使用する予定の場合は、IBM Spectrum Protect V8.1.10 を使用していることを確認してください。

クラウド・ストレージ要件

ディスク・キャッシュ領域

クラウドとアーカイブのターゲットとの間でのデータのコピー操作とリストア操作に関連するすべての機能を使用するには、vSnap サーバーで、ディスク・キャッシュ領域が vSnap サーバーに存在している必要があります。

- コピー操作中に、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。
- リストア操作中に、ディスク・キャッシュ領域は、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可能性があ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とインストールの手順については、[IBM Spectrum Protect Plus Blueprints](#) を参照してください。

マルチパス

オブジェクト・ストレージへのコピー操作中、IBM Spectrum Protect Plus は、vSnap サーバー上の仮想クラウド装置の接続と切り離しを行います。vSnap サーバーで **dm-multipath** を使用してマルチパス構成が有効になっている場合、この構成がコピー操作を妨害する可能性があります。この妨害を回避するには、仮想クラウド装置をマルチパス構成から除外する必要があります。マルチパス構成ファイル /etc/multipath.conf の blacklist セクションの下に以下の行を追加してください。

```
blacklist {
    device {
        vendor "LIO-ORG"
        product ".*"
    }
}
```

この変更を行った後、次のコマンドを使用して、マルチパス構成を再ロードします。

```
sudo systemctl reload multipathd
```

証明書

- **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・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・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・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

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・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 のルート証明書または中間証明書を各 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

vSnap サーバーとクラウドまたはリポジトリ・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 8. ターゲットがクラウド・サーバーまたはリポジトリ・サーバーのエンドポイントである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
443	TCP	vSnap サーバー (vSnap server)	クラウド・サーバー・エンドポイント	vSnap サーバーが Amazon Simple Storage Service (S3)、Microsoft Azure、または IBM Cloud Object Storage のエンドポイントと通信できるようにします。
9000	TCP	vSnap サーバー (vSnap server)	リポジトリ・サーバー・エンドポイント	vSnap サーバーが IBM Spectrum Protect (リポジトリ・サーバー) エンドポイントと通信できるようにします。

SSL をインスペクションするか、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のディープ・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・コピー・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

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、自動的に永久差分バックアップ・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

- **標準オブジェクト・ストレージ:** 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・オブジェクト・ストレージ:** 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

- **標準オブジェクト・ストレージ:** 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、Write Once Read Many (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。バケットでは、Name Index 設定が有効になっている必要があります。
- **アーカイブ・オブジェクト・ストレージ:** 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。バケットでは、Name Index 設定が有効になっている必要があります。

• Microsoft Azure の要件

- **標準オブジェクト・ストレージ:** 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・ストレージ・アカウントまたはクール・ストレージ・アカウント内の既存のコンテナを指定する必要があります。
- **アーカイブ・オブジェクト・ストレージ:** 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・ストレージ・アカウントまたはクール・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・サーバー) の要件

- **標準オブジェクト・ストレージ:** 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・オブジェクト・ストレージ:** 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 9. クラウド・プロバイダーのコピーおよびアーカイブ・コピーの要件		
操作	プロバイダー	要件
コピー	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。
コピー	IBM Cloud オブジェクト・ストレージ	既存のバケットを指定する必要があります。バケットでは、Name Index 設定が有効になっている必要があります。
コピー	Microsoft Azure	Hot Storage Tier または Cool Storage Tier から、既存のコンテナを指定する必要があります。
コピー	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・コピー	Amazon S3	vSnap サーバーは、IBM Spectrum Protect (リポジトリ・サーバー) エンドポイントと通信できる必要があります。
アーカイブ・コピー	IBM Cloud オブジェクト・ストレージ	Archive Tier から既存のバケットを指定する必要があります。バケットでは、Name Index 設定が有効になっている必要があります。
アーカイブ・コピー	Microsoft Azure	Hot Storage Tier または Archive Tier から、既存のコンテナを指定する必要があります。
アーカイブ・コピー	IBM Spectrum Protect	IBM Spectrum Protect Plus は、IBM Spectrum Protect 磁気テープにコピーされる独自の固有バケットを作成します。

ハイパーバイザー (Microsoft Hyper-V および VMware) とクラウド・インスタンス (Amazon EC2) のバックアップとリストアの要件

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 304861](#) 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
- Hyper-V Server 2019 (IBM Spectrum Protect Plus V10.1.4 以降) または Microsoft Hyper-V on Windows Server 2019 (IBM Spectrum Protect Plus V10.1.3 以降)

IBM Spectrum Protect Plus は、Hyper-V Replica 機能が使用可能になっている仮想マシン (VM) を保護します。ご使用の Hyper-V 環境によっては、システム環境を IBM Spectrum Protect Plus V10.1.6 に更新するときいくつかの SLA ポリシーを更新する必要があります。Hyper-V 環境の VM をアップグレードするため

の要件について詳しくは、[174 ページの『Hyper-V Replica 環境で仮想マシンを更新するための追加のステップ』](#)を参照してください。

Hyper-V データを保護するには、最初に Hyper-V サーバーを IBM Spectrum Protect Plus に追加してから、[266 ページの『Hyper-V データのバックアップとリストア』](#)で説明されているように、Hyper-V データをバックアップおよびリストアするためのジョブを作成します。

Hyper-V サーバーを構成する前に、それぞれの構成ステップの要件を確認してください。

- バックアップするプロバイダーの登録

Hyper-V サーバーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (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が DNS 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 仮想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。

- SLA ポリシーの構成

VM 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。

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。

- 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の確認

- Microsoft Windows 環境の場合は、[Supported Windows guest operating systems for Hyper-V on Windows Server](#) 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。

Hyper-V データのバックアップまたはリストアを行う前に、以下のアクションを実行してください。

- 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ことを確認します。「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。

- バックアップ操作とリストア操作を開始するユーザーに適切な役割とリソース・グループが割り当てられていることを確認してください。「アカウント」ペインを使用して、ユーザーに役割とリソース・グループを付与します。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。
- クローン・モードおよび元の IP 構成を使用して VM をリストアする予定の場合は、バックアップ・ジョブ定義内の「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資格情報が設定されていることを確認してください。

制約事項

- Hyper-V データの場合、バックアップ操作とリストア操作は、仮想ハード・ディスク (VHDX) でのみサポートされます。詳しくは、[Known Issues and Limitations: IBM Spectrum Protect Plus V10.1.6.x](#) を参照してください。
- IBM Spectrum Protect アーカイブからファイルをリストアする場合、ファイルは最初にテープ・ストレージからステージング・プールにマイグレーションされます。リストアするファイルのサイズによっては、このプロセスに数時間かかることもあります。

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 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) (IBM Spectrum Protect Plus V10.1.2 以降)
- vSphere 7.0 (すべての更新およびパッチ・レベルを含む) (IBM Spectrum Protect Plus V10.1.6 以降)

最新バージョンの VMware Tools が VMware VM 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 VM のタグをサポートします。

暗号化された VM のバックアップとリストアは、vSphere 6.5 以降でサポートされます。

ネットワーク・ファイル・システム (NFS) ボリュームが、同じ vCenter に属する任意の数のデータ・センターにマウントされる場合があります。NFS ボリュームが複数のデータ・センターにマウントされる場合、vCenter は同じボリュームを 2 つの異なるデータ・ストアとして扱います。IBM Spectrum Protect Plus は、それを単一のデータ・ストアとして扱い、データ・ストアがマウントされているすべてのデータ・センターのデータ・ストアにあるすべての VM と仮想マシン・ディスク (VMDK) を結合します。このデータ・ストアに対して SLA を選択すると、さまざまなデータ・センターにあるすべての VM が IBM Spectrum Protect Plus でバックアップまたはリストアされます。

IBM Spectrum Protect Plus V10.1.5 以降は、VMware Cloud (VMC) on Amazon Web Services (AWS) の Software-Defined Data Center (SDDC) によって管理されている VM を保護します。詳しくは、[IBM Spectrum Protect Plus for VMware Cloud on AWS](#) を参照してください。

VMware データを保護するには、最初に vCenter Server インスタンスを IBM Spectrum Protect Plus に追加してから、241 ページの『[VMware データのバックアップとリストア](#)』で説明されているように、データをバックアップおよびリストアするためのジョブを作成します。

- 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ます。ユーザーがバックアップとリストアのジョブ、およびレポートを実行できるようにするために、インベントリーが必要です。
- VMware データに対して少なくとも 1 つの SLA ポリシーが構成されている必要があります。
- 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」ペインを使用して、ユーザーに役割とリソース・グループを付与します。
- VM 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。
- リストア・ジョブ用の宛先が IBM Spectrum Protect Plus に登録されていることを確認してください。この要件は、データを新規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。
- クローン・モードおよび元の IP 構成を使用して VM をリストアする予定の場合は、バックアップ・ジョブ定義内の「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資格情報が設定されていることを確認してください。

制約事項

- リストアされた VM テンプレートは、VM の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。
- セキュア・シェル (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ありません。
- 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。
- 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。pRDM モード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 VM 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 VM のバックアップ操作の一環としては処理されません。

Amazon EC2 の要件

IBM Spectrum Protect Plus V10.1.6 以降では、Amazon EC2 インスタンスでのデータのバックアップとリストアに対するサポートが追加されています。

Amazon EC2 データを保護するには、最初に EC2 アカウントを IBM Spectrum Protect Plus に追加してから、279 ページの『[Amazon EC2 データのバックアップとリストア](#)』で説明されているように、そのアカウントに関連付けられている EC2 インスタンスの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。

Amazon EC2 データのバックアップまたはリストアを行う前に、以下の要件を確認してください。

- EC2 アカウントを IBM Spectrum Protect Plus に追加するには、アクセス・キーが必要です。アクセス・キーは、Identity and Access Management (IAM) ユーザーまたは AWS アカウントのルート・ユーザーの長期の資格情報です。
- Amazon EC2 アカウントが IBM Spectrum Protect Plus に追加されると、そのアカウントに関連付けられているインスタンスのインベントリがキャプチャーされます。その後、バックアップ・ジョブとリストア・ジョブを実行して、インスタンスに関するレポートを生成することができます。
- EC2 インスタンスに対して 1 つ以上の SLA ポリシーが構成されていることを確認してください。
- バックアップおよびリストアのジョブを構成するユーザーに 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ことを確認してください。
- アカウントが複数の 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。
- 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。

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 304861](#) を参照してください。

一般

- ハイパーバイザー操作では、IBM Spectrum Protect Plus は、ハイパーバイザーで使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、ハイパーバイザーの資料を参照してください。
- IBM Spectrum Protect Plus は、本書にリストされていないファイル・システムを使用する仮想マシン (VM) 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の操作に適格であるのは、リストされているファイル・システムのみです。
- ゲスト・オペレーティング・システムに直接マップされる Internet Small Computer Interface (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 VM の構成で指定されているようにマウントされる仮想マシン・ディスク (VMDK) 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、環境内の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 仮想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するスペースは、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。
- 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・サーバーにコピーされたリストア・ポイントからはサポートされません。
- 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 のユーザー名**」および「**ゲスト OS のパスワード**」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。

VMware 要件

- 最新バージョンの VMware Tools が VMware VM にインストールされていることを確認してください。
- 拡張構成における VM の設定では、**disk.EnableUUID** パラメーターが **true** に設定されなければなりません。

Hyper-V 要件

- ご使用の Hyper-V VM に最新バージョンの 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てください。
- ファイル索引付けとリストアの操作は、Hyper-V 環境における SCSI ディスクをサポートします。
 - 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。
 - Integrated Drive Electronics (IDE) ディスクはサポートされません。

Windows 要件

表 10. Windows x64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス				
IBM Spectrum Protect Plus	Windows Server 2008 R2* Standard Edition および Datacenter Edition	Windows Server 2012 R2 および Windows Server 2012R2 core* Standard Edition および Datacenter Edition	Windows Server 2016 および Windows Server 2016 core* Standard Edition および Datacenter Edition	Windows Server 2019 および Windows Server 2019 core* Standard Edition および Datacenter Edition
V10.1.0	✓	✓	✓	--
V10.1.1	✓	✓	✓	--
V10.1.2	✓	✓	✓	--
V10.1.3	✓	✓	✓	✓ (Windows Server 2019 Core のみ)
V10.1.4	✓	✓	✓	✓
V10.1.5	✓	✓	✓	✓
V10.1.6	✓	✓	✓	✓
* 基本リリースとそれ以降の保守レベルがサポートされます。				

表 11. サポートされているファイル・システムおよびディスク・ストレージのタイプのカバレッジ・マトリックス

サポートされるファイル・システム	<ul style="list-style-type: none"> • New Technology File System (NTFS) • Resilient File System (ReFS) • ファイル割り振り表 (FAT)
サポートされるディスク・ストレージ・タイプ	<p>以下の区画がある基本ディスク</p> <ul style="list-style-type: none"> • MBR (マスター・ブート・レコード) • GPT (GUID 区画テーブル) <p>制約事項: 動的ディスク上のファイルのバックアップもリストアも行うことはできません。</p>

制約事項

- Windows Remote Shell (WinRM) が有効でなければなりません。
- **重要:** IBM Spectrum Protect Plus は、本書にリストされていないファイル・システムを使用する VM 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の操作に適格であるのは、リストされているファイル・システムのみです。
- Windows 環境でファイルに索引が付けられる場合、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。

¥Program Files

¥Program Files (x86)

¥Windows

¥winnt

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。

- Windows VM のファイル索引付けおよびファイル・リストアを行うには、WindowsPowerShell バイナリー・パスが %PATH% 環境変数で設定されている必要があります。
- 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。
- 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 からのジョブ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 にファイルをリストアすることはできません。
- 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。

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、システム内の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・スペースを使用できるようにしてください。

接続要件

- IBM Spectrum Protect Plus 仮想アプライアンスのホスト名は、Windows VM 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 VM のインターネット・プロトコル (IP) アドレスは、vSphere クライアントまたは 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 VM は、IBM Spectrum Protect Plus 仮想アプライアンスでセキュア・シェル (SSH) プロトコルを使用するポート 22 への発信接続をサポートしている必要があります。
- Microsoft Windows Remote Management (WinRM) サービスが実行されている必要があります。
- IBM Spectrum Protect Plus が WinRM 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必要があります。
- 登録するマシンの IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。両方のサーバーで、WinRM サービスがポート 5985 で listen している必要があります。
- IBM Spectrum Protect Plus 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録できます。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスによって解決可能で、vSnap サーバーから解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で解決可能でなければなりません。

認証と特権の要件

VM 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・サーバーの管理ツール・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 チャレンジ応答 (NTLM) プロトコルを使用します。Hyper-V VM 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 vM の資格情報が設定されている必要があります。
- 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 仮想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 は、ローカル・ユーザー・アカウントの使用をサポートしておらず、すべての VM が単一ドメインにある環境にのみ適しています。
- 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、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 仮想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。

グループ・ポリシー・オブジェクトの要件

「グループ ポリシー オブジェクト (GPO)」設定は、以下にナビゲートすることで指定できます。

- 「コンピュータの構成」 > 「ポリシー」 > 「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」 > 「ネットワークセキュリティ:NTLM を制限する: 着信 NTLM トラフィック」

または

- 「コンピュータの構成」 > 「ポリシー」 > 「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」 > 「ネットワークセキュリティ:NTLM を制限する: 送信 NTLM トラフィック」

次に、以下のいずれかのオプションを選択します。

- すべて許可
- すべてのアカウントを許可 (Allow all accounts)

Linux 要件

表 12. Linux® x86_64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス								
IBM Spectrum Protect Plus	RHEL 6.4*	RHEL 7.0*	RHEL 8.0*	CentOS 6.4*	CentOS 7.0*	CentOS 8.0*	SLES 12.0*	SLES 15.0*
V10.1.0	✓	✓	--	✓	✓	--	✓	--
V10.1.1	✓	✓	--	✓	✓	--	✓	--
V10.1.2	✓	✓	--	✓	✓	--	✓	--
V10.1.3	✓	✓	--	✓	✓	--	✓	--
V10.1.4	✓	✓	--	✓	✓	--	✓	--
V10.1.5	✓	✓	--	✓	✓	--	✓	--
V10.1.6	✓	✓	✓	✓	✓	✓	✓	✓
* 基本リリースとそれ以降の保守レベルがサポートされます。								

表 13. サポートされているファイル・システムのカバレッジ・マトリックス	
サポートされるファイル・システム	<ul style="list-style-type: none">• ext2• ext3• ext4• XFS

制約事項

- 新しいカーネル・バージョンで作成されたファイル・システムが、旧カーネル・バージョン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。
- Linux 環境でファイルに索引が付けられる場合、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、システム内の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・スペースを使用できるようにしてください。

ソフトウェア要件

- **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** パッケージは、バージョン 1.7.6p2 以降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。

ヒント: 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 オペレーティング・システムに含まれています。

- サポートされるバージョンの Linux x86_64 がインストールされていることを確認します。
- オペレーティング・システムに対応している International Components for Unicode (libicu) rpm パッケージがインストールされている必要があります。
- 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。
- IBM Spectrum Protect Plus エージェント・ユーザーおよび IBM Db2 インスタンス・ユーザーの有効ファイル・サイズ **ulimit -f** 値が、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。

- **Red Hat® Enterprise Linux** および **CentOS 6** のユーザー:

次のコマンドを実行して、util-linux-ng パッケージが最新であることを確認します。

```
yum update util-linux-ng
```

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。

- データが論理ボリューム・マネージャー (LVM) ボリューム上にある場合、LVM のバージョンが 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** コマンドを実行します。必要に応じてパッケージを更新するには **yum update lvm2** コマンドを実行します。

- 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・グループのスナップショットおよび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。このサービスを無効にするには、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 ファイルを編集して、以下の設定を指定します。

```
use_lvmetad = 0
```

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・システムにあり、**xfsprogs** パッケージのバージョンが 3.2.0 から 4.1.9 の間である場合、ファイル・リストア操作が失敗する可能性があります。この原因は、汎用固有 ID (UUID) が変更されるときにクローンまたはスナップショット・ファイル・システムが破損する、**xfsprogs** の既知の問題です。この問題を解決するには、**xfsprogs** をバージョン 4.2.0 以降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 用の Secure File Transfer Protocol (SFTP) サブシステムが使用可能であること。
- SSH サービスがプロキシ・ホスト・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 を使用してプロキシ・ホスト・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。
- IBM Spectrum Protect Plus は、ネットワーク・ファイル・システム (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。Linux では、ネイティブ Linux NFS クライアントが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 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録できます。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスによって解決可能で、vSnap サーバーから解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で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 仮想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。

認証と特権の要件

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で、**sudo** を使用する root 権限が必要です。VM の資格情報には、次の **sudo** 特権を持つユーザーが指定されている必要があります。

- **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** 設定が指定されている必要があります。

推奨される方法では、サンプル構成に示されている特権を持つ専用の IBM Spectrum Protect Plus エージェント・ユーザーを作成します。

- 次のコマンドを使用して、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。

- 次のコマンドを使用して、パスワードを設定します。

```
passwd sppagent_password
```

- 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。/etc/sudoers 構成ファイルの末尾に以下の行を追加します。

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

ファイル・システムの要件



Microsoft Windows ファイル・システム を IBM Spectrum Protect Plus に登録する前に、ご使用のシステム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 304861](#) を参照してください。

IBM Spectrum Protect Plus に対する IBM ファイル・システム 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

アプリケーションのバージョン

IBM Spectrum Protect Plus	Microsoft Windows Resilient® File System (ReFS)	Microsoft New Technology File System (NTFS)
V10.1.6		

制約事項: 割り振り表 (FAT) などの他の Microsoft Windows ファイル・システムがインベントリー・プロセス中に検出されても、それらのファイル・システムをジョブに追加することも、保護することもできません。

オペレーティング・システム

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Standard Edition および Datacenter Edition	Microsoft Windows Server 2016* Standard Edition および Datacenter Edition	Microsoft Windows Server 2019* Standard Edition および Datacenter Edition
V10.1.6			
* 基本リリースとそれ以降の保守レベル (64 ビット・カーネル) がサポートされます。			

IBM Spectrum Protect Plus は、物理 (ベアメタル) サーバーおよび仮想化環境で実行されているプロキシ・ホスト・サーバーをサポートします。

制約事項

以下の制約事項が適用されます。

- IBM Spectrum Protect Plus は、ファイル・システム 共有および Microsoft クラスター・ボリュームを保護しません。
- Microsoft FAT ファイル・システムはサポートされていません。
- IBM Spectrum Protect HSM for Windows のスタブ・ファイルはサポートされていません。
- ファイル・システ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。
- ネットワーク共有は、リストア・ジョブに有効な代替ロケーションではありません。
- 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。

認証と特権

認証

Windows ファイル・システムを登録するには、IBM Spectrum Protect Plus 管理ユーザーが、保護されるファイル・システムが置かれているクライアント・ホストで登録する必要があります。

Windows ファイル・サーバーは、管理者ユーザー ID を使用して登録できます。ユーザーがドメイン管理者または管理者特権を持つローカル・ユーザーである場合は、ドメイン・ユーザー ID を使用してファイル・サーバーを登録できます。

特権

Windows ファイル・サーバーを登録するためのユーザー ID は、以下のいずれかの Windows 構成でセットアップできます。

- ユーザー・アカウント制御 (UAC) セキュリティー・コンポーネントを使用して、ローカル・システム管理者ユーザー・アカウントを無効にします。
 - Windows システムの「コントロール パネル」>「ユーザー アカウント制御の設定」を開きます。
 - スライダーを「通知しない」に移動します。
- ローカル管理者グループのメンバーのユーザーに対する管理者承認モードのセキュリティー・ポリシー設定を無効にします。
 - このユーザーとして、Windows システムの「ローカル セキュリティ ポリシー」を開きます。
 - 「セキュリティーの設定」メニューで「ローカル ポリシー」>「セキュリティー オプション」>「ユーザー アカウント制御: 管理者承認モードですべての管理者を実行する」ポリシーを選択します。
 - 「ユーザー アカウント制御: 管理者承認モードですべての管理者を実行する」を無効にします。
 - ローカル管理者グループにポリシー「サービスとしてログオン」が含まれていることを確認します。

[User Account Control Group Policy and registry key settings](#) も参照してください。

前提条件および操作

前提条件

リソースの保護を開始する前に、以下の前提条件が満たされている必要があります。詳しくは、[ファイル・システムの前提条件](#)を参照してください。

- 登録されているファイル・システムに保管されているデータのバックアップを開始する前に、バックアップ・ホスト上、および vSnap リポジトリ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。
- データを代替ロケーションにリストアする予定の場合は、追加のスペースを使用できるようにしてください。リストア・プロセス中、どのファイルも上書きされません。同じ名前のファイルが検出された場合は、両方のコピーが保持されます。
- IBM Spectrum Protect Plus ファイル・システム・エージェントが実行されている場合、自己署名証明書および鍵が作成されます。証明書を作成してその配置を管理することで、IBM Spectrum Protect Plus によるファイル・システムのファイルを保護するためのセキュア・アクセスを強化できます。

操作

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- ReFS または NTFS 上のデータの保護を開始するには、ファイル・システムが配置されているホストのアドレスを追加する必要があります。ファイル・システム・サーバーの追加で説明されているように、この手順を繰り返して、IBM Spectrum Protect Plus で保護する必要があるすべてのホストを追加できます。
- 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」ペインを使用して、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、[ユーザー・アクセスの管理](#)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。

バックアップ・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- 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 Common Internet File System (CIFS) 共有を作成します。差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。[ファイル・システム・データのバックアップ](#)で説明されているように、IBM Spectrum Protect Plus ファイル・システム・エージェントは、バックアップが実行されるサーバーに共有をマウントします。
- バックアップ・ジョブでは、特定のドライブ、ディレクトリー、またはファイルを除外するための除外規則を定義できます。これらのファイルは、SLA ポリシーの一環としても、アドホック・バックアップ・ジョブの一環としてもバックアップされません。リストア・ジョブの実行時には、除外規則は、除外規則に指定されたドライブ、ディレクトリー、またはファイルが新規コピーにリストアされないことを意味します。詳しくは、[除外規則の構文](#)を参照してください。
- ファイル・システム・データを vSnap リポジトリ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。データを元の位置にリストアすることも、別のクライアント・ホスト上の代替ロケーションにリストアすることもできます。[ファイル・システム・データのリストア](#)で説明されているように、他のリカバリー・オプションを指定することもできます。
- リストア・プロセスは、IBM Spectrum Protect Plus の「ジョブと操作」では追跡されません。ファイル・システムのファイル・レベル・リストア・ブラウザーを使用して、ジョブにドライブ、ディレクトリー、およびファイルを指定してください。このブラウザーで、リストア操作の代替ロケーションを定義したり、リストア・ジョブが完了するまでモニターしたりすることができます。
- リストア・ジョブの IBM Spectrum Protect の宛先ターゲットが登録され、正しくセットアップされていることを確認してください。
- リストア・ジョブが完了したら、「ジョブと操作」ウィンドウの「アクティブ・リソース」タブからリソースを削除する必要があります。アクティブ・リソースがキャンセルされるまで、別のリストア・ジョブを実行することはできません。

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。

- 接続に使用されるネットワーク・アダプターは、Microsoft ネットワークのクライアントとして構成する必要があります。
- Microsoft Windows Remote Management (WinRM) サービスが実行されている必要があります。
- IBM Spectrum Protect Plus が WinRM 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必要があります。
- IBM Spectrum Protect Plus のファイル・システムのファイル・レベル・リストア・ブラウザーがリストア・サービス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必要があります。
- 登録するクライアント・ホストの IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。Windows ファイル・システム・エージェントでは、Windows Remote Management サービスがポート 5985 で listen している必要があります。
- IBM Spectrum Protect Plus 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンス・サーバーおよび vSnap サーバーによって解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で解決可能でなければなりません。

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。

表 14. ターゲットが *IBM Spectrum Protect Plus* エージェントである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
5985	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus 仮想アプライアンス ¹	Windows ファイル・システム	Windows ベースのサーバーに Microsoft WinRM サービスへのアクセスを提供します
5986	TCP	IBM Spectrum Protect Plus 仮想アプライアンス ¹	Windows ファイル・システム	Windows ベースのサーバーに Microsoft WinRM サービスへのアクセスを提供します
9085	TCP	ファイル・システムのファイル・レベル・リストア・ブラウザ	Windows ファイル・システム	リストア操作時に使用されるファイル・システムのファイル・レベル・リストア・ブラウザは、その UI とファイル・サーバーを接続します

¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (製品のコンポーネントを参照)。

表 15. イニシエーターが *IBM Spectrum Protect Plus* エージェント・ユーザーである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
445	TCP	Windows ファイル・システム	vSnap サーバー (vSnap server)	トランザクション・ログのバックアップ操作とリカバリ操作にファイル・システム共有をマウントするのに使用される vSnap サーバーの CIFS ターゲット・ポートを提供します

ハードウェア

表 16. 最小のハードウェア要件

システム	ディスク・スペース	メモリ
「ソフトウェア」セクションに示す Windows オペレーティング・システム・バージョンのいずれかに対応している x86_64 ベースのハードウェア。	バックアップ・エージェント・デプロイメントに使用可能な 500 MB の空きディスク・スペース。	保護する必要があるファイル・システムでは 100 万ファイル当たり 5 GB RAM。 注: スケーラビリティ・テストでは、バックアップ候補の特定用のファイル・システムのスキャンに使用されるモジュールが、予想を上回るメモリーを消費することが判明しました。APAR がこの制約に対処します。

Kubernetes Backup Support の要件

IBM Spectrum Protect Plus Kubernetes Backup Support を Kubernetes 環境にデプロイする前に、ご使用のシステム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 304861](#) を参照してください。

Kubernetes Backup Support は、IBM Spectrum Protect Plus バージョン 10.1.6 では英語でのみ使用できます。






構成

アプリケーションのバージョン

Docker コンテナは、Kubernetes Backup Support でサポートされています。

オペレーティング・システム

表 17. Linux x86_64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス

IBM Spectrum Protect Plus	RHEL 7.6	RHEL 7.7	RHEL 7.8
V10.1.5			--
V10.1.6			

追加要件

IBM Spectrum Protect Plus は、以下のソフトウェアとシステムをサポートします。

- Kubernetes 1.18 およびそれ以降のパッチと更新
- Kubernetes 1.17 およびそれ以降のパッチと更新
- Kubernetes 1.16 およびそれ以降のパッチと更新
- Ceph Container Storage Interface (CSI) ドライバー 1.2、2.0、および 2.1 と Rados Block Device (RBD) ストレージ
- Helm v2.16.1 以降

制約事項: Helm v3 はサポートされていません。

以下の Kubernetes および Ceph CSI ドライバーのバージョンを使用する場合は、IBM Spectrum Protect Plus V10.1.5 を使用してください。

- Kubernetes v1.13 およびそれ以降のパッチと更新
- Kubernetes v1.14 およびそれ以降のパッチと更新
- Kubernetes v1.15 およびそれ以降のパッチと更新
- Ceph CSI ドライバー 1.1 と RBD ストレージ

Kubernetes のリリースについては、[Kubernetes Release Versioning](#) を参照してください。

コンテナ・バックアップ・サポートをインストールして構成するには、Kubernetes Backup Support ソフトウェアを Kubernetes 環境にデプロイする必要があります。手順については、[143 ページの『第 5 章 Kubernetes Backup Support のインストール』](#)を参照してください。

制約事項

- ロー・ブロック・ボリュームのバックアップ操作はサポートされていません。
- リストア要求が確実に正しく機能するように、Kubernetes Backup Support によって保護されているボリュームのスナップショットを手動で削除しないでください。
- スナップショットまたはコピー・バックアップを別の名前空間またはクラスターにリストアすることはできません。
- スナップショットまたはコピー・バックアップを元の永続ボリュームにリストアすることはできません。
- スナップショットまたはコピー・バックアップは、新しい永続ボリュームにのみリストアすることができます。新規ボリュームに対する Persistent Volume Claim (PVC) は、リストア操作時に自動的に作成されます。
- 前のバージョンの Kubernetes Backup Support へのロールバックはサポートされていません。つまり、Kubernetes Backup Support V10.1.5 を使用して、Kubernetes Backup Support V10.1.6 によってバックアップされたデータをリストアすることはできません。
- Kubernetes Backup Support V10.1.5 からの製品のアップグレードはサポートされていません。
- Kubernetes Backup Support V10.1.6 で BaaSReq オブジェクトが根本的に変更されたため、Kubernetes Backup Support V10.1.5 によってバックアップされたデータをリストアするために、Kubernetes Backup Support V10.1.6 を使用することはできません。

ソフトウェア

クラスターの前提条件

クラスターに関する以下の前提条件が満たされていることを確認してください。

- Kubernetes Backup Support は、CSI をサポートするストレージ・プラグインによって割り振られた永続ストレージのみを保護します。
- CSI サポートを備えた Kubernetes クラスターを稼働する必要があります。
- 永続ストレージは CSI ドライバーによって提供される必要があります、CSI ドライバーは CSI スナップショット機能をサポートしている必要があります。
- CSI スナップショット・サポートは、**kubect1** コマンド・ラインで有効にする必要があります。
- Kubernetes コマンド・ライン・ツール **kubect1** は、インストール済み環境のホストおよびローカル・パスでアクセス可能でなければなりません。
- コピー操作にデータ・ムーバーにマウントできるのは、フォーマット済みボリュームのみです。
- オプション: 製品のパフォーマンスとスケーラビリティを最適化するには、Kubernetes Metrics Server v0.3.5 以降がクラスターでインストールおよび実行されていることを確認してください。手順については、[144 ページの『Metrics Server が稼働していることの確認』](#)を参照してください。
- Kubernetes 1.16 のみ: コピー・バックアップおよびスナップショットのリストア 操作を実行するには、**VolumeSnapshotDataSource** のアルファ版のフィーチャーが有効になっている必要があります。**VolumeSnapshotDataSource** のアルファ版のフィーチャーを有効にするには、Kubernetes のスケジ

ューラー、コントローラー、および API サーバーにパッチを適用する必要があります。手順については、[143 ページの『VolumeSnapshotDataSource フィーチャーの有効化』](#)を参照してください。

- 保護されている永続ボリュームに対してストレージ・クラスを定義する必要があります。
- ターゲット・イメージ・レジストリーは、Kubernetes クラスターからアクセス可能でなければなりません。ターゲット・イメージ・レジストリーは、ローカル・イメージ・レジストリーまたは外部イメージ・レジストリーにすることができます。外部イメージ・レジストリーの場合、環境を保護するためにイメージ・プル・シークレットを構成できます。手順については、[145 ページの『外部レジストリーで使用するイメージ・プル・シークレットの作成』](#)を参照してください。
- Kubernetes Backup Support のインストールに使用されるホストは cluster-admin 特権の KUBECONFIG で kubeconfig ファイルを使用している必要があります、Helm 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。
- 新規のクラスター全体のリソースを作成するには、cluster-admin 特権を持つユーザーとしてターゲット・ユーザーにログインする必要があります。
- ユーザー ID、パスワード、およびキーを含む Kubernetes Backup Support 秘密が分散キー・バリュー・ストアの etcd に暗号化されて保存されていることを確認してください。詳しくは、[Encrypting Secret Data at Rest](#) を参照してください。

Helm の前提条件

- **helm** コマンド・ラインを使用して新規デプロイメントを実行できるように、Helm ツールがターゲット・クラスターで構成されている必要があります。Helm を使用してパッケージをデプロイすると、クラスター全体の役割ベースのアクセス制御 (RBAC) ルールと役割バインディングを生成できます。
- Kubernetes クラスターでは、Kubernetes 管理ユーザー・アカウントを持つ root ユーザーとして Helm をインストールするには、インストール・パッケージに含まれている次のスクリプトを実行します。

```
./helm_install_k8s.sh
```

IBM Spectrum Protect Plus 前提条件

IBM Spectrum Protect Plus および IBM Spectrum Protect Plus vSnap サーバーなどの外部の非コンテナ・コンポーネントは、IBM Spectrum Protect Plus 管理者によってプロビジョンおよび構成される必要があります。

- Kubernetes Backup Support 用の管理アカウントが IBM Spectrum Protect Plus で構成されている必要があります。

この管理アカウントは、データ・センターでグローバルな Lightweight Directory Access Protocol (LDAP) アカウントとして構成できます。このグローバル・アカウントは、Kubernetes Backup Support が連携するすべての外部コンポーネントにアクセスするために必要になります。

Kubernetes Backup Support をデプロイする前に、このアカウントの名前を `baas_config.cfg` 構成ファイルで `BAAS_ADMIN` パラメーターに指定する必要があります。`baas_config.cfg` は、`installer` ディレクトリーにあります。手順については、[146 ページの『Kubernetes 環境での Kubernetes Backup Support イメージのインストールとデプロイメント』](#)を参照してください。

- IBM Spectrum Protect Plus インスタンスは、VMware 仮想アプライアンスとしてデプロイされ、ライセンス交付を受けている必要があります。

ターゲット・クラスターとの間にネットワーク接続が存在している必要があります。Kubernetes Backup Support をデプロイする前に、IBM Spectrum Protect Plus のインターネット・プロトコル (IP) アドレスおよびポート番号が `baas_config.cfg` ファイルで指定されている必要があります。すべての IBM Spectrum Protect Plus インスタンスで使用するためにポート (443) を 1 つのみ指定できます。

- IBM Spectrum Protect Plus vSnap インスタンスは、VMware 仮想アプライアンスとしてデプロイされる必要があります。

– ターゲット Kubernetes クラスターおよび IBM Spectrum Protect Plus vSnap インスタンスとの間にネットワーク接続が存在している必要があります。

- vSnap インスタンスは、バックアップを保管するための外部 vSnap サーバーとして構成される必要があります。手順については、[103 ページの『第 3 章 vSnap サーバーのインストール』](#)を参照してください。
- バックアップが保存時に暗号化される場合、vSnap サーバーで暗号化用に十分な容量が割り振られていることを確認してください。

認証と特権

- IBM Spectrum Protect Plus 管理アカウントのユーザー名を必ず `baas_config.cfg` 構成ファイルで指定してください。詳しくは、[146 ページの『Kubernetes 環境での Kubernetes Backup Support イメージのインストールとデプロイメント』](#)を参照してください。
- 永続ボリュームに関連付けられている装置にアクセスするには、データ・ムーバー・コンテナが特権コンテナでなければなりません。
- [312 ページの『ユーザー役割』](#)で説明されているように、エンタープライズ・アプリケーション開発者とバックアップ管理者は、それぞれの役割に応じて、コンテナ内の永続データを保護するためにさまざまなユーザー・インターフェースと対話します。

前提条件および操作

前提条件

[52 ページの『ソフトウェア』](#)、[55 ページの『接続性』](#)、および [54 ページの『認証と特権』](#)の要件が満たされていることを確認してください。

Kubernetes Backup Support が Kubernetes 環境にインストールされている必要があります。[143 ページの『第 5 章 Kubernetes Backup Support のインストール』](#)を参照してください。

操作

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- Kubernetes Backup Support がインストールされた後、Kubernetes Backup Support コンテナ用のアプリケーション・ホストは、Kubernetes のクラスター・ホストの始動時に自動的に登録されます。クラスターが IBM Spectrum Protect Plus に登録されると、クラスターのリソースのインベントリが自動的に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。
- Kubernetes クラスターに接続されている永続ボリュームを保護するには、IBM Spectrum Protect Plus ユーザー・インターフェースで SLA ポリシーを作成して、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。コンテナにデフォルトの SLA ポリシーを使用する計画がない場合は、必ず SLA ポリシーを構成してください。手順については、[234 ページの『Kubernetes クラスター用の SLA ポリシーの作成』](#)を参照してください。
- バックアップ・ジョブを実行するユーザーに適切な役割とリソース・グループが割り当てられていることを確認してください。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。手順については、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)を参照してください。
- バックアップ要求は、保護するボリュームの PVC に送信されます。バックアップ・ジョブをスケジュールする前に、以下のアクションを実行してください。
 - 指定された名前空間に PVC が存在していることを確認してください。
 - PVC がフォーマット設定されていることを確認してください。PVC は、バックアップされる前にフォーマット設定される必要があります。PVC を正しくフォーマット設定するには、マウントされていて書き込まれている必要があります。ロー・ブロック・ボリュームのバックアップ操作はサポートされていません。
 - PVC に割り当てる SLA ポリシーを決定します。使用可能な SLA ポリシーを表示する手順については、[311 ページの『SLA ポリシー』](#)を参照してください。
 - PVC 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。

バックアップ・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、バックアップ操作とリストア操作のジョブを作成したり、Kubernetes Backup Support ジョブを期限切れにしたり、モニターしたり、レポートを作成したりすることができます。手順については、[314 ページの『IBM Spectrum Protect Plus ユーザー・インターフェースを使用した Kubernetes クラスターのバックアップおよびリストア』](#)を参照してください。
- Kubernetes 環境のアプリケーション開発者は、コンテナ・データのバックアップとリストアを行い、Kubernetes Backup Support 要求の状況を照会するために Kubernetes コマンド・ライン・インターフェースを使用することで、Kubernetes Backup Support 要求を送信することができます。手順については、[327 ページの『コマンド・ラインを使用したコンテナの保護』](#)を参照してください。

接続性

次の接続要件を満たしているようにしてください。

- セキュア・シェル (SSH) の Secure File Transfer Protocol (SFTP) サブシステムが有効になっていること。
- SSH サービスが Kubernetes NodePort サービスで実行中であること。
- IBM Spectrum Protect Plus が Kubernetes クラスターの NodePort ポート範囲を介して SSH を使用することでデータ・ムーバー・コンテナ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。NodePort サービスでは、NodePort 範囲内の特定のポートを実行時に Kubernetes によって決定できます。
- IBM Spectrum Protect Plus は、ネットワーク・ファイル・システム (NFS) プロトコルを使用して、バックアップ操作とリストア操作のストレージ・ボリュームをマウントします。ネイティブ Linux NFS クライアントがプロキシ・ホスト・サーバー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 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスおよび vSnap サーバーによって解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で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 仮想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。

ポート

以下の通信ポートが IBM Spectrum Protect Plus エージェントによって使用されます。

表 18. ターゲットが IBM Spectrum Protect Plus エージェントである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
Kubernetes で NodePort サービスによって割り当てられます	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus v 仮想アプライアンス ¹	Kubernetes	IBM Spectrum Protect Plus でエージェントをデプロイして実行するためにデータ・ムーバー・コンテナに接続するのに使用されます
¹ 5 ページの『製品のコンポーネント』 で説明されているように、IBM Spectrum Protect Plus 仮想アプライアンスのコンポーネントである IBM Spectrum Protect Plus サーバーを指します。				

Kubernetes 環境のコンテナ間の SSH 接続には、ポート 22 が使用されます。Kubernetes ホスト上でも、クラスターの外部でも、その他の接続には、実行時に NodePort サービスによって割り当てられるポートが使用されます。

表 19. イニシエーターが IBM Spectrum Protect Plus エージェントである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
111	TCP	Kubernetes	vSnap サーバー (vSnap server)	Open Network Computing (ONC) クライアントが ONC サーバーと通信するためのポートを検出できるようにします
443	TCP	Kubernetes	vSnap サーバー (vSnap server)	バックアップ、リストア、インベントリ、その他の構成の操作を実行するために IBM Spectrum Protect Plus によって発行されたコマンドに使用されます
2049	TCP	Kubernetes	vSnap サーバー (vSnap server)	vSnap サーバーとの間での NFS データ転送に使用されます。
20048	TCP	Kubernetes	vSnap サーバー (vSnap server)	VMware vStorage API for Data Protection (VADP) プロキシ、アプリケーション・サーバー、および仮想化データ・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

関連概念

309 ページの『[コンテナの保護](#)』

Kubernetes Backup Support は、データ保護を Kubernetes クラスター内のコンテナに拡張する IBM Spectrum Protect Plus のフィーチャーです。Kubernetes は、ホストのクラスター全体でコンテナのオーケストレーションを行うためのシステムです。

Db2 の要件

Db2 を IBM Spectrum Protect Plus に登録する前に、ご使用のシステム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 304861](#) 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。

アプリケーションのバージョン











表 20. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス

IBM Spectrum Protect Plus	Db2 V10.5* Enterprise Edition	Db2 V11.1* Enterprise Edition	Db2 V11.5* Enterprise Edition
V10.1.2			--
V10.1.3			--
V10.1.4			--
V10.1.5			
V10.1.6			

* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。

オペレーティング・システム

表 21. IBM PowerPC でサポートされているオペレーティング・システムのカバレッジ・マトリックス

IBM Spectrum Protect Plus	IBM AIX 7.1*	IBM AIX 7.2*
V10.1.2		
V10.1.3		
V10.1.4		
V10.1.5		
V10.1.6		

* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。

表 22. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス















IBM Spectrum Protect Plus	RHEL 6.8*	RHEL 7.0*	SLES 11.0 SP4*	SLES 12.0 SP1*
V10.1.2				
V10.1.3				

表 22. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス (続き)

V10.1.4				
V10.1.5				
V10.1.6				
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。				

表 23. Linux on Power Systems (リトル・エンディアン) でサポートされているオペレーティング・システムの カバレッジ・マトリックス

IBM Spectrum Protect Plus	RHEL 7.1*	SLES 12.0 SP1*
V10.1.4		
V10.1.5		
V10.1.6		
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。		

制約事項

- IBM Db2 pureScale® はサポートされていません。
- 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。
- 複数の区画を保護する予定の場合は、Db2 が並列バックアップ・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編集して有効にすることができます。詳しくは、[Db2 の前提条件](#)を参照してください。**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** 変数を使用できない場合は、**DB2_WORKLOAD = SAP** を指定することで要件を満たすことができます。

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。
ヒント: 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。
- ご使用の環境に最新の Db2 のパッチおよび更新をインストールしてください。
- 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。最新のパッチと更新がインストールされていることを確認してください。
- オペレーティング・システムに対応している International Components for Unicode (libicu) RPM パッケージがインストールされている必要があります。

- 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・サイズ値 `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。
- Linux 環境では、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、Linux ユーティリティ・パッケージの `util-linux-ng` または `util-linux` が最新であることを確認してください。
- **RHEL および CentOS 6 のユーザー:** `util-linux-ng` パッケージまたは `util-linux` パッケージが最新であることを確認するには、コマンド `yum update package_name` を実行してください。

認証と特権

認証

- Db2 サーバーは、Db2 サーバー上に存在するオペレーティング・システム・ユーザーを使用して IBM Spectrum Protect Plus に登録する必要があります。このユーザーは、*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。

特権

Db2 データベースを使用するには、IBM Spectrum Protect Plus エージェント・ユーザーに以下の権限が必要です。

- 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れらの特権が必要です。
 - `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` 設定値を設定する必要があります。[Db2 の sudo 特権の設定](#)を参照してください。
- `/usr/local/bin` ディレクトリーで **db21s** コマンドを使用して Db2 インベントリーを読み取る特権。IBM Spectrum Protect Plus では、Db2 インスタンスとデータベースに関する情報を検出し、収集するのにこれらの特権が必要です。

前提条件および操作

前提条件

リソースの保護を開始する前に、以下の前提条件が満たされている必要があります。詳しくは、[Db2 の前提条件](#)を参照してください。

- 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 データベース管理システム、バックアップ操作のボリューム・グループ、およびリストア操作中にファイルをコピーするためのターゲット・ボリュームで十分なスペースを使用できる必要があります。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。
 - Db2 データベースをバックアップする前に、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。
 - AIX の場合、Enhanced Journaled File System (JFS2) 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。
- 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。このセットアップは、マウントされた vSnap からターゲット・ホストへのデータのコピーをサポートします。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。
- 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管理システム (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、[LVM2 および JFS2](#) を参照してください。

オペレーション

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- Db2 インスタンスが置かれているホストのアドレスを IBM Spectrum Protect Plus に追加する必要があります。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。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」ペインを使用して、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、[ユーザー・アクセスの管理](#)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。この切り捨てが原因で、特定時点リストア・ジョブが失敗する可能性があります。
- 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。
- 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予定の場合は、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。すべての区画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。

バックアップ・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- データを保護するために、定期的にスケジュールされた 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操作を有効にし、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もできます。説明については、[Db2 データのバックアップ](#)を参照してください。
- 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

スタンスにリストアするか、別のクライアント・ホスト上の代替インスタンスにリストアすることができます。説明については、[Db2 データのリストア](#)を参照してください。

接続性

次の接続要件を満たしているようにしてください。

- セキュア・シェル (SSH) の Secure File Transfer Protocol (SFTP) サブシステムが有効になっていること。
- セキュア・シェル (SSH) サービスがプロキシ・ホスト・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 を使用してプロキシ・ホスト・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。
- IBM Spectrum Protect Plus は、ネットワーク・ファイル・システム (NFS) プロトコルを使用して、バックアップ操作とリストア操作のストレージ・ボリュームをマウントします。
 - Linux では、ネイティブ Linux NFS クライアントがプロキシ・ホスト・サーバーにインストールされていることを確認してください。
 - AIX では、次のコマンドを使用して、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。

```
nfsd -p -o nfs_use_reserved_port=1
```
- IBM Spectrum Protect Plus 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスおよび vSnap サーバーによって解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で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 仮想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。

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。

表 24. ターゲットが IBM Spectrum Protect Plus エージェントである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
22	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus 仮想アプライアンス ¹	Db2 サーバー	ゲスト・アプリケーション・コンポーネントを実行しているリモート・プロキシ・ホスト・サーバーの SSH プロトコルを使用したトラブルシューティングとメンテナンスのためのアクセスを提供します
¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (製品のコンポーネント を参照)。				

表 25. イニシエーターが IBM Spectrum Protect Plus エージェントである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
111	TCP	Db2 サーバー	vSnap サーバー (vSnap server)	Open Network Computing (ONC) クライアントが ONC サーバーと通信するためのポートを検出できるようにします
2049	TCP	Db2 サーバー	vSnap サーバー (vSnap server)	vSnap サーバーとの間での NFS データ転送に使用されます。
20048	TCP	Db2 サーバー	vSnap サーバー (vSnap server)	VMware vStorage API for Data Protection (VADP) プロキシ、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

ハードウェア

表 26. 最小のハードウェア要件	
システム	ディスク・スペース
オペレーティング・システムおよび Db2 データベース・サーバー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 500 MB 以上のディスク・スペース

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 304861](#) 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

アプリケーションのバージョン

表 27. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス

IBM Spectrum Protect Plus	Microsoft Exchange Server 2013 CU16* Standard Edition および Enterprise Edition	Microsoft Exchange Server 2016 CU5* Standard Edition および Enterprise Edition	Microsoft Exchange Server 2019* Standard Edition および Enterprise Edition
V10.1.3	✓	✓	✓
V10.1.4	✓	✓	✓
V10.1.5	✓	✓	✓
V10.1.6	✓	✓	✓
* 基本リリースとそれ以降の累積更新および保証レベルがサポートされます。			

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

表 28. Windows x64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Standard Edition および Datacenter Edition	Microsoft Windows Server 2016* Standard Edition および Datacenter Edition	Microsoft Windows Server 2019* Standard Edition および Datacenter Edition
V10.1.3	✓	✓	✓
V10.1.4	✓	✓	✓
V10.1.5	✓	✓	✓
V10.1.6	✓	✓	✓
* 基本リリースとそれ以降の保守レベルがサポートされます。			

IBM Spectrum Protect Plus は、物理 (ベアメタル) サーバーおよび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ています。

- VMware Elastic Sky X (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

66 ページの『差分バックアップ』で、書き込み範囲の追跡を有効にするための最小要件を参照してください。

制約事項

以下の制約事項が適用されます。

- Server Core オプションを使用する Windows Server 2019 はサポートされています。ただし、Server Core インストール・オプションでは高細分度リストア機能はサポートされていません。
- 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 Exchange Server インスタンスは一度に 1 つのみです。
- 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際、メールボックス・リストア・ブラウザー表示は非 Unicode の .pst ファイルでのみ使用できます。
- 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際、「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別のメールボックスにドラッグすることはできません。
- メール項目を非 Unicode の個人用フォルダー (.pst) ファイルにリストアする際、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。

66 ページの『差分バックアップ』で、変更されたバイトの追跡でサポートされていないテクノロジーに関する具体的な制約事項を参照してください。

ソフトウェア

- ご使用の環境に最新の Microsoft Exchange データベースのパッチおよび更新をインストールしてください。
- サポートされているバージョンの Windows 64 ビット・オペレーティング・システムをご使用の環境にインストールしてください。最新のパッチと更新が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 を使用する前に、以下のソフトウェアをインストールする必要があります。
 - 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 (CDO) で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。
- Microsoft Exchange Server 2016 または 2019 で高細分度リストア機能を使用する場合、Microsoft 32 ビットの Outlook 2013、Outlook 2016、または Outlook 2019 が必要です。
- Microsoft に必要な以下のソフトウェアは、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 Package
 - 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。

認証と特権

認証

IBM Spectrum Protect Plus に各 Microsoft Exchange Server を名前または IP アドレスで登録します。

制約事項: IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。各 Microsoft Exchange Server の完全修飾ドメイン名は、解決可能で、IBM Spectrum

Protect Plus サーバーおよび vSnap サーバーから経路指定できる必要があります。IBM Spectrum Protect Plus サーバーの完全修飾ドメイン名は、解決可能で、Microsoft Exchange Server から経路指定できる必要があります。

ユーザー ID には、ノード上で IBM Spectrum Protect Plus Tools Service をインストールして開始するのに十分な特権が必要です。詳しくは、Microsoft の記事 [Add the Log on as a service Right to an Account](#) を参照してください。

特権

Exchange データベースを使用するには、IBM Spectrum Protect Plus エージェント・ユーザーに適切な特権が必要です。特権の割り当ての手順については、[380 ページの『特権』](#)を参照してください。

特権および制約事項に関する以下の情報を確認してください。

- 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するには、ユーザー名がセキュリティ・ポリシーで許可されている必要があります。
- 暗号化ファイル・システム (EFS) がローカルまたはグループのドメイン・ポリシーで有効になっていて、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。
- メールボックス・ブラウザーを高細分度リストア操作に使用する場合は、Exchange デジタル証明書がインストールされ、構成されている必要があります。

ヒント : Microsoft Exchange Server 2016 および 2019 では、Exchange Server は、デフォルトで Transport Layer Security (TLS) を使用するように構成されます。この TLS セキュリティは、ローカル・サーバー上の内部 Exchange Server 間および Exchange サービス間の通信を暗号化します。

前提条件および操作

前提条件

[64 ページの『ソフトウェア』](#)、[66 ページの『接続性』](#)、および [64 ページの『認証と特権』](#)の要件が満たされていることを確認してください。

リソースの保護を開始する前に、以下の前提条件が満たされている必要があります。詳しくは、[379 ページの『Exchange Server の前提条件』](#)を参照してください。

操作

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- 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 IBM Spectrum Protect Plus に登録されていることを確認してください。手順については、[381 ページの『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。
- SLA ポリシーを構成します。手順については、[384 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。
- バックアップおよびリストアのジョブを作成するユーザーに適切な役割とリソース・グループが割り当てられていることを確認してください。手順については、[503 ページの『第 18 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・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- Microsoft Exchange データベースを保護する目的で、差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。手順については、[383 ページの『Exchange データベースのバックアップ』](#)を参照してください。
- IBM Spectrum Protect アーカイブからファイルをリストアする場合、ファイルは最初にテープ・ストレージからステー징・ストレージ・プールにマイグレーションされます。リストアされるファイルのサイズによっては、このプロセスに数時間かかることもあります。
- 代替インスタンスまたは新規ファイル・ロケーションにデータをリストアする予定の場合は、「宛先パス」フィールドに入力する宛先ディレクトリーがアプリケーション・ホストに存在している必要があります。ディレクトリーがサーバーに存在していない場合は、リストア操作を実行する前に作成しておく必要があります。

- 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。「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。元のインスタンスにデータをリストアするジョブを定義できます。手順については、[Exchange データベースのリストア](#)を参照してください。

バックアップ・ジョブに適用される要件と制約事項の詳細については、[差分バックアップ](#)を参照してください。

差分バックアップ

IBM Spectrum Protect Plus では、Microsoft Exchange Server 環境における差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。

書き込み範囲の追跡を有効にするには、システム環境が以下の要件を満たしている必要があります。

- Windows Server 2012 R2 以降
- New Technology File System (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 Transparent Failover (TFO)
- スケールアウト・ファイル共有を使用する 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、割り振られるスペースのサイズが 2 倍の最大 2 GB まで増えます。

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。

以下の条件が検出されると、ファイルの基本バックアップが強制されます。

- ジャーナルの不連続性が報告されます。この問題は、ログが最大サイズに達した場合、ジャーナリングが無効になっている場合、またはカタログされている USN ID が変更された場合に起こることがあります。
- ファイル・サイズが、追跡のしきい値 (デフォルトで 1 MB) 以下である。
- 前のバックアップ操作後にファイルが追加される。

接続性

次の接続要件を満たしているようにしてください。

- 接続に使用されるネットワーク・アダプターは、Microsoft ネットワークのクライアントとして構成する必要があります。
- Microsoft Windows Remote Management (WinRM) サービスが実行されている必要があります。
- IBM Spectrum Protect Plus が WinRM 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必要があります。
- 登録するクライアント・ホストの IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。Microsoft Exchange Server では、WinRM サービスがポート 5985 で listen している必要があります。
- IBM Spectrum Protect Plus 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスによって解決可能で、vSnap サーバーから解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で解決可能でなければなりません。

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。

表 29. ターゲットが <i>IBM Spectrum Protect Plus</i> エージェントである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
5985	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus アプライアンス ¹	Microsoft Exchange Server	Windows ベースのサーバーに Microsoft WinRM サービスへのアクセスを提供します
5986	TCP	IBM Spectrum Protect Plus アプライアンス ¹	Microsoft Exchange Server	Windows ベースのサーバーに Microsoft WinRM サービスへのアクセスを提供します

¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (5 ページの『製品のコンポーネント』を参照)。

表 30. イニシエーターが <i>IBM Spectrum Protect Plus</i> エージェント・ユーザーである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
3260 このノードには iSCSI イニシエーターが必要です。	TCP	Microsoft Exchange Server	vSnap サーバー (vSnap server)	バックアップ操作とリカバリー操作に LUN をマウントするのに使用される Microsoft Internet Small Computer System Interface (iSCSI) Initiator Service の vSnap ターゲット・ポート
443	TCP	Microsoft Exchange Server	IBM Spectrum Protect Plus アプライアンス ¹	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エージェントが IBM Spectrum Protect Plus と通信できるようにするポート
445	TCP	Microsoft Exchange Server	vSnap サーバー (vSnap server)	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 サーバーの SMB または CIFS のターゲット・ポートを提供します

¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (5 ページの『製品のコンポーネント』を参照)。

ポートの更新:

- Microsoft Exchange Server では、ポート 443 を IBM Spectrum Protect Plus V10.1.4 以降で使用できます。
- 以前のバージョンでは、vSnap サーバーのポート 137、138、および 139 は、SMBv1 を使用するアプリケーション・エージェントによって使用されていました。IBM Spectrum Protect Plus V10.1.6 以降では、SMBv1 プロトコルは使用されません。すべてのエージェントが SMBv2 以降を使用するため、ポート 137、138、および 139 は不要です。

ハードウェア

表 31. 最小のハードウェア要件		
システム	ディスク・スペース	高細分度リストア操作のディスク・スペース
64 ビット・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 500 MB 以上のディスク・スペース	自動的にインストールされる Microsoft ソフトウェアに必要な最小 2.1 GB のディスク・スペース

MongoDB の要件

IBM Spectrum Protect Plus V10.1.3 以降では、MongoDB データベース・データのバックアップとリストアに対するサポートが追加されています。MongoDB アプリケーション・サーバーを IBM Spectrum Protect Plus に登録する前に、システム環境が以下の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 304861](#) を参照してください。

構成要件

アプリケーションのバージョン

表 32. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス			
IBM Spectrum Protect Plus	MongoDB V3.6* Community Server およ び Enterprise Server の 各エディション	MongoDB V4.0* Community Server およ び Enterprise Server の 各エディション	MongoDB V4.2* Community Server およ び Enterprise Server の 各エディション
V10.1.3	✓	✓	--
V10.1.4	✓	✓	--
V10.1.5	✓	✓	--
V10.1.6	✓	✓	✓
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。			

表 33. Linux x86_64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス					
IBM Spectrum Protect Plus	RHEL 6.8*	RHEL 7.0*	CentOS 6.8*	CentOS 7.0*	SLES 12.0 SP1*
V10.1.3	✓	✓	✓	✓	✓
V10.1.4	✓	✓	✓	✓	✓
V10.1.5	✓	✓	✓	✓	✓
V10.1.6	✓ IT322842: 『制約事項』を参照	✓	✓ IT322842: 『制約事項』を参照	✓	✓
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。					

表 34. Linux on Power Systems (リトル・エンディアン) でサポートされているオペレーティング・システムのカバレッジ・マトリックス		
IBM Spectrum Protect Plus	RHEL 7.1*	CentOS 7.0*
V10.1.4	✓	✓
V10.1.5	✓	✓
V10.1.6	✓ IT322842: 『制約事項』を参照	✓ IT322842: 『制約事項』を参照
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。		

以下のいずれかのゲスト・オペレーティング・システムで稼働している場合に、MongoDB 環境を IBM Spectrum Protect Plus によって保護します。

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server Kernel-based Virtual Machine (KVM)

制約事項

- ユーザー認証が有効になっていない MongoDB インスタンスはすべて、引き続き上記のすべてのオペレーティング・システムでサポートされます。APAR IT32842 の時点では、暗号化された資格情報の問題のために、ユーザー認証が有効になっている MongoDB インスタンスは、以下のオペレーティング・システムの IBM Spectrum Protect Plus V10.1.6 ではサポートされません。
 - Linux x86_64: RHEL 6.8 以降の保守レベルとモディフィケーション・レベル、CentOS 6.8 以降の保守レベルとモディフィケーション・レベル
 - Linux on Power Systems: RHEL7.1 以降の保守レベルとモディフィケーション・レベル、CentOS 7.0 以降の保守レベルとモディフィケーション・レベル
- Linux on Power Systems (リトル・エンディアン) では、MongoDB Enterprise Server Edition のみがサポートされます。

- MongoDB 共有クラスター構成は、インベントリーの実行時に検出されますが、これらのリソースはバックアップ操作とリストア操作に適格ではありません。
- 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。
- スケジュール済みバックアップ・ジョブの実行中にインベントリー・ジョブを実行しないでください。
- ネストされたマウント・ポイントを構成しないでください。

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 はバージョン 1.7.6p2 以降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。
- ヒント: 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 Linux x86_64 および Linux on 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。
- ご使用の環境に最新の MongoDB のパッチおよび更新をインストールしてください。
- サポートされるバージョンの Linux x86_64 または Linux on Power Systems (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。最新のパッチと更新がインストールされていることを確認してください。
- オペレーティング・システムに対応している International Components for Unicode (**libicu**) RPM パッケージがインストールされている必要があります。
- IBM Spectrum Protect Plus エージェント・ユーザーおよび MongoDB インスタンス・ユーザーの `ulimit -f` が、`unlimited` に設定されていることを確認します。あるいは、バックアップ・ジョブとリストア・ジョブで最大のデータベース・ファイルのコピーをサポートするのに十分に高い値を設定します。`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。
- Linux 環境では、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、Linux ユーティリティー・パッケージの `util-linux-ng` または `util-linux` が最新であることを確認してください。
- **RHEL および CentOS 6 のユーザー:** `util-linux-ng` パッケージまたは `util-linux` パッケージが最新であることを確認するには、`package_name` をパッケージ名に置き換えて、次のコマンドを実行してください。

```
yum update package_name
```

- **RHEL および CentOS 6 のユーザー:** 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 以降であることを確認してください。バージョンを更新するには、次のコマンドを実行します。

```
yum update openssl
```

認証と特権

認証

- MongoDB サーバーは、MongoDB サーバー上に存在するオペレーティング・システム・ユーザーを使用して IBM Spectrum Protect Plus に登録する必要があります。このユーザーは、IBM Spectrum Protect Plus 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。
- MongoDB Enterprise Server Edition では、暗号化されたストレージ・エンジンのみがサポートされます。

特権

MongoDB データベースを使用するには、IBM Spectrum Protect Plus エージェント・ユーザーに以下の権限が必要です。

- 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さまざまなタスクにこれらの特権が必要です。

- 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。[423 ページの『sudo 特権の設定』](#)を参照してください。
- 標準の MongoDB サーバー・モジュール /usr/local/bin/mongod を読み取る特権。IBM Spectrum Protect Plus では、インスタンスの割り当て済みドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレス名とポートを使用して MongoDB サーバーに接続するように 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、[421 ページの『MongoDB 用の役割』](#)で説明されているように、適切な特権をセットアップする必要があります。

前提条件および操作

前提条件

[70 ページの『ソフトウェア』](#)、[72 ページの『接続性』](#)、[70 ページの『認証と特権』](#)、および要件が満たされていることを確認してください。

リソースの保護を開始する前に、以下の前提条件が満たされている必要があります。詳しくは、[420 ページの『MongoDB の前提条件』](#)を参照してください。

- 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。
- 保護される各 MongoDB インスタンスを IBM Spectrum Protect Plus に登録する必要があります。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。
- 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。
- 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 スナップショット論理ボリュームごとに、ボリューム・グループ内で少なくとも 10% 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。詳しくは、[422 ページの『MongoDB 保護のためのスペース前提条件』](#)を参照してください。
- ターゲット・サーバーでリストア操作のために十分なディスク・スペースが割り振られていることを確認してください。
- 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は単一のボリューム上に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、[422 ページの『Linux LVM2』](#)を参照してください。

操作

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- 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、[423 ページの『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、[429 ページの『通常の SLA 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操作とリストア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。詳しくは、503 ページの『第 18 章 ユーザー・アクセスの管理』および 421 ページの『MongoDB 用の役割』を参照してください。

バックアップ・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- 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。手順については、427 ページの『MongoDB データのバックアップ』を参照してください。
- 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からリストアするか、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、別のクライアント・ホスト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ことができます。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。手順については、432 ページの『MongoDB データのリストア』を参照してください。
- ファイルのコピー用に専用のボリュームが割り振られていることを確認します。
- 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を使用できることを確認します。
- IBM Spectrum Protect アーカイブからデータをリストアする場合、ファイルは最初にテープ・ストレージからステージング・ストレージ・プールにマイグレーションされます。リストアされるファイルのサイズによっては、このプロセスに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・ホストとクライアント・ホストで同じバージョン・レベルでなければなりません。

接続性

次の接続要件を満たしているようにしてください。

- セキュア・シェル (SSH) の Secure File Transfer Protocol (SFTP) サブシステムが有効になっていること。
- セキュア・シェル (SSH) サービスがプロキシ・ホスト・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 を使用してプロキシ・ホスト・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。
- IBM Spectrum Protect Plus は、ネットワーク・ファイル・システム (NFS) プロトコルを使用して、バックアップ操作とリストア操作のストレージ・ボリュームをマウントします。ネイティブ Linux NFS クライアントがプロキシ・ホスト・サーバー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 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスおよび vSnap サーバーによって解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で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 仮想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。

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。

表 35. ターゲットが IBM Spectrum Protect Plus エージェントである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
22	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus v 仮想アプライアンス ¹	MongoDB	ゲスト・アプリケーション・コンポーネントを実行しているリモート・プロキシ・ホスト・サーバーの SSH プロトコルを使用したトラブルシューティングとメンテナンスのためのアクセスを提供します

¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、サイト、vSnap サーバー、および VADP プロキシが組み込まれています (5 ページの『製品のコンポーネント』を参照)。

表 36. イニシエーターが IBM Spectrum Protect Plus エージェントである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
111	TCP	MongoDB	vSnap サーバー (vSnap server)	Open Network Computing (ONC) クライアントが ONC サーバーと通信するためのポートを検出できるようにします。
2049	TCP	MongoDB	vSnap サーバー (vSnap server)	vSnap サーバーとの間での NFS データ転送に使用されます。
20048	TCP	MongoDB	vSnap サーバー (vSnap server)	VMware vStorage API for Data Protection (VADP) プロキシ、アプリケーション・サーバー、および仮想化データ・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。

ハードウェア

表 37. 最小のハードウェア要件

システム	ディスク・スペース
オペレーティング・システムおよび MongoDB 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 500 MB 以上のディスク・スペース。

Office 365 の要件

この資料では、IBM Spectrum Protect Plus の Microsoft Office 365 のバックアップとリストアの要件の詳細を説明します。プロキシ・ホストを IBM Spectrum Protect Plus に登録する前に、システム環境が以下の要件を満たしていることを確認してください。プロキシ・ホスト・サーバーは、ユーザー・インターフェース (UI) ではアプリケーション・サーバーと呼ばれます。

クラウド・サービス構成

IBM Spectrum Protect Plus V10.1.5 以降では、Microsoft Office 365 データのバックアップとリストアに対するサポートが追加されています。

Microsoft Office 365 を IBM Spectrum Protect Plus で保護する場合は、IBM Spectrum Protect Plus for Microsoft Office 365 を購入する必要があります。この資格について詳しくは、[IBM Spectrum Protect V10.1.5 の発表レター](#)を参照してください。

製品名称の更新: Microsoft Corporation は、2020 年 4 月 21 日付で、中堅規模ビジネスのお客様向けの Office 365 オファリングの新しい製品名称を発表しました。この発表により、中堅規模ビジネスのお客様向けのすべてのプランは新しい Microsoft 365 ブランドに移行しました。IBM Spectrum Protect Plus V10.1.6 のユーザー・インターフェースおよび資料では、元の製品名称の Office 365 を使用しています。詳しくは、[New Microsoft 365 offerings for small and medium-sized businesses](#) を参照してください。

プロキシ・ホスト・サーバーを IBM Spectrum Protect Plus に登録する前に、システム環境が以下の要件を満たしていることを確認してください。

構成

クラウド・サービス

Microsoft Office 365 アプリケーションを保護するには、アプリケーションを Azure Active Directory に登録して、適切な権限を付与する必要があります。開始するには、以下の項目が必要です。

- アクティブな Microsoft Office 365 サブスクリプション
- Microsoft Office 365 管理ユーザー ID およびパスワード

手順については、[Azure Active Directory への登録](#)を参照してください。

Microsoft Office 365 管理アカウントがある場合は、ユーザーを追加して、有効なライセンスを持っていることを確認することができます。手順については、[Microsoft 365 in Visual Studio subscriptions](#) を参照してください。

注: IBM Spectrum Protect Plus サーバーおよびエージェント・ユーザーは、Microsoft Office 365 テナントの管理ユーザー ID およびパスワードを保管しません。

アプリケーションのバージョン

表 38. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス					
IBM Spectrum Protect Plus	Microsoft 365 Business Basic、Business Standard、Business Premium の各エディション	Office 365 for Enterprise E1、E3、E5 の各エディション	Office365 for Education A1、A3、A5 の各エディション	Office 365 for Firstline Workers F3 エディション	Microsoft 365 for Enterprise E3、E5 の各エディション

表 38. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス (続き)

	旧製品名称: Office 365 Business: Business、 Essentials、 Business Premium の各 エディション		旧製品名称: Office 365 Education エデ ィション	旧製品名称: Microsoft 365 F1	
V10.1.5	✓	✓	✓	✓	✓
V10.1.6	✓	✓	✓	✓	

オペレーティング・システム

表 39. Linux x86_64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス

IBM Spectrum Protect Plus	RHEL 7.0*	RHEL 8.0*	CentOS 7.0*
V10.1.5	✓	--	✓
V10.1.6	✓	✓	✓

* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。

IBM Spectrum Protect Plus は、物理 (ベアメタル) および仮想化環境で実行されているプロキシ・ホスト・サーバーをサポートします。

制約事項

Microsoft Office 365 テナントは、Microsoft によって定義されているグローバルな地域になければなりません。国内の地域はサポートされていません。地域について詳しくは、[National cloud deployments](#) を参照してください。

ソフトウェア

- Java™ 8 がインストールされていることを確認してください。
- 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 はバージョン 1.7.6p2 以降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。ヒント: 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 Linux x86_64 オペレーティング・システムに含まれています。
- ご使用の環境に最新の Microsoft Office 365 のパッチおよび更新をインストールしてください。
- サポートされているバージョンの Linux x86_64 をご使用の環境にインストールしてください。
- 最新のパッチと更新がインストールされていることを確認してください。ご使用のオペレーティング・システムに対応しているバージョンの International Components for Unicode (libicu) RPM パッケージがインストールされている必要があります。IBM Spectrum Protect Plus エージェントの有効ファイル・サイズを指定する有効ファイル・サイズ ulimit -f 値が unlimited に設定されていることを確認してください。あるいは、この値を、バックアップ・ジョブとリストア・ジョブで最大の Office 365 ファイルのコピーをサポートするのに十分に高い値に設定します。

- Linux 環境で、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、Linux ユーティリティー・パッケージの util-linux-ng または util-linux が最新であることを確認してください。

認証と特権

認証

- プロキシ・ホスト・サーバーは、エージェント・ホスト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 に登録されなければなりません。このユーザーは、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。

特権

IBM Spectrum Protect Plus エージェント・ユーザーには、sudo を使用して root ユーザーとしてコマンドを実行するための特権が必要です。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。

前提条件および操作

前提条件

リソースの保護を開始する前に、以下の前提条件が満たされている必要があります。

- Office 365 アプリケーションを保護するには、アプリケーションを Azure Active Directory に登録して、適切な権限を付与する必要があります。新しいアプリケーションを Azure Active Directory に登録すると、アプリケーション ID やアプリケーション・シークレットなどのアプリケーション資格情報が Azure Active Directory ポータルで使用可能になります。手順については、『Azure Active Directory への登録』を参照してください。
- IBM Spectrum Protect Plus エージェントが Office 365 テナントにアクセスできるように、Office 365 テナント資格情報とプロキシ・ホスト・サーバーを IBM Spectrum Protect Plus に登録する必要があります。この手順は、Office 365 データを確実に IBM Spectrum Protect Plus にバックアップできるようにするために実行する必要があります。手順については、『IBM Spectrum Protect Plus への Office 365 テナントの登録』を参照してください。

操作

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- SLA ポリシーを適用します。手順については、[バックアップ・ポリシーの作成](#)を参照してください。

バックアップ・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- Microsoft Office 365 の E メール、カレンダー、連絡先、およびデータを OneDrive クラウド・ストレージにバックアップするには、[Office 365 データのバックアップ](#)を参照してください。
- vSnap サーバーまたはリモート・ストレージのバックアップ・コピーから Office 365 データをリストアするには、[Office 365 データのリストア](#)を参照してください。

接続性

次の接続要件を満たしているようにしてください。

- セキュア・シェル (SSH) の Secure File Transfer Protocol (SFTP) サブシステムが有効になっていること。
- セキュア・シェル (SSH) サービスがプロキシ・ホスト・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 を使用してプロキシ・ホスト・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。
- IBM Spectrum Protect Plus は、ネットワーク・ファイル・システム (NFS) プロトコルを使用して、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。ネイティブ Linux NFS クライアントがプロキシ・ホスト・サーバー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 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスおよび vSnap サーバーによって解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で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 仮想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。

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。

表 40. ターゲットが IBM Spectrum Protect Plus エージェント・ユーザーである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
22	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus 仮想アプライアンス ¹	プロキシ・ホスト・サーバー	ゲスト・アプリケーション・コンポーネントを実行しているリモート・プロキシ・ホスト・サーバーの SSH プロトコルを使用したトラブルシューティングとメンテナンスのためのアクセスを提供します
¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (製品のコンポーネントを参照)。				

表 41. イニシエーターが IBM Spectrum Protect Plus エージェント・ユーザーである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
111	TCP	プロキシ・ホスト・サーバー	vSnap サーバー (vSnap server)	Open Network Computing (ONC) クライアントが ONC サーバーと通信するためのポートを検出できるようにします
443	TCP	プロキシ・ホスト・サーバー	vSnap サーバー (vSnap server)	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エージェントが IBM Spectrum Protect Plus と通信できるようにするポート
2049	TCP	プロキシ・ホスト・サーバー	vSnap サーバー (vSnap server)	vSnap サーバーとの間での NFS データ転送に使用されます。

表 41. イニシエーターが IBM Spectrum Protect Plus エージェント・ユーザーである場合の通信ポート (続き)

ポート	プロトコル	イニシエーター	ターゲット	説明
20048	TCP	プロキシ・ホスト・サーバー	vSnap サーバー (vSnap server)	VMware vStorage API for Data Protection (VADP) プロキシ、アプリケーション・サーバー、および仮想化データ・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

ハードウェア

表 42. 最小のハードウェア要件

システム	ディスク・スペース	メモリ
オペレーティング・システムによってサポートされているクワッド・コア・プロセッサ搭載の互換ハードウェア	実行時に一時ファイルに使用できる 5 GB のディスク・スペース	4 GB のランダム・アクセス・メモリー (RAM)

Oracle サーバー・データベースのバックアップ要件とリストア要件

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 304861](#) を参照してください。

構成

アプリケーションのバージョン

表 43. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス

IBM Spectrum Protect Plus	Oracle 11g R2* Enterprise Edition	Oracle 12c R1* Enterprise Edition	Oracle 12c R2* Enterprise Edition	Oracle 18c* Enterprise Edition	Oracle 19c* Enterprise Edition
V10.1.1	✓	✓	✓	--	--
V10.1.2	✓	✓	✓	--	--
V10.1.3	✓	✓	✓	✓	--
V10.1.4	✓	✓	✓	✓	--

表 43. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス (続き)

IBM Spectrum Protect Plus	Oracle 11g R2* Enterprise Edition	Oracle 12c R1* Enterprise Edition	Oracle 12c R2* Enterprise Edition	Oracle 18c* Enterprise Edition	Oracle 19c* Enterprise Edition
V10.1.5	✓	✓	✓	✓	✓
V10.1.6	✓	✓	✓	✓	✓
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。					

ヒント : 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・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、Recovery Manager (RMAN) と組み合わせたインスタント・ディスク・リストアのリカバリー操作を使用して実行できます。

オペレーティング・システム

表 44. IBM PowerPC でサポートされているオペレーティング・システムのカバレッジ・マトリックス

IBM Spectrum Protect Plus	IBM AIX 6.1 TL9*	IBM AIX 7.1*
V10.1.1	✓	✓
V10.1.2	✓	✓
V10.1.3	✓	✓
V10.1.4	✓	✓
V10.1.5	✓	✓
V10.1.6	✓	✓
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。		

表 45. Linux® x86_64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス

IBM Spectrum Protect Plus	RHEL 6.5*	RHEL 7.0*	RHEL 8.0*	CentOS 6.5*	CentOS 7.0*	CentOS 8.0*	SLES 11.0 SP4*	SLES 12.0 SP1*	SLES 15.0*
V10.1.1	✓	✓	--	✓	✓	--	✓	✓	--
V10.1.2	✓	✓	--	✓	✓	--	✓	✓	--

表 45. Linux® x86_64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス (続き)

IBM Spectrum Protect Plus	RHEL 6.5*	RHEL 7.0*	RHEL 8.0*	CentOS 6.5*	CentOS 7.0*	CentOS 8.0*	SLES 11.0 SP4*	SLES 12.0 SP1*	SLES 15.0*
V10.1.3	✓	✓	--	✓	✓	--	✓	✓	--
V10.1.4	✓	✓	--	✓	✓	--	✓	✓	✓
V10.1.5	✓	✓	--	✓	✓	--	✓	✓	✓
V10.1.6	✓	✓	✓	✓	✓	✓	✓	✓	✓
* 基本リリースとそれ以降の保守レベルおよびモディフィケーション・レベルがサポートされます。									

制約事項

- 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・リカバリー操作は、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有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。
- 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。

ネットワーク・ファイル・システム (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操作には、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・ディレクトリー内の実行可能な `oracle_home/bin/oradism` が root ユーザーによって所有され、**setuid** 特権を持っている必要があります。通常、バイナリーは 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、このバイナリーに必要な特権がない場合があります。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`

ここで、`oinstall` にはインストール済み環境を所有するグループを指定して、`oracle_home` には Oracle ホーム・ディレクトリーを指定します。

- `chmod 750 oracle_home/bin/oradism`

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、および実行中の Oracle プロセスのリストを検索して、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、それらのデータ・ファイル、ログ・ファイル、およびその他のファイル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、差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で作成されます。

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** パッケージは、バージョン 1.7.6p2 以降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。

ヒント: 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 オペレーティング・システムに含まれています。

- ご使用の環境に最新の Oracle サーバーのパッチおよび更新をインストールしてください。
- サポートされるバージョンの Linux x86_64 または Linux on Power Systems (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。最新のパッチと更新がインストールされていることを確認してください。
- ご使用のオペレーティング・システムに対応しているバージョンの International Components for Unicode (libicu) rpm パッケージがインストールされている必要があります。
- IBM Spectrum Protect Plus エージェント・ユーザーおよび Oracle 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、Oracle インスタンスを再始動して、構成を完了します。
- Linux 環境では、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、Linux ユーティリティー・パッケージの **util-linux-ng** または **util-linux** が最新であることを確認してください。
- Red Hat Enterprise Linux および CentOS 6 のユーザー: **util-linux-ng** パッケージまたは **util-linux** パッケージが最新であることを確認するには、次のコマンドを実行してください。

```
yum update package_name
```


認証と特権

認証

- 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。このユーザーは、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。

特権

Oracle サーバーを使用するには、IBM Spectrum Protect Plus エージェント・ユーザーに以下の権限が必要です。

- 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 または 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、データベースと自動ストレージ管理 (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。

これらの特権を実現するには、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、82 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。

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_password
```

- 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。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。以下の例に示すように、コマンドは構造化されています。

```
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オペレーティング・システム (OSDBA) グループにユーザーを追加します。

```
usermod -a -G oinstall,dba sppagent
```

- ASM を使用する予定の場合は、OSASM グループにもユーザーを追加します。

```
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
```

前提条件および操作

前提条件

81 ページの『ソフトウェア』、84 ページの『接続性』、および 82 ページの『認証と特権』の要件が満たされていることを確認してください。

操作

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- 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」ペインを使用して、リソースへのアクセス権限と、役割およびリソースをユーザーに付与します。詳しくは、[503 ページの『第 18 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、[448 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、[157 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。

バックアップ・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- 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。uid 値および gid 値については、Oracle データベースの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。この問題を回避するために、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してください。
- 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。この動作が原因で、特定時点リストア・ジョブが失敗する可能性があります。
- 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、[450 ページの『Oracle データのバックアップ』](#)で説明されているように、バックアップ・ジョブを使用します。
- 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、ジョブ定義時に選択されたバージョンから vSnap クローンを作成して、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、[453 ページの『Oracle データのリストア』](#)で説明されているように、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。
- IBM Spectrum Protect アーカイブからデータをリストアする場合、ファイルは最初にテープ・ストレージからステージング・プールにマイグレーションされます。リストアされるファイルのサイズによっては、このプロセスに数時間かかることもあります。
- 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。

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。

接続性

次の接続要件を満たしているようにしてください。

- セキュア・シェル (SSH) の Secure File Transfer Protocol (SFTP) サブシステムが有効になっていること。
- SSH サービスがプロキシ・ホスト・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 を使用してプロキシ・ホスト・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。
- IBM Spectrum Protect Plus は、ネットワーク・ファイル・システム (NFS) プロトコルを使用して、バックアップ操作とリストア操作のストレージ・ボリュームをマウントします。ネイティブ Linux NFS クライアントがプロキシ・ホスト・サーバー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 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、IBM Spectrum Protect Plus 仮想アプライアンスおよび vSnap サーバーから解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で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 仮想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 ノードは、物理 IP または名前登録されます。仮想名または Single Client Access Name (SCAN) を使用しないでください。

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。

表 46. ターゲットが IBM Spectrum Protect Plus エージェントである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
22	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus v 仮想アプライアンス ¹	Oracle サーバー	ゲスト・アプリケーション・コンポーネントを実行しているリモート・プロキシ・ホスト・サーバーの SSH プロトコルを使用したトラブルシューティングとメンテナンスのためのアクセスを提供します
¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (5 ページの『製品のコンポーネント』を参照)。				

表 47. イニシエーターが IBM Spectrum Protect Plus エージェント・ユーザーである場合の通信ポート

ポート	プロトコル	イニシエーター	ターゲット	説明
111	TCP	Oracle サーバー	vSnap サーバー (vSnap server)	Open Network Computing (ONC) クライアントが ONC サーバーと通信するためのポートを検出できるようにします
443	TCP	Oracle サーバー	IBM Spectrum Protect Plus v 仮想アプライアンス ¹	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エージェントが IBM Spectrum Protect Plus と通信できるようにするポート
2049	TCP	Oracle サーバー	vSnap サーバー (vSnap server)	vSnap サーバーとの間での NFS データ転送に使用されます。
20048	TCP	Oracle サーバー	vSnap サーバー (vSnap server)	VMware vStorage API for Data Protection (VADP) プロキシ、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

¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (5 ページの『製品のコンポーネント』を参照)。

ハードウェア

表 48. 最小のハードウェア要件

システム	ディスク・スペース
オペレーティング・システムおよび Oracle サーバー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 500 MB 以上のディスク・スペース

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

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 304861](#) を参照してください。

構成

アプリケーションのバージョン

表 49. IBM Spectrum Protect Plus によってサポートされているアプリケーション・レベルのカバレッジ・マトリックス

IBM Spectrum Protect Plus	Microsoft SQL Server 2008 R2 SP3* Standard Edition および Enterprise Edition	Microsoft SQL Server 2012* Standard Edition および Enterprise Edition	Microsoft SQL Server 2014* Standard Edition および Enterprise Edition	Microsoft SQL Server 2016* Standard Edition および Enterprise Edition	Microsoft SQL Server 2017* Standard Edition および Enterprise Edition	Microsoft SQL Server 2019* Standard Edition および Enterprise Edition
V10.1.1	✓	✓	✓	✓	✓ V10.1.1 パッチ 1 以降	--
V10.1.2	✓	✓	✓	✓	✓	--
V10.1.3	✓	✓	✓	✓	✓	--
V10.1.4	✓	✓	✓	✓	✓	--
V10.1.5	✓	✓	✓	✓	✓	✓ V10.1.5 パッチ 1 以降
V10.1.6	✓	✓	✓	✓	✓	✓

* 基本リリースとそれ以降の累積更新および保証レベルがサポートされます。

オペレーティング・システム

表 50. Windows x64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Standard Edition および Datacenter Edition	Microsoft Windows Server 2016* Standard Edition および Datacenter Edition	Microsoft Windows Server 2019* Standard Edition および Datacenter Edition
V10.1.1	✓	✓	--
V10.1.2	✓	✓	--
V10.1.3	✓	✓	✓

表 50. Windows x64 でサポートされているオペレーティング・システムのカバレッジ・マトリックス (続き)

IBM Spectrum Protect Plus	Microsoft Windows Server 2012 R2* Standard Edition および Datacenter Edition	Microsoft Windows Server 2016* Standard Edition および Datacenter Edition	Microsoft Windows Server 2019* Standard Edition および Datacenter Edition
V10.1.4	✓	✓	✓
V10.1.5	✓	✓	✓
V10.1.6	✓	✓	✓
* 基本リリースとそれ以降の保守レベルがサポートされます。			

制約事項

以下の制約事項が適用されます。

- 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。
- バックアップ操作時の 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。
- Volume Shadow Copy Service (VSS) リストア・ファイル・パスは 256 文字以下に制限されています。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、実動リストア・ジョブ用の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。
- VSS フレームワークの制約上、先行スペース、末尾スペース、および印刷不能文字をデータベース名に使用しないでください。詳しくは、[Backing up a SQL Server database using a VSS backup application may fail for some databases](#) を参照してください。
- SQL Server データベースの制約事項により、New Technology File System (NTFS) またはファイル割り振り表 (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。

ソフトウェア

- ご使用の環境に最新の Microsoft SQL Server のパッチおよび更新をインストールしてください。
- サポートされているバージョンの Windows 64 ビット・オペレーティング・システムをご使用の環境にインストールしてください。最新のパッチと更新がインストールされていることを確認してください。

認証と特権

認証

IBM Spectrum Protect Plus に各 Microsoft SQL Server を名前または IP アドレスで登録します。SQL Server クラスター・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。

制約事項: IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。両方のサーバーで、Windows Remote Management (WinRM) サービスがポート 5985 で listen している必要があります。完全修飾ドメイン名は、解決可能で、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから経路指定できる必要があります。

ユーザー ID には、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。これらの権限には、ローカル・セキュリティ・ポリシー内の「サービスとしてログオン」および「バッチ・ジョブとしてログオン」などの権限があります。詳しくは、Microsoft の記事 [Add the Log on as a service Right to an Account](#) を参照してください。

SQL Server 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、ユーザー ID は、ローカル管理者の名前と一致しています。

Kerberos 認証

Kerberos ベースの認証は、IBM Spectrum Protect Plus 仮想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 NT LAN Manager (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を認証する必要があります。

特権

Microsoft SQL Server を使用するには、IBM Spectrum Protect Plus エージェント・ユーザーに以下の許可が必要です。

- Microsoft 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 Always On および SQL Server フェイルオーバー・クラスター・インスタンス (FCI) 環境でクラスター・リソースにアクセスする許可

各 Microsoft SQL Server ホストは、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、バックアップ操作およびリストア操作をログに記録するには、SQL Server Virtual Device Interface (VDI) ベースのフレームワークが使用されます。VDI 接続には Microsoft 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 Microsoft SQL Server サービス・アカウントには、Microsoft 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](#) の『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、ユーザーは次のエラーを受け取る場合があります。

A specified logon session does not exist. It might already have been terminated.

この動作は、ネットワーク・アクセス・グループ・ポリシー設定が有効になっている場合に起こります。この設定の無効化の手順については、Microsoft サポートの記事 [Task Scheduler Error "A specified logon session does not exist"](#) を参照してください。

グループ・ポリシー・オブジェクト

「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 Manager 認証レベル」ポリシーの設定で、以下のいずれかのオプションを指定します。

- 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)

「NTLMv2 応答のみ送信する」オプションは、vSnap Common Internet File System (CIFS) および Server Message Block (SMB) のバージョンと互換性がないため、CIFS 認証の問題の原因となる可能性があります。

「グループ ポリシー オブジェクト (GPO)」設定は、以下にナビゲートすることで指定できます。

- 「コンピュータの構成」 > 「ポリシー」 > 「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」 > 「ネットワークセキュリティ: NTLM を制限する: 着信 NTLM トラフィック」

または

- ・「コンピュータの構成」 > 「ポリシー」 > 「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」 > 「ネットワークセキュリティ: NTLM を制限する: 送信 NTLM トラフィック」

次に、以下のいずれかのオプションを選択します。

- ・すべて許可
- ・すべてのアカウントを許可 (Allow all accounts)

前提条件および操作

前提条件

87 ページの『ソフトウェア』、91 ページの『接続性』、および 87 ページの『認証と特権』の要件が満たされていることを確認してください。

リソースの保護を開始する前に、以下の前提条件が満たされている必要があります。

- ・ Microsoft SQL Server システムと vSnap サーバーとの間の Internet Small Computer Interface (iSCSI) 経路が有効になっている必要があります。詳しくは、[Microsoft iSCSI Initiator Step-by-Step Guide](#) を参照してください。
- ・ Windows PowerShell バイナリー・パスが %PATH% 環境変数で設定されている必要があります。
- ・ テスト・モードでリストアされたデータベースをバックアップする 予定の場合は、グローバル設定を使用して、バックアップ・ターゲット・ボリュームのサイズを 64 TB 未満に制限してください。このグローバル設定は、データベースを保護する SLA で最初にバックアップを実行する前に設定する必要があります。バックアップ・ターゲット・ボリュームのサイズが 64 TB 以上である場合、バックアップ・ジョブは失敗します。

操作

バックアップ操作またはリストア操作を開始する前に、以下を行ってください。

- ・ バックアップする SQL Server を登録します。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がキャプチャーされ、IBM Spectrum Protect Plus に追加されます。インベントリは、バックアップとリストアのジョブ、およびレポートの実行に必要です。手順については、[461 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。手順については、[157 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、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)を参照してください。
- ・ SQL バックアップ・ジョブをセットアップして実行する前に、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してください。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**」タブをクリックします。ソース・ボリューム・サイズと入出力 (I/O) アクティビティに応じて、「**最大サイズ (Maximum size)**」値を「**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、バックアップ・ジョブの実行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。
- ・ 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、最大ワーカー・スレッド数のデフォルト値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。

す。最大ワーカー・スレッド数オプションの増加の手順については、[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。

- 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。

バックアップ・ジョブとリストア・ジョブの作成に関する以下の情報を確認してください。

- 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。手順については、[463 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 は、データベース・バックアップとトランザクション・ログ・バックアップをサポートします。IBM Spectrum Protect Plus から開始されたバックアップによって作成されたレコードの msdb.dbo.backupset に製品名が取り込まれます。
- 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。[467 ページの『SQL Server データのリストア』](#)の説明に従って、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。
- 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。
- 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・ファイルで使用する必要があります。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。
- IBM Spectrum Protect アーカイブからデータをリストアする場合、ファイルは最初にテープ・ストレージからステージング・ストレージ・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。
- 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・ジョブを開始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。

インメモリー・オンライン・トランザクション処理 (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、Microsoft 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。

- リストア・ファイル・パスは 256 文字以下に制限されています。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・シャドウ・コピー・サービス (VSS) および Microsoft SQL Server のリストア機能を条件とします。

Always On 可用性グループの構成

Microsoft 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. 構成する可用性グループを選択します。次に、「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。
4. 「バックアップを実行する場所 (Where should backups occur)」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。

Microsoft 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。

「リカバリーなし」オプションでは、SQL AlwaysOn 可用性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。

差分バックアップ

IBM Spectrum Protect Plus では、Microsoft SQL Server 環境における差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。

書き込み範囲の追跡を有効にするには、システム環境が以下の要件を満たしている必要があります。

- 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)
- SMB 3.0 プロトコル
- SMB Transparent Failover (TFO)
- 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、オーバーフローの検出時に、割り振られるスペースのサイズが 2 倍の最大 2 GB まで増えます。

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。ソース・ボリュームのフリー・スペースが 100 MB 未満の場合、Microsoft SQL Server エージェントは、ソース・ボリュームのスペースを検査して、バックアップ操作を失敗させます。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。

- ジャーナルの不連続性が報告されます。この状態は、ログが最大サイズに達した場合、ジャーナリングが無効になっている場合、またはカタログされている USN ID が変更された場合に起こることがあります。
- ファイル・サイズが、追跡のしきい値 (デフォルトで 1 MB) 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

SQL ログ・バックアップが確実に正しく機能するために、Windows の「グループ ポリシー オブジェクト」設定の更新が必要になる場合があります。詳しくは、[グループ・ポリシー・オブジェクト](#)を参照してください。

接続性

次の接続要件を満たしているようにしてください。

- 接続に使用されるネットワーク・アダプターは、Microsoft ネットワークのクライアントとして構成する必要があります。
- Microsoft Windows Remote Management (WinRM) サービスが実行されている必要があります。

- IBM Spectrum Protect Plus が WinRM 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必要があります。
- 登録するマシンの IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。SQL Server では、WinRM サービスがポート 5985 で listen している必要があります。
- IBM Spectrum Protect Plus 環境に追加されるすべてのサーバー、プロキシ、アプリケーション、およびハイパーバイザーは、ドメイン・ネーム・システム (DNS) 名またはインターネット・プロトコル (IP) アドレスを使用して登録される必要があります。
- DNS 名が使用される場合は、ネットワーク経由で IBM Spectrum Protect Plus 仮想アプライアンスによって解決可能で、vSnap サーバーから解決可能でなければなりません。すべての IBM Spectrum Protect Plus コンポーネントも DNS 名で解決可能でなければなりません。

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。

表 51. ターゲットが <i>IBM Spectrum Protect Plus</i> エージェントである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
5985	伝送制御プロトコル (TCP)	IBM Spectrum Protect Plus v 仮想アプライアンス ¹	Microsoft SQL Server	Windows ベースのサーバーに Microsoft WinRm サービスへのアクセスを提供します
5986	TCP	IBM Spectrum Protect Plus v 仮想アプライアンス ¹	Microsoft SQL Server	Windows ベースのサーバーに Microsoft WinRm サービスへのアクセスを提供します
¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (製品のコンポーネントを参照)。				

表 52. イニシエーターが <i>IBM Spectrum Protect Plus</i> エージェント・ユーザーである場合の通信ポート				
ポート	プロトコル	イニシエーター	ターゲット	説明
3260 このノードには iSCSI イニシエーターが必要です。	TCP	Microsoft SQL Server	vSnap サーバー (vSnap server)	バックアップ操作とリカバリー操作用に LUN をマウントするのに使用される Microsoft iSCSI Initiator Service の vSnap ターゲット・ポート
443	TCP	Microsoft SQL Server エージェント	IBM Spectrum Protect Plus v 仮想アプライアンス ¹	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エージェントが IBM Spectrum Protect Plus と通信できるようにするポート

表 52. イニシエーターが IBM Spectrum Protect Plus エージェント・ユーザーである場合の通信ポート (続き)

ポート	プロトコル	イニシエーター	ターゲット	説明
445	TCP	Microsoft SQL Server エージェント	vSnap サーバー (vSnap server)	トランザクション・ログのバックアップ操作とリカバリ操作作用にファイル・システム共有をマウントするのに使用される vSnap サーバーの SMB または CIFS のターゲット・ポートを提供します

¹ IBM Spectrum Protect Plus 仮想アプライアンスには、基本コンポーネントの IBM Spectrum Protect Plus サーバー、vSnap サーバー、および VADP プロキシが組み込まれています (製品のコンポーネントを参照)。

ポートの更新

- Microsoft SQL Server では、ポート 443 を IBM Spectrum Protect Plus V10.1.4 以降で使用できます。
- 以前のバージョンでは、vSnap サーバーのポート 137、138、および 139 は、SMBv1 を使用するアプリケーション・エージェントによって使用されていました。IBM Spectrum Protect Plus V10.1.6 以降では、SMBv1 プロトコルは使用されません。すべてのエージェントが SMBv2 以降を使用するため、ポート 137、138、および 139 は不要です。

ハードウェア

表 53. 最小のハードウェア要件

システム	ディスク・スペース
オペレーティング・システムおよび Microsoft SQL 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 500 MB 以上のディスク・スペース

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 5693313](#) 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

[167 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・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

94 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。

96 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。

103 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。ご使用の IBM Spectrum Protect Plus 環境の一部として、vSnap サーバーが少なくとも 1 つインストールされている必要があります。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。Blueprints を使用すると、必要な vSnap サーバー数を判別できます。

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。

- 21 ページの『コンポーネントの要件』および 37 ページの『ハイパーバイザー (Microsoft Hyper-V および VMware) とクラウド・インスタンス (Amazon EC2) のバックアップとリストアの要件』に記載されている IBM Spectrum Protect Plus システム要件を確認します。
- 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 `<part_number>.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 5693313](#) 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、98 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。

注： IBM Spectrum Protect Plus および vSnap アプライアンスは、クローズされたシステムであり、アンチウィルス (AV) のインストールは仮想デプロイメントおよび物理デプロイメントではサポートされません。

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. IBM Spectrum Protect Plus をデプロイします。vSphere Client (HTML5) または vSphere Web クライアント (FLEX) のどちらかを使用して、「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。
2. <part_number>.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。
3. 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。
4. 適切な宛先の計算リソースを選択します。「次へ」をクリックします。
5. テンプレートの詳細を確認します。「次へ」をクリックします。

重要： vSphere Web クライアント (FLEX) を使用する場合は、「追加構成」で `disk.enableUUID = true` と示されていることを確認してください。そうでない場合、または vSphere Client (HTML5) 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。

6. エンド・ユーザーのご使用条件を読み、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。
7. 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・ファイルを収容するのに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・スペースは少なく済みます。「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. 仮想アプライアンスのプロパティ値 (ホスト名、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、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： これらのプロパティは 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 アドレスの割り当て](#)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そのアプライアンス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。	99 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。	155 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。

- 21 ページの『コンポーネントの要件』および 37 ページの『ハイパーバイザー (Microsoft Hyper-V および VMware) とクラウド・インスタンス (Amazon EC2) のバックアップとリストアの要件』に記載されている IBM Spectrum Protect Plus システム要件を確認します。
- インストール・ファイル <part_number>.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 5693313](#) 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。

注: IBM Spectrum Protect Plus および vSnap アプライアンスは、クローズされたシステムであり、アンチウィルス (AV) のインストールは仮想デプロイメントおよび物理デプロイメントではサポートされません。

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. <part_number>.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、「仮想マシンをインプレースで登録 (既存の一意な ID を使用する (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」を確認します。「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。ナビゲーション・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をメモしてください。「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一ファイル名を再使用してください。ステップ 12 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: フォルダーが存在するディスク・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」を確認します。「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、[98 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。

重要: Hyper-V フェイルオーバー・クラスタリングを使用してデプロイされた IBM Spectrum Protect Plus または vSnap の仮想マシンは、仮想ネットワーク・アダプターごとに静的メディア・アクセス制御 (MAC) アドレスで構成する必要があります。動的 MAC アドレスを使用すると、新しい MAC アドレスが仮想ネットワーク・アダプターに割り当てられるため、フェイルオーバー後に Linux ネットワーキング構成が失われる可能性があります。MAC アドレスを構成するには、Hyper-V マネージャーまたはフェイルオーバー・クラスター・マネージャーで仮想マシンの設定を編集します。静的 MAC アドレスを各仮想ネットワーク・アダプターに確実に割り当てると、ネットワーク構成が失われることはありません。

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。	99 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。	155 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-SysXyz 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#)のパスワード要件の規則を参照してください。
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

[94 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。

[96 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

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。

以下の手順を使用して有効な製品キーを適用すると、IBM Spectrum Protect Plus 機能は無期限に使用可能になります。

手順

注：評価期間内で試用ライセンスを使用している IBM Spectrum Protect Plus サーバーのカatalog・バックアップが、評価期間内で試用ライセンスを使用している別の IBM Spectrum Protect Plus サーバーにリストアされると、Catalog・バックアップのソース・サーバーの試用ライセンスの残りの日のカウントが適用されます。これは、有効な製品キーを使用する実動ライセンスには適用されません。

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-SysXyz 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#)のパスワード要件の規則を参照してください。

3. 「**ライセンス管理**」をクリックします。
4. 「**ライセンスの更新**」ボタンをクリックしてから、「**ファイルの選択**」をクリックし、ご使用のコンピューター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. ライセンス・ファイルがアップロードされた場合は、「**ログアウト**」をクリックしてください。

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。	155 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・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・トラフィックを、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・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には、下記のコマンドを使用します。

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・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
```

iSCSI イニシエーター・ユーティリティのインストール

Internet Small Computer System Interface (iSCSI) ユーティリティをインストールする必要があるのは、iSCSI マウント・ストレージ・デバイスが IBM Spectrum Protect Plus アプライアンスまたは vSnap サーバーに直接接続される場合です。iSCSI イニシエーター・ユーティリティがインストールされると、そのパッケージがインストールされたアプライアンスまたはサーバーに、iSCSI マウント・ストレージ・デバイスを接続できます。

このタスクについて

iSCSI イニシエーター・ユーティリティは、IBM Spectrum Protect Plus アプライアンスまたは vSnap サーバーにインストールすることができます。iSCSI イニシエーター・ユーティリティは、IBM Spectrum Protect Plus と一緒に提供されますが、自動的にインストールされません。ユーティリティをインストールするには、次の手順に従います。

手順

1. iSCSI マウント・ストレージに直接接続されるアプライアンスまたはサーバーにログオンします。
 - IBM Spectrum Protect Plus アプライアンスでは、セキュア・シェル (SSH) プロトコルを使用して、適切な管理資格情報を使用して認証します。
 - vSnap サーバーの場合、SSH を使用するか、サーバーに直接アクセスし、適切な管理資格情報を使用して認証します。
2. 以下のコマンドを実行して、iSCSI イニシエーター・ユーティリティをインストールします。

```
sudo /usr/bin/yum --disablerepo=* --enablerepo=base,updates install iscsi-initiator-utils
```


第 3 章 vSnap サーバーのインストール

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。組み込みの vSnap サーバーは、デモンストレーションやテストの目的でのみ使用して、実稼働環境では使用しないでください。環境に少なくとも 1 つの vSnap サーバーがデプロイされている必要があります。

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。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。ご使用の IBM Spectrum Protect Plus 環境の一部として、vSnap サーバーが少なくとも 1 つインストールされている必要があります。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。Blueprints を使用すると、必要な vSnap サーバー数を判別できます。

始める前に

以下のステップを実行してください。

1. [21 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。ファイルおよびその他の有用な情報のダウンロードについて詳しくは、サポート・ページ <https://www.ibm.com/support/pages/node/567387> を参照してください。

注：IBM Spectrum Protect Plus および vSnap アプライアンスは、クローズされたシステムであり、アンチウィルス (AV) のインストールは仮想デプロイメントおよび物理デプロイメントではサポートされません。

重要：vSnap を含む IBM Spectrum Protect Plus コンポーネントは、IBM Spectrum Protect Server と同じマシン (物理または仮想) にインストールしないでください。

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、[29 ページの『vSnap サーバーの物理インストール』](#)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 モードを以下のように Permissive に変更します。

```
SELINUX=permissive
```

3. 再起動せずに設定をすぐに適用するには、setenforce 0 を以下のように発行します。

```
$ setenforce 0
```

4. vSnap インストール・ファイル <part_number>.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 5693313](#) を参照してください。
5. 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。

```
$ chmod +x <part_number>.run
```

6. 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。

```
$ ./<part_number>.run
```

あるいは、noprrompt オプションを使用して vSnap の非対話式のインストールまたは更新を開始することができます。このオプションが使用されると、vSnap インストーラーでは応答のプロンプトをスキップし、以下のプロンプトに対して応答として「はい」を想定します。

- ご使用条件
- カーネルをインストールして更新する
- インストールの終了時にリブートするか、必要な場合は更新する

noprrompt オプションを使用するには、次のコマンドを発行します。次のように 2 つ並んだダッシュの前後に意図的にスペースを挿入します。

```
$ sudo ./<part_number>.run -- noprrompt
```

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。	109 ページの『第 4 章 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 サーバーのインストール

仮想 vSnap サーバーを 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。このテンプレートにより、vSnap サーバ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 [98 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. vSnap サーバー・テンプレート・ファイル <part_number>.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 5693313](#) を参照してください。
2. vSnap サーバーをデプロイします。vSphere Client (HTML5) または vSphere Web クライアント (FLEX) を使用して、「アクション」メニューをクリックしてから「OVF テンプレートのデプロイ (Deploy OVF Template)」をクリックします。
3. <part_number>.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。
5. 適切な宛先の計算リソースを選択します。「次へ」をクリックします。
6. テンプレートの詳細を確認します。「次へ」をクリックします。
7. エンド・ユーザーのご使用条件を読み、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. 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・ファイルを収容するのに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。
9. 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。
10. 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tring がサポートされています。各 String はスペースを使用せずにコマンド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。

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: VM の電源は入れたままにする必要があります。

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。	109 ページの『 第 4 章 vSnap サーバーの管理 』を参照してください。

アクション	ハウツー
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 アドレスを割り当てます。 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、IP アドレスを割り当てます。	手順については、98 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。ネットワーク・プロパティを構成する際には、ネットワーク管理者と作業を行ってください。

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 <part_number>.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 5693313](#) 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「仮想マシンをインプレースで登録」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、[98 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。	109 ページの『第 4 章 vSnap サーバーの管理』 を参照してください。

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 サーバーを完全に削除する場合は、IBM Spectrum Protect Plus サーバーをクリーンアップする必要があります。この場合にクリーンアップする必要がある項目は、以下のとおりです。

- vSnap サーバーに保管されているバックアップのレコード。
- 他の vSnap サーバーとの複製関係。
- 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。IBM Spectrum Protect Plus サーバーから vSnap サーバーを登録抹消する必要があります。詳細については、[110 ページの『vSnap サーバーの登録抹消』](#)を参照してください。



重要: vSnap サーバーをアンインストールすると、データが失われる可能性があります。

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-SysXyz 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#)のパスワード要件の規則を参照してください。

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、[123 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、IBM Spectrum Protect Plus 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 vSnap サーバーの管理

バックアップ・ジョブとリストア・ジョブを有効にするには、IBM Spectrum Protect Plus に少なくとも 1 つの vSnap サーバーが必要です。vSnap サーバーは独自のアプライアンスであり、仮想的にデプロイされるか、最小要件を満たすシステム上に物理的にインストールされます。環境内の各 vSnap サーバーが認識されるには、IBM Spectrum Protect Plus に登録されなければなりません。IBM Spectrum Protect Plus に組み込まれているデモ・サイトに登録されている vSnap サーバーは、テストおよびデモの目的でのみ使用する必要があります。実稼働環境でバックアップの宛先として使用することはできません。

バックアップ・ストレージ・プロバイダーとしての vSnap サーバーの登録

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て登録した後、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を選択することができます。詳しくは、[111 ページの『バックアップ・ストレージ・オプションの構成』](#)を参照してください。

vSnap サーバーが VADP プロキシとしても登録される場合、VADP プロキシ登録が正常に行われるには、vSnap の「**ストレージ・プロパティ**」フィールドで追加されるアカウントに **sudo** 特権が必要です。詳しくは、[509 ページの『許可タイプ』](#)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・デバイスとして登録するには、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・コンソールにログインします。初期パスワードは `sppDP758-SysXyz` です。
初回ログイ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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#)でパスワード要件の規則を参照してください。
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**」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 [109 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。	120 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。	114 ページの『バックアップ・ストレージ・パートナーの構成』 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。	111 ページの『バックアップ・ストレージ・オプションの構成』 を参照してください。

関連タスク

[155 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。

- 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。
- 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。
- 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 サーバーの登録抹消

必要に応じて、ご使用の IBM Spectrum Protect Plus 環境で使用されなくなった vSnap サーバーを登録抹消できます。

始める前に

vSnap サーバーが登録抹消されると、次回の保守ジョブ中に vSnap サーバーに関連付けられているすべてのリカバリー・ポイントは、IBM Spectrum Protect Plus からパージされます。



重要: vSnap サーバーを登録抹消すると、データが失われる可能性があります。

vSnap サーバーを登録抹消する前に、シナリオを検討して登録抹消が適切かどうか、または他のアクションを実行する必要があるかどうかを判別します。

シナリオ 1: vSnap サーバーは、ストレージまたはネットワークの問題のために一時的にダウンしています。

- vSnap サーバーを登録抹消しないでください。vSnap サーバーを登録抹消すると、そのサーバーに関連付けられているリカバリー・ポイントはパージされ、バックアップはリベースされます。
- 必要なストレージまたはネットワークのメンテナンスを完了して、vSnap サーバーをオンラインに戻します。

シナリオ 2: vSnap サーバーに新規ホスト名または IP アドレスが割り当てられます。

- vSnap サーバーを登録抹消しないでください。vSnap サーバーを登録抹消すると、そのサーバーに関連付けられているリカバリー・ポイントはパージされ、バックアップはリベースされます。
- vSnap サーバーの設定を編集して、新しいホスト名または IP アドレスを指定してください。vSnap サーバーの設定を編集するには、[110 ページの『vSnap サーバーの設定の編集』](#)の指示に従います。

シナリオ 3: vSnap サーバーは使用中ではなく、再利用する予定はありません。

- vSnap サーバーを登録抹消し、vSnap サーバーに関連付けられているリカバリー・ポイントが IBM Spectrum Protect Plus から確実にパージされるように、保守ジョブを実行してください。
 - vSnap サーバーに存在していたデータの差分バックアップは、以降は使用できなくなります。
 - vSnap サーバーに存在していたデータのリカバリーは、以降は実行できなくなります。
- これ以降のバックアップ・ジョブの実行では、同じサイト内の別の vSnap サーバー上に新規ボリュームが自動的に作成され、新しい基本バックアップが実行されます。

シナリオ 4: vSnap プールが失われ、同じ vSnap サーバー上に新しいプールを構築したいと考えています。


1. vSnap サーバーを登録抹消し、古い vSnap プールに関連付けられているリカバリー・ポイントが IBM Spectrum Protect Plus から確実にパージされるように、保守ジョブを実行してください。
 - 古いプールに存在していたデータの差分バックアップは、以降は実行できなくなります。
 - 古いプールに存在していたデータのリカバリーは、以降は実行できなくなります。
2. vSnap サーバーに、プールを作成します。
3. vSnap サーバーを IBM Spectrum Protect Plus に追加して戻します。vSnap サーバーを IBM Spectrum Protect Plus に追加するには、[109 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 vSnap サーバーの登録』](#)を参照してください。
 - これ以降のバックアップ・ジョブの実行では、同じサイト内のこの vSnap サーバーまたは別の vSnap サーバー上にボリュームが自動的に作成され、新しい基本バックアップが実行されます。

シナリオ 5: vSnap プールまたはサーバーが破損し、それを修復しようとしています。これは vSnap 複製サーバーからデータを複製することによって修復することができます。

- vSnap サーバーを IBM Spectrum Protect Plus から登録抹消しないでください。削除プロセスによって、バックアップがリベースされます。
- vSnap サーバーを置き換えてください。障害が起きた 1 次 vSnap サーバーの置き換えについては、セクション [129 ページの『vSnap サーバーのトラブルシューティング』](#)を参照してください。

手順

vSnap サーバーを登録抹消するには、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削除アイコン  をクリックします。
3. テキスト・ボックスにコードを入力して、vSnap サーバーの削除を確認します。「削除」をクリックして、サーバーを IBM Spectrum Protect Plus から削除します。

バックアップ・ストレージ・オプションの構成


1 次および 2 次のバックアップ・ストレージ・ホスト用に追加のストレージ関連オプションを構成できます。

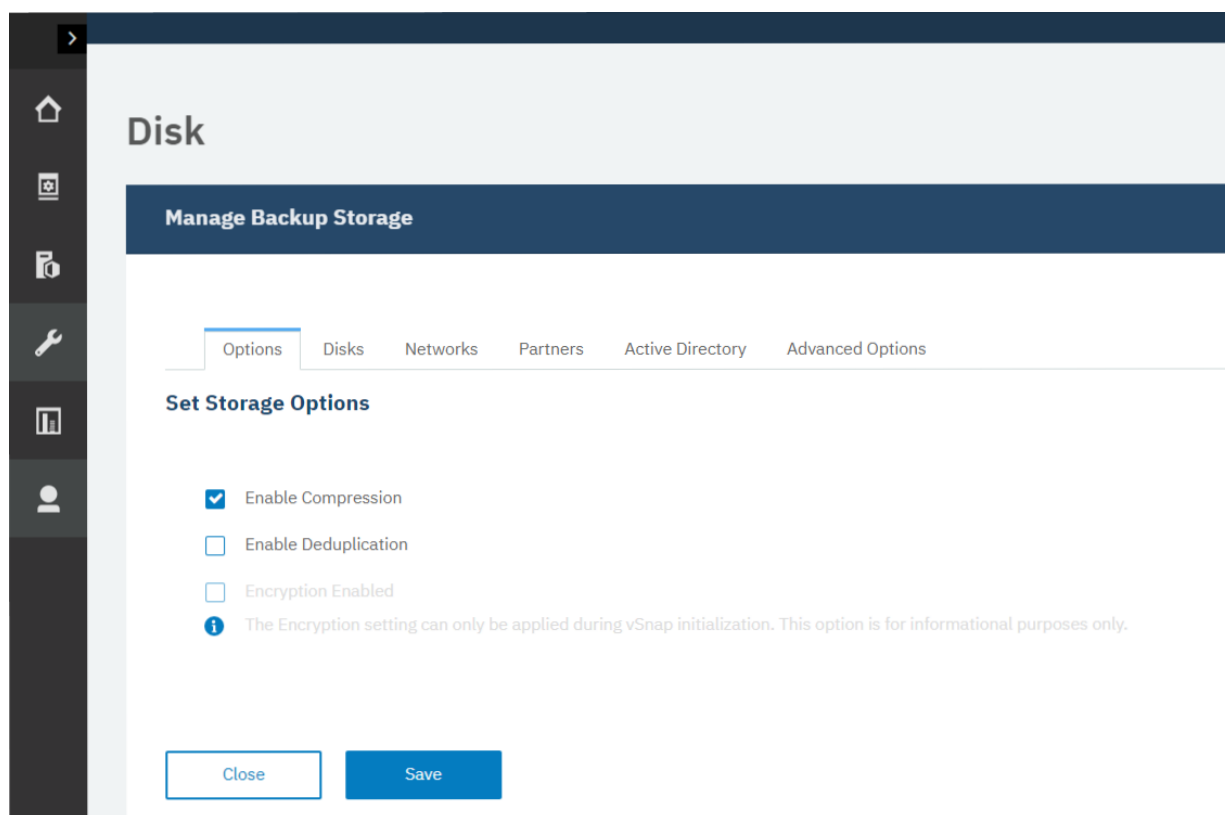
手順

登録済みディスクのバックアップ・ストレージ・オプションを構成するには、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」 、「バックアップ・ストレージ」 > 「ディスク」をクリックします。

「ディスク・ストレージ」テーブルには、バージョンと容量使用量を示す 1 次サイトと 2 次サイトのホスト名がリストされます。

2. 「ディスク・ストレージ」ペインで、更新するディスクに関連付けられている設定アイコン  をクリックします。
3. 表示されているようにストレージ・オプションから選択します。



圧縮を有効にする: このオプションを選択すると、データがストレージ・プールに書き込まれる前に、圧縮アルゴリズムを使用してデータの各着信ブロックを圧縮します。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: このオプションを選択すると、データの各着信ブロックがハッシュされ、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、デフォルトでは選択解除されています。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。

暗号化が有効: このオプションは、1 次と 2 次のバックアップ・ストレージ・ホスト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。このペインで、このオプションを変更することはできません。



4. 「保存」をクリックします。

バックアップ・ストレージへの新規ディスクの追加

選択されたストレージ・プール内のバックアップ操作の追加スペースが必要な場合は、未使用のディスク・ストレージを追加できます。これは、1 次または 2 次のバックアップ・ストレージに適用されます。

手順

新しい未使用ディスクをディスク・ストレージ・プールに追加するには、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. 「ディスク・ストレージ」ペインで、編集するサーバーに関連付けられている管理アイコン  をクリックします。

3. 「バックアップ・ストレージに新規ディスクを追加する」表で、使用可能なディスクのリストからストレージ環境に追加するディスクを選択します。

Disk

Manage Backup Storage

Options Disks Networks Partners Active Directory Advanced Options

Download Logs

Add New Disks to Backup Storage

Select one or more unused disks to add to the storage pool

Select	Disk	Size	Vendor	Model
<input type="checkbox"/>	/dev/sdaj	9.1 TiB	HGST	HUH721010AL5200

Close Save

4. 「保存」をクリックします。


ネットワーク・インターフェース・コントローラーの構成

さまざまな特定の機能に対して複数のネットワーク・インターフェース・コントローラー (NIC) を使用するように 1 次および 2 次のバックアップ・ストレージを構成できます。IBM Spectrum Protect Plus 環境内の NIC は、バックアップ、リストア、および複製の操作でデータを転送するように構成できます。NIC は、バックアップ、リストア、および複製のデータ転送を行うように、あるいは「バックアップとリストア」または「複製」のどちらかのデータ転送を行うように構成できます。別個の NIC を構成する場合、一方のネットワークを複製操作の専用にし、他方のネットワークをバックアップとリストアの操作の専用にできます。

始める前に

V10.1.6 より前のバージョンの vSnap サーバーは、この機能をサポートしていません。vSnap サーバーを更新するには、[170 ページの『vSnap サーバーの更新』](#)に記載されている手順に従います。


このタスクについて

IBM Spectrum Protect Plus から vSnap サーバーへの管理コマンドの送信専用のネットワークは、「ネットワーク」ページの  で示されます。

vSnap サーバーとさまざまなクライアント (アプリケーション・サーバー、ハイパーバイザー・ホスト、VADP プロキシ、およびバックアップ・ストレージとの間でデータを転送する環境内の他のコンポーネントなど) の間に接続を確立することができます。

手順

バックアップ操作および複製操作用に NIC を構成するには、以下のステップを実行します。

- 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。
- 「ネットワーク」タブで、リストされている NIC に対して必要な構成を選択します。
 - バックアップ操作とリストア操作に関してのみデータ転送を行うように NIC を構成するには、「バックアップ」を選択します。バックアップとリストアの操作中、この NIC の IP アドレスを使用して vSnap サーバーへの接続が確立されます。「バックアップ」オプションが複数の NIC によって指定されている場合、最初に正常に接続された NIC が使用されます。
 - 複製に関してのみデータ転送を行うように NIC を構成するには、「複製」を選択します。vSnap サーバーへの着信複製操作中に、ターゲット vSnap サーバーでこの NIC の IP アドレスを使用して接続が確立されます。ターゲット vSnap サーバー上の複数の NIC に対して「複製」オプションが指定され

ている場合は、ソース vSnap サーバーから正常に接続された最初のターゲット IP アドレスが使用されます。

- 「複製」、および「バックアップとリストア」の両方でのデータ転送のために NIC を構成するには、「バックアップ」と「複製」の両方を選択します。

Manage Backup Storage dk-vsnap-1

Options Disks **Networks** Partners Active Directory Advanced Options [Download Logs](#)

Configure Network Interface Controllers
Configure a specific network interface controller to function as the backup or replication network. [Learn More](#)

Name	MAC Address	IP Address	Backup	Replication
ailcash	12:50:33:88:99:bc	199.12.4.222	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Close](#) [Save](#)

3. 「保存」をクリックします。

バックアップ・ストレージ・パートナーの構成


他のサイトとの複製パートナーシップを確立して、環境を拡張するように、バックアップ・ストレージの 1 次サイトおよび 2 次サイトを構成することができます。複製パートナーを構成した後、追加のデータ保護層のために、サイト間でデータをコピーすることができます。

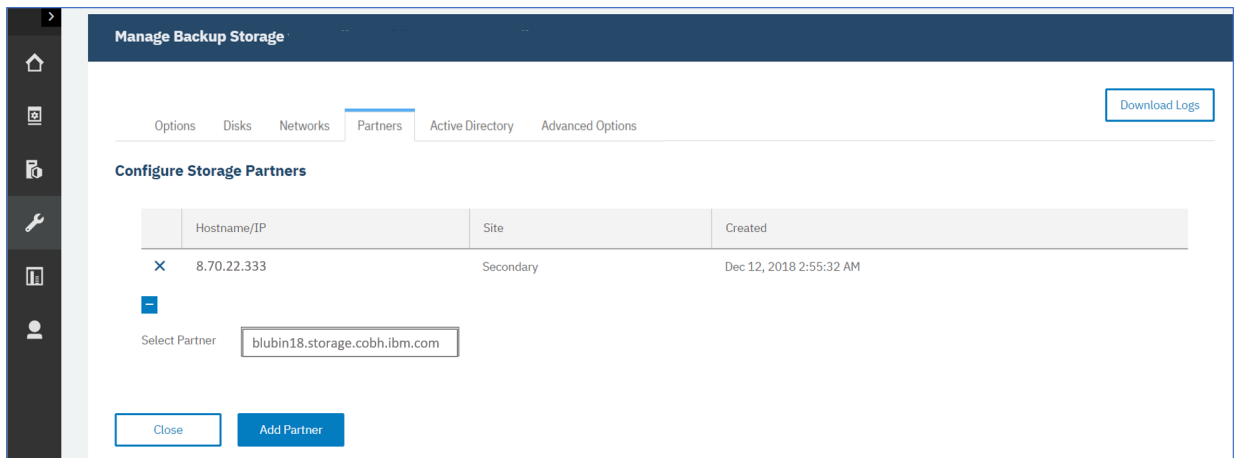
始める前に

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

ストレージ環境内のサーバーにパートナーを追加するには、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。
追加されている構成済みパートナーが表にリストされます。
2. 「パートナー」ペインで、ドロップダウン・メニューから 1 次バックアップ・ストレージ・ホストまたは 2 次バックアップ・ストレージ・ホストに追加するパートナーを選択します。



3. 「パートナーの追加」をクリックして、パートナーを追加し、ウィンドウを閉じます。

Active Directory の構成



1 次および 2 次のバックアップ・ストレージを Active Directory・ドメインと関連付けることができます。1 次または 2 次のホストがドメインに追加されると、そのホストに関連付けられているすべての Microsoft SQL Server ログ・バックアップ・ジョブが、ドメイン認証を使用してログ・バックアップ・ボリュームをマウントします。そのため、ログ・バックアップ操作の際に、アプリケーション・サーバー上のローカル・ステージング領域を使用する必要がなくなります。

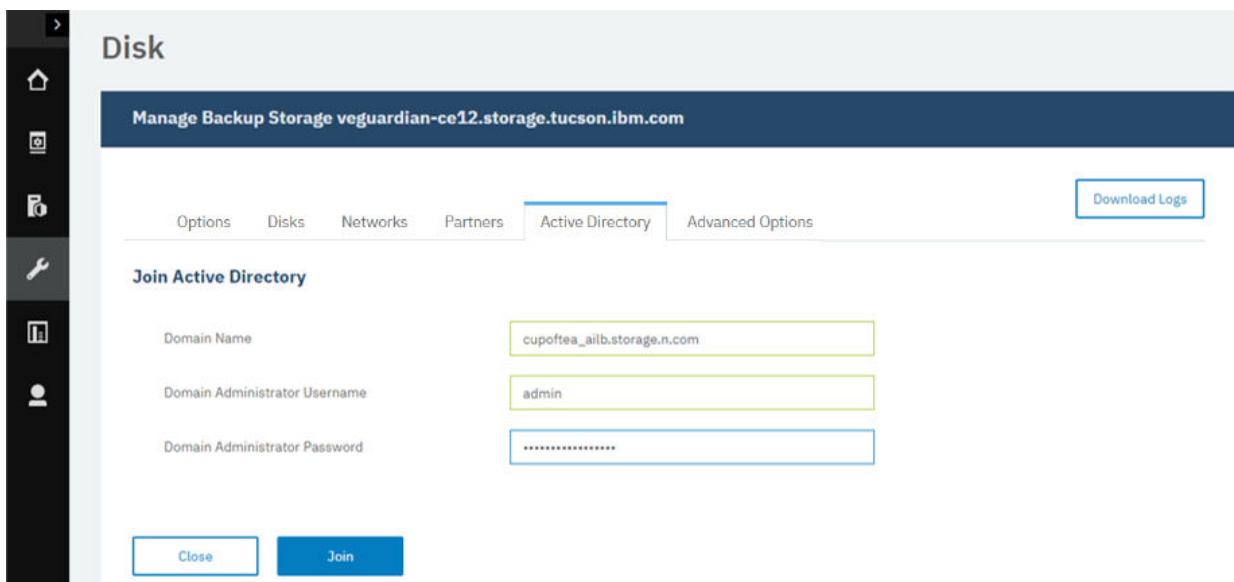
始める前に

ドメイン・コントローラーをネットワークで使用可能にし、1 次または 2 次のホストに関連付けられるように、ドメイン・ネーム・システム (DNS) サーバーを構成することが必要な場合があります。

手順

バックアップ操作およびリストア操作に Active Directory 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」、「バックアップ・ストレージ」>「ディスク」をクリックします。
2. 「Active Directory」タブで、編集する 1 次ホストまたは 2 次ホストに関連付けられている管理アイコンをクリックします。
3. 以下の図に示すように、Active Directory のドメイン名を、Active Directory 管理者のユーザー名とパスワードとともに入力します。





4. 「結合 (Join)」をクリックします。

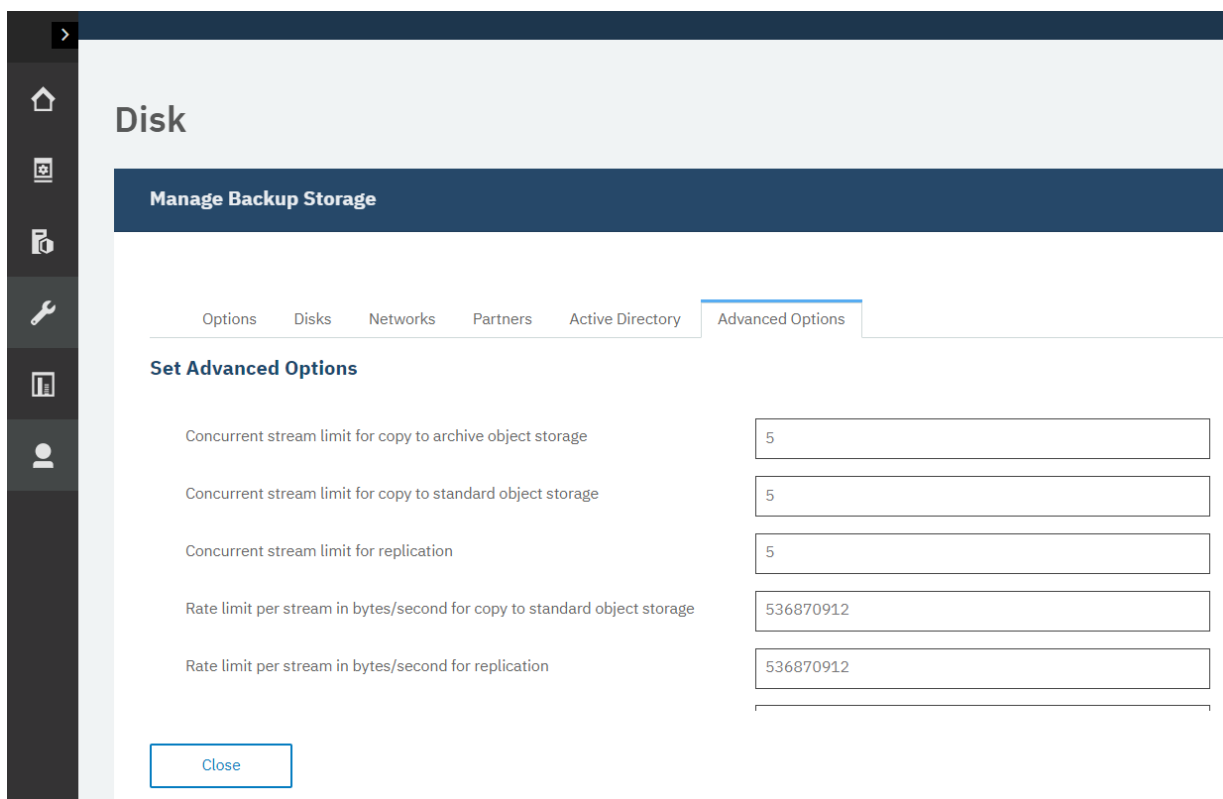
高度なストレージ・オプションの構成

ご使用の環境の1次バックアップ・ストレージまたは2次バックアップ・ストレージ用に、高度なストレージ関連オプションを設定できます。

手順

バックアップ・ストレージ用の高度なオプションを構成するには、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」、「バックアップ・ストレージ」>「ディスク」をクリックします。
2. 「バックアップ・ストレージの管理」ペインで、管理するホストに関連付けられている設定アイコンをクリックします。
3. 以下の例に示すように、「高度なオプション」タブで、拡張オプションを構成します。



The screenshot shows the 'Disk' configuration page with the 'Advanced Options' tab selected. The page title is 'Disk' and the subtitle is 'Manage Backup Storage'. The tabs are 'Options', 'Disks', 'Networks', 'Partners', 'Active Directory', and 'Advanced Options'. The 'Set Advanced Options' section contains the following settings:

Setting	Value
Concurrent stream limit for copy to archive object storage	5
Concurrent stream limit for copy to standard object storage	5
Concurrent stream limit for replication	5
Rate limit per stream in bytes/second for copy to standard object storage	536870912
Rate limit per stream in bytes/second for replication	536870912

A 'Close' button is located at the bottom left of the configuration area.

図 10. バックアップ・ストレージの高度なオプションを管理します。

- ・ **アーカイブ・オブジェクト・ストレージへのコピーの同時ストリームの制限 (Concurrent stream limit for copy to archive object storage):** この値は、データをアーカイブ・オブジェクト・ストレージにコピーするときに、このバックアップ・ホストによって使用される同時ストリームの最大数を定義します。
- ・ **標準オブジェクト・ストレージへのコピーの同時ストリームの制限 (Concurrent stream limit for copy to standard object storage):** この値は、データを標準オブジェクト・ストレージにコピーするときに、このバックアップ・ホストによって使用される同時ストリームの最大数を定義します。
- ・ **複製の同時ストリームの制限 (Concurrent stream limit for replication):** この値は、データを他のバックアップ・ホストに複製するときに、このバックアップ・ホストによって使用される同時ストリームの最大数を定義します。
- ・ **標準オブジェクト・ストレージへのコピーのストリーム当たりの速度の制限 (バイト/秒) (Rate limit per stream in bytes/second for copy to standard object storage):** この値は、標準のオブジェクト・ストレージにデータをコピーする際に、バックアップ・ホストが各データ・ストリームに使用する最大転送速度をバイト/秒単位で定義します。指定された値は、その他の制限要因がない場合の最大値で


す。各データ・ストリームの実際の速度は、この値より小さい場合が可能性があり、使用可能なシステム・リソース、ネットワーク条件、およびサイト・オプションで定義された帯域幅調整によって異なります。

- **複製のストリーム当たりの速度の制限 (バイト/秒) (Rate limit per stream in bytes/second for replication):** この値は、複製する際に、バックアップ・ホストが各データ・ストリームに使用する最大転送速度をバイト/秒単位で定義します。指定された値は、その他の制限要因がない場合の最大値です。各データ・ストリームの実際の速度は、この値より小さい場合が可能性があり、使用可能なシステム・リソース、ネットワーク条件、およびサイト・オプションで定義された帯域幅調整によって異なります。
- **AWS アーカイブ・オブジェクト・ストレージ (一括、標準、または迅速) からのリストアのための取り出し層 (Retrieval tier for restore from AWS archive object storage (Bulk, Standard, or Expedited)):** この値は、Amazon Glacier アーカイブ・オブジェクト・ストレージからのリストア操作時にこのバックアップ・ホストによって使用される取り出し層を指定します。この値は、「一括」、「標準」、または「迅速」に指定する必要があります。取り出し層を変更することで、より高いデータ料金と引き換えに、リストア操作時間を短縮できます。使用可能な取り出し層のオプションおよび関連する価格設定については、Amazon Web Services の資料を参照してください。
- **同時バックアップ:** このオプションは、複数のジョブが同時に実行される際の、ホストへの同時バックアップ・ストリームの最大数を指定します。アプリケーション・バックアップ操作の場合、各データベースは単一のストリームとして処理されます。ハイパーバイザー・バックアップ操作の場合、各仮想ディスクは単一のストリームとして処理されます。同時バックアップのオプションを使用すると、複数または多数の SLA ポリシーによって多すぎるデータ・ストリームが、負荷に対応できない小さなサイズのバックアップ・ホストへ送信されることを防ぐことができます。バックアップ操作の処理時間を短縮するために、このオプションを以下のいずれかに設定します。

無制限: 無制限の数の同時バックアップ・ストリームを実行できます。

一時停止: このバックアップ・ホストの使用を一時停止します。このバックアップ・ホストを使用しようとしているジョブは、この設定が選択されている間は停止しています。このオプションは、バックアップ・ホストが緊急時保守を必要とし、ジョブを一時的に使用できないようにする際に使用してください。

限度: 同時に実行できるバックアップ・ストリームの最大数に制限を設定します。同時ストリームの最大数を指定する数値を入力します。

ヒント: オプション値を変更した場合、次のオプション・フィールドをクリックすると新しい値が適用されます。更新されたオプションには、以下のメッセージが表示されます。  Updated。

4. 「クローズ」をクリックします。

vSnap ストレージ・プールの削除および再作成の方法

破損またはその他の理由により vSnap ストレージ・プールを削除する必要性が生じたシナリオでは、ストレージ・プールを削除して再作成するための手順を実行できます。この手順は、既存の vSnap ストレージ・プール内のすべてのデータを破棄する破壊操作です。プール内のすべてのバックアップ・データが失われ、リカバリーできなくなるため、続行する前に注意が必要です。これが行われた後、空の代替プールを作成できます。

手順

1. ストレージ・プールの除去の準備をするには、最初に、vSnap サーバーを除去して登録を抹消する必要があります。

vSnap サーバーの登録抹消について詳しくは、[110 ページの『vSnap サーバーの登録抹消』](#)を参照してください。

2. 「ジョブと操作」 > 「スケジュール」を開いて、vSnap サーバー上でメンテナンス・ジョブを実行しま

す。リストでメンテナンス・ジョブを見つけます。アクション・アイコン



をクリックし、「開始」をクリックします。

メンテナンス・ジョブが完了すると、vSnap サーバーに関するすべての情報が SPP カタログから削除されます。VM バックアップに関連付けられているすべてのリカバリー・ポイントとメタデータ、および登録が抹消された vSnap に保管されているすべてのレプリカ・コピーが削除されます。すべてのデータが削除され、リカバリーに使用できなくなります。

メンテナンス・ジョブについて詳しくは、479 ページの『[ジョブ・タイプ](#)』を参照してください。

3. vSnap サーバーで、以下のコマンドを実行して、クリーンアップされた vSnap サーバーを初期化します。

```
$ vsnap system init --skip_pool
```

システムがあらかじめ初期化されていた場合には、確実にこのコマンドを再実行できます。このステップにより、必要なカーネル・モジュールがインストールされ、ロードされることが確実にになります。

4. 以下のコマンドを実行して、既存のストレージ・プール ID を識別します。

```
$ vsnap pool show
```

ストレージ・プールがオンラインの場合、ID は *ID* フィールドに表示されます。ストレージ・プールがオフラインの場合は、プール情報を表示できないことを示すエラー・メッセージが表示されます。このエラー・メッセージには、プールの ID が表示されます。

5. ストレージ・プール ID に対して `delete` コマンドを実行して、ストレージ・プールを強制的に削除します。

```
$ vsnap pool delete --id <ID> --force
```

コマンドが完了すると、次のメッセージが表示されます。

```
Storage pool was deleted successfully but the pool was not unmounted because the 'force'
option was set.
Reboot the system to ensure disks that were previously in use are released.
```

6. システムを再始動して、まだ使用中のディスクを解放します。この場合、以下のコマンドを入力します。

```
$ sudo reboot -n
```

このコマンドを実行した後にシステムを再始動して、古いプールでまだ使用中のディスクが解放されるようにすることが重要です。

7. 再始動が終了したら、次の `status` コマンドを実行します。

```
$ vsnap_status
```

このコマンドの出力は、すべての vSnap サーバー・サービスの状況を示します。すべてのサービスがアクティブであることを確認してください。1 つ以上のサービスがアクティブ化中である場合、後ですべてがアクティブ状態になるまで状況を確認してください。

8. プールに追加する必要があるディスクを識別します。

古いプールを構成している同じディスク・セットを再使用する場合は、以下のコマンドがそれらのディスクの識別に役立ちます。

```
$ vsnap disk show
```

`show` コマンドの出力で、**USED AS** 列は、ディスク上に存在するのがファイル・システムか、区画テーブルかを示します。古いプールに含まれていたディスクは、`vsnap_pool` として識別されます。古いプールが暗号化されている場合は、一部またはすべてのディスクを `crypto_LUKS` として識別できません。

出力例

UUID							
KNAME	NAME		TYPE	VENDOR	MODEL	SIZE	USED AS

```
-----
6000c299371bdc647c80720602079bc | SCSI | VMware | Virtual disk | 70.00GB | LVM2_member |
sda | /dev/sda
6000c29b8ea25349e3a884d58f72e640 | SCSI | VMware | Virtual disk | 100.00GB | vsnap_pool |
sdb | /dev/sdb
6000c297cb8078cf9f56ab688a326a24 | SCSI | VMware | Virtual disk | 128.00GB | LVM2_member |
sdc | /dev/sdc
6000c2950248c5d831b6661ab0ec8843 | SCSI | VMware | Virtual disk | 16.00GB | vsnap_pool |
sdd | /dev/sdd
6000c29359661cbd915a7f24c8b44cf8 | SCSI | VMware | Virtual disk | 16.00GB | vsnap_pool |
sde | /dev/sde
```

9. **重要:** このステップのコマンドは、指定されたディスクから区画テーブルおよびファイル・システム・メタデータを削除し、それらに未使用のマークを付けます。このコマンドは注意して使用し、使用されなくなったディスクのみを指定するようにしてください。

次のコマンドを実行して、未使用としてマークされるディスク名のコンマ区切りリストを指定します。

```
$ vsnap disk wipe <disk_list>
```

次のコマンドは、disk wipe コマンドの一例です。\$ vsnap disk wipe /dev/sdb,/dev/sdd,/dev/sde

10. 次のコマンドを使用して新しいプールを作成します。

```
$ vsnap pool create --name <pool_name> <options> --disk_list <disk_list>
```

ここで、*pool_name* は新しいプールの名前です。*options* は RAID タイプまたは暗号化オプションを指定します。このオプションをブランクのままにすると、デフォルト・オプションが適用されます。*disk_list* は、プールに追加されるディスクのコンマ区切りリストを表します。**vsnap disk show** コマンドを実行する場合、指定するディスクの状況は **unused** でなければなりません。

次のコマンドは、create コマンドの一例です。

```
$ vsnap pool create --name primary --disk_list /dev/sdb,/dev/sdd
```

ディスクのリストを指定する場合は、メイン・データ・ディスクとして使用する予定のディスクのみを指定してください。キャッシュ・ディスクまたはログ・ディスクは、個別のコマンドを実行して後で追加できます。キャッシュ・ディスクおよびログ・ディスクを構成するための推奨事項および手順について詳しくは、[Blueprints](#) を参照してください。

ヒント:

ヘルプを開くには、vsnap pool create --help コマンドを実行してください。

11. プール情報を表示するには、次のコマンドを実行します。

```
$ vsnap pool show
```

コマンドに正しいプール情報が表示されていること、およびコマンドがエラーなしで完了することを確認してください。

12. 選択したサイトで IBM Spectrum Protect Plus に vSnap サーバーを登録して、セットアップを完了します。

vSnap サーバーの登録方法の詳細については、[109 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 vSnap サーバーの登録』](#)を参照してください。

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

初期化プロセス中に、vSnap は、物理インストール用にシステムに接続されている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。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。vSnap の仮想デプロイメントの場合、デフォルトで 100 GB の未使用仮想ディスクが定義され、プールを作成するために使用されます。

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、[125 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 コマンド・ライン・インターフェース (CLI) を使用できます。

IBM Spectrum Protect Plus にデプロイされ追加されているサーバーでは、IBM Spectrum Protect Plus 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 コマンド・ライン・インターフェース (CLI) 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インストールされたオンボード vSnap 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。IBM Spectrum Protect Plus に組み込まれているデモ・サイト内の vSnap サーバーは、テストおよびデモの目的でのみ使用する必要があります。実稼働環境でバックアップの宛先として使用することはできません。

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・アイコン  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

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の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. SSH を使用してユーザー ID `serveradmin` で vSnap サーバー・コンソールにログインします。仮想的にデプロイされる場合、初期パスワードは `sppDP758-SysXyz` 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#)でパスワード要件の規則を参照してください。物理的にデプロイされる場合、インストール時に `serveradmin` アカウント用に作成したパスワードを使用します。

`vsnap user create` コマンドを使用してあらかじめ作成された、vSnap 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、[123 ページの『vSnap サーバー管理の解説』](#)を参照してください。

2. **`--skip_pool`** オプションを指定した **`$ vsnap system init`** コマンドを発行し、ストレージ・プールの作成は行わずに vSnap サーバーを初期化します。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。次のコマンドを発行します。

```
$ vsnap system init --skip_pool
```

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	125 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・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。

始める前に

この手順の前に、仮想ディスクまたは物理ディスクを vSnap サーバーに追加する必要があります。既存のボリュームの拡張はサポートされていません。

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。

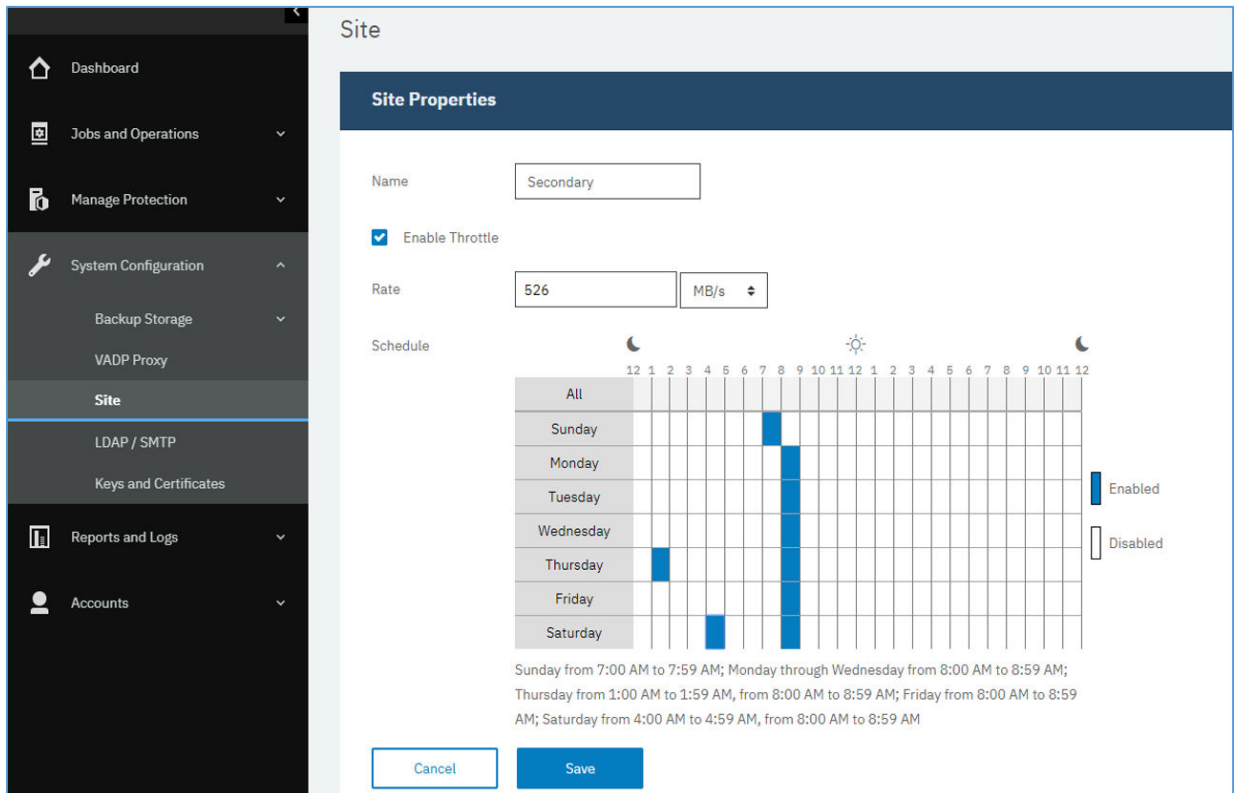
1. ナビゲーション・ペインで、「システム構成」 > 「バックアップ・ストレージ」 > 「ディスク」をクリックします。
2. 再スキャン対象の vSnap サーバーについて、「アクション」 > 「再スキャン」を選択します。
3. vSnap サーバーに関連付けられている管理アイコン  をクリックして、「バックアップ・ストレージに新規ディスクを追加」セクションを展開します。
4. 選択したディスクを追加して保存します。追加されたディスクのサイズだけ、vSnap プールが拡張されます。

スループット率の変更

サイト複製およびコピー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・アクティビティを管理できるようにします。

手順

- 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」ペインを開きます。
- 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。
- 「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。
- 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。



Site

Site Properties

Name: Secondary

☒ Enable Throttle

Rate: 526 MB/s

Schedule

	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
All																									
Sunday																									
Monday																									
Tuesday																									
Wednesday																									
Thursday																									
Friday																									
Saturday																									

Sunday from 7:00 AM to 7:59 AM; Monday through Wednesday from 8:00 AM to 8:59 AM; Thursday from 1:00 AM to 1:59 AM, from 8:00 AM to 8:59 AM; Friday from 8:00 AM to 8:59 AM; Saturday from 4:00 AM to 4:59 AM, from 8:00 AM to 8:59 AM

Cancel Save

図 11. 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

- 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。

- 「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。

障害が起きた vSnap サーバーの置き換え

IBM Spectrum Protect Plus 環境で、ターゲット vSnap サーバーとは、データをバックアップするための宛先です。vSnap サーバーが破損した場合、または応答できない場合は、vSnap サーバーを新規サーバーに置き換えて、保管されているデータをリカバリーすることができます。

始める前に

重要: 障害が起きたサーバーを IBM Spectrum Protect Plus から登録抹消しないでください。置き換え手順を正常に実行できるように、障害が起きたサーバーは登録されたままにする必要があります。

このプロセスを正常に完了するには、1 つ以上の初期化されたアクティブな vSnap レプリカ・サーバーが環境内に存在している必要があります。

このタスクについて

障害が起きた vSnap サーバーを置き換える手順は、[技術情報 1103847](#) の資料に記載されています。

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。

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 サーバーは、コマンド・ライン・インターフェースを使用して管理できます。コマンド・ライン・インターフェースは、vSnap サーバーを管理するための主な手段です。ユーザー ID `serveradmin` または vSnap 管理特権を割り当てられているその他のオペレーティング・システム・ユーザーを使用して SSH 経由で接続した後、vSnap サーバーのインターフェースから **vsnap** コマンドを実行します。初期の `serveradmin` パスワードは `sppDP758-SysXyz` 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#) でパスワード要件の規則を参照してください。

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。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、設定を編集します。

関連タスク

[109 ページの『vSnap サーバーの管理』](#)

バックアップ・ジョブとリストア・ジョブを有効にするには、IBM Spectrum Protect Plus に少なくとも 1 つの vSnap サーバーが必要です。vSnap サーバーは独自のアプライアンスであり、仮想的にデプロイされるか、最小要件を満たすシステム上に物理的にインストールされます。環境内の各 vSnap サーバーが認識されるには、IBM Spectrum Protect Plus に登録されなければなりません。IBM Spectrum Protect Plus に組み込まれているデモ・サイトに登録されている vSnap サーバーは、テストおよびデモの目的でのみ使用する必要があります。実稼働環境でバックアップの宛先として使用することはできません。

[116 ページの『高度なストレージ・オプションの構成』](#)

ご使用の環境の 1 次バックアップ・ストレージまたは 2 次バックアップ・ストレージ用に、高度なストレージ関連オプションを設定できます。

ユーザー管理

vsnap user コマンドを実行して、vSnap サーバー・サーバーを管理することができます。ユーザーの作成、ユーザー特権の付与と取り消し、ユーザーの照会、ユーザーのパスワードの更新に、このコマンドと使用可能なオプションが使用されます。

vSnap サーバーで作成されるユーザーは、vSnap オペレーティング・システム・グループに追加されるオペレーティング・システム・ユーザーです。vSnap オペレーティング・システム・グループのユーザーには、**sudo** 特権は割り当てられません。そのため、これらのユーザーには、コマンドを実行するためのパスワードが必要です。

create コマンドを実行して、vSnap ユーザーを作成することができます。この方法により、**vsnap** グループに割り当てられ、vSnap コマンドを実行でき、API 呼び出しを行うことができるオペレーティング・システム・ユーザーを作成します。次の **create** コマンドを実行します。

```
$ vsnap user create
```

対話式に実行する場合は、ユーザー名、パスワード、および確認のための 2 回目のパスワードの入力を求めるプロンプトが表示されます。非対話式に実行する場合は、**create** コマンドで以下のオプションを使用できます。

--username <username>

ユーザーのユーザー名を入力します。

--password <password>

ユーザーのパスワードを入力します。

ユーザーが vSnap コマンドを実行して API 呼び出しを行えるように、既存のオペレーティング・システム・アカウントに特権を付与することができます。特権を付与するには、**grant** コマンドを実行します。

```
$ vsnap user grant
```

対話式に実行する場合は、ユーザー名、パスワード、および確認のための 2 回目のパスワードの入力を求めるプロンプトが表示されます。非対話式に実行する場合は、**grant** コマンドで以下のオプションを使用できます。

--username <username>

ユーザーのユーザー名を入力します。

--password <password>

ユーザーのパスワードを入力します。アカウントがシステムに既に存在している場合は、オペレーティング・システム・アカウントのパスワードでなければなりません。

vsnap グループに割り当てられているユーザーの特権を取り消すことができます。そのユーザーは、オペレーティング・システム・ユーザーのままになりますが、vSnap コマンドを実行することも、API 呼び出しを行うこともできなくなります。特権を取り消すには、**revoke** コマンドを実行します。

```
$ vsnap user revoke
```

対話式に実行する場合は、ユーザー名の入力を求めるプロンプトが表示されます。非対話式に実行する場合は、**revoke** コマンドで以下のオプションを使用できます。

--username <username>

ユーザーのユーザー名を入力します。

vSnap サーバー上の **vsnap** グループに属している vSnap ユーザーのリストを表示するには、**show** コマンドを実行します。

```
$ vsnap user show
```

vSnap ユーザーは、アカウントのパスワードを変更できます。その場合、システムでそのユーザーのパスワードが更新されます。**update** コマンドを実行します。

```
$ vsnap user update
```

対話式に実行する場合は、ユーザー名、旧パスワード、新規パスワード、および確認のための 2 回目の新規パスワードの入力を求めるプロンプトが表示されます。非対話式に実行する場合は、**update** コマンドで以下のオプションを使用できます。

--username <username>

ユーザーのユーザー名を入力します。

--password <old_password>

ユーザーの旧パスワードを入力します。

--new_password <new_password>

ユーザーの新規パスワードを入力します。

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、バックアップ・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。



重要: ディスクは、ストレージ・プールに追加された後、削除することはできません。ディスクを削除すると、ストレージ・プールが破損します。

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、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。このディスクの処理と削除の方法については、**Blueprints** で詳細を参照してください。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。RAID 構成を使用して、シック・プロビジョンされた VMDK を使用する仮想 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

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 サーバーの外部の別の場所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、serveradmin ユーザーとして以下のコマンドを使用して、鍵を一時的な場所にコピーしてから、それらを vSnap ホストの外部の目的の安全なバックアップ・ロケーションにコピーします。

最初に、鍵がバックアップされるディレクトリーを作成します。

```
$ mkdir /tmp/keybackup-$(hostname)
```

次に、鍵ファイルを一時的な場所にコピーします。


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

最後に、ディレクトリー keybackup-<hostname> を vSnap ホストの外部にある安全なバックアップ・ロケーションにコピーします。ここで、<hostname> は、vSnap サーバーに割り当てられている名前です。

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・アイコン  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を示されます。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

120 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、126 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** オプションを渡します。

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クアップされているデータ・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、126 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、「ディスク」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。

vSnap サーバーのネットワークは、コマンド・ライン・インターフェース (CLI) で **network** コマンドを使用して変更できます。任意のコマンドの後で **--help** オプションを使用することで、追加情報を取得できます。

ネットワーク・インターフェース情報の表示

show コマンドを実行して、ネットワーク・インターフェースおよび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。

```
$ vsnap network show
```

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。

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。

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。

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。

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。

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

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。

```
$ vsnap network update
```

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、repl、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える場合、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。

カーネル・ヘッダーとカーネル・ツールのインストール

カーネル・ヘッダーおよびツールは、デフォルトではインストールされません。カスタム・ドライバー、モジュール、またはその他のソフトウェアをコンパイルして使用する予定の場合は、適切なカーネル・ヘッダーまたはカーネル・ツールを vSnap サーバーにインストールしてください。

このタスクについて

vSnap がインストールまたは更新されると、Linux カーネル・バージョン 4.19 がデフォルトでインストールされます。V4.19 へのカーネル・アップグレードをオプトアウトして、V3.10 に留まる場合は、vSnap サーバーと互換性のあるカーネル V3.10 がインストールされ、使用されます。どちらの場合も、そのカーネルに関連するカーネルのヘッダーとツールはインストールされません。カスタム・ドライバー、モジュール、またはその他のソフトウェアをコンパイルまたは使用する予定の場合は、カーネル・パッケージをインストールする必要があります。カーネルのヘッダーおよびツール用の Red Hat Package Manager (RPM) インストーラーは、vSnap インストール・ディレクトリーにあります。

手順

1. serveradmin ユーザーとして vSnap サーバーにログオンします。初期パスワードは sppDP758-SysXyz 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#) のパスワード要件の規則を参照してください。
2. Linux カーネル・バージョンを判別するには、コマンド・ラインを開き、以下のコマンドを発行します。

```
$ uname -r
```

出力が表示されます。ここで xxxx はカーネルの改訂番号を表します。

```
$ 4.19.xxxx
```

3. 以下のディレクトリーに移動します。

```
$ cd /opt/vsnap/config/pkgs/kernel/
```

4. ディレクトリーで、インストールされるパッケージである `xxxxxxxx.rpm` ファイルを見つけます。インストールされている Linux カーネル・バージョンに関して正しいパッケージが指定されていることを確認してください。カーネルのヘッダーまたはツールをインストールするには、次のコマンドを発行します。

```
$ sudo yum localinstall xxxxxxxx.rpm
```

タスクの結果

カーネルのヘッダーまたはツールがインストールされます。

vSnap サーバーのトラブルシューティング

IBM Spectrum Protect Plus 環境の vSnap サーバーは、バックアップ・プロセスと複製プロセスを通してデータを保護するためのディスク・ストレージを提供します。ご使用の環境で構成されている vSnap サーバーは、ターゲット、ソース、またはサーバーとターゲットの両方として使用される場合があります。障害を起こした vSnap サーバーの修復または交換を行うために、最初に、影響を受けた vSnap サーバーを機能する状態にして、バックアップと複製のサービスを再開できるようにするために従うべきステップがあります。これは、データの損失を最小限に抑えるためです。

vSnap パスワードと CIFS パスワードの同期化によるジョブ失敗の防止

vSnap サーバーと共通インターネット・ファイル・システム (CIFS) 共有の間の通信は、資格情報は共有されているものの、パスワードが同期されていない場合には中断される可能性があります。ジョブの失敗を防ぐには、vSnap パスワードと CIFS パスワードを同期化する必要があります。

このタスクについて

パスワードの同期化の方法については、[124 ページの『ユーザー管理』](#)を参照してください。

vSnap サーバーがまだオフラインになっているのはなぜですか？

vSnap サーバーを再始動した後、IBM Spectrum Protect Plus ユーザー・インターフェースには引き続きオフラインの状況が表示されます。

vSnap サーバーでデータ重複排除が有効になっているか、以前に有効になっていた場合、vSnap サーバーの始動プロセス中に重複排除テーブル (DDT) がメモリーにプリロードされます。DDT のプリロード・プロセスにより、vSnap サーバー・サービスの始動が 15 分遅れます。その間、vSnap サーバーで **Offline** の状況が表示されます。このプロセスが完了して、vSnap サーバーが **Online** 状況に戻るまで、少なくとも 15 分待ってください。vsnap_status コマンドを実行して、vSnap サーバー・サービスをモニターすることができます。

いずれかの vSnap サービスが activating 状態である場合は、vSnap サービスが開始中であることを意味します。すべてのサービスが active 状態になると、vSnap サーバーはオンラインに戻っています。

IBM Spectrum Protect Plus 環境で障害を起こした vSnap サーバーを修復できますか？

IBM Spectrum Protect Plus 環境で構成される vSnap サーバーは、バックアップ・プロセスと複製プロセスを通してデータを保護するためのディスク・ストレージを提供します。環境のいずれかの vSnap サーバーが障害を起こしたか、交換する必要がある場合は、修復するための手順を実行して、保管されているデータをリストアし、バックアップと複製のサービスが正常に提供されるようにする必要があります。

このタスクについて

重要：

注: 環境のすべての vSnap サーバーが複製によって保護されていることを想定しています。vSnap サーバーが複製されていない状態で失われた場合は、ソースまたはターゲットのディスク・ストレージとしての役割を果たし続けるための状態にリカバリーすることはできません。複製されていない場合は、新規の vSnap サーバーを作成して、SLA ポリシーをセットアップする必要があります。その際、新規のフルバックアップ・プロセスが実行されます。

vSnap サーバーは、環境で以下の役割を果たすことができます。

- バックアップ操作のソース・ディスク・ストレージとしての vSnap
- 別の vSnap サーバーからの複製操作のターゲット・ディスク・ストレージとしての vSnap
- バックアップと複製のサービスでソース とターゲット の両方の役割を果たす vSnap サーバー

修復操作は、通常の処理を続行できる状態に vSnap サーバーをリカバリーすることを目的としています。修復操作の結果は、修復している vSnap サーバーの役割に応じて異なります。

- ソース vSnap サーバーを修復する場合、修復操作では、ターゲット vSnap サーバーからのサイトのリカバリー・ポイントをリカバリーして、バックアップ操作で実動ワークロードからの差分変更の処理を続行できるようになるため、フルバックアップは必要ありません。この場合、ソース vSnap サーバーの最後のリカバリー・ポイントはリストアされませんが、ターゲット vSnap サーバーでのリカバリーと再利用に引き続き使用できることに注意してください。
- ターゲット vSnap サーバーを修復する場合、修復操作では、次の複製操作を正常に実行できるように、関係を再確立します。修復プロセスでは、データは転送されません。修復プロセスが完了した後、次のように処理が続行されます。
 - SLA スケジュール実行に従って、差分バックアップ・データがソース・ターゲット vSnap サーバーに送信されます。
 - SLA スケジュールに従って複製ジョブが開始され、修復プロセスの実行後にソース vSnap サーバーで作成されたすべてのリカバリー・ポイントが複製されます。この時点で、ソース vSnap サーバーからターゲット vSnap サーバーにデータが複製されます。これは、上記の最後のリカバリー・ポイントを表すために必要なすべてのデータのフルデータ転送として行われます。

vSnap サーバーの役割に応じて、下記のセクションの指示に従ってください。

手順

IBM Spectrum Protect Plus 環境で障害を起こした vSnap サーバーを修復するにはどうすればよいですか？

IBM Spectrum Protect Plus 環境の vSnap サーバーは、バックアップ・プロセスと複製プロセスを通してデータを保護するためのディスク・ストレージを提供します。IBM Spectrum Protect Plus 環境で構成されている、障害を起こした vSnap サーバーを、バックアップと複製のサービスのソース の役割を果たすように修復して交換することができます。バックアップと複製のサービスを再開できるようにするために、ソース vSnap サーバーを修復する必要があります。

始める前に

重要: 環境のすべての vSnap サーバーが複製によって保護されていることを想定しています。vSnap サーバーが複製されていない状態で障害を起こした場合は、ソースまたはターゲットのディスク・ストレージとしての役割を果たし続けられる状態にリカバリーすることはできません。複製プロセスが行われていない場合は、新規の vSnap サーバーを作成して、SLA ポリシーをセットアップする必要があります。ポリシーを実行すると、新規の vSnap サーバーに対して新規のフルバックアップ・プロセスが実行されます。

どのタイプの修復プロセスがご使用の vSnap サーバーに適用されるかを判断するには、[技術情報 1103847](#) を参照してください。

このタスクについて

重要: 障害を起こした vSnap サーバーを IBM Spectrum Protect Plus から登録抹消したり、削除したりしないでください。交換手順が正しく機能するためには、障害を起こした vSnap サーバーが登録されたままになっている必要があります。

この手順では、IBM Spectrum Protect Plus 環境で、障害を起こしたソース vSnap サーバーに取って代わる新規のソース vSnap サーバーを設定します。新規の vSnap サーバーには、最後のリカバリー・ポイントのみが含まれます。

注: 新規の vSnap サーバーのバージョンは、デプロイされている IBM Spectrum Protect Plus アプライアンスのバージョンと一致している必要があります。

手順

1. セキュア・シェル (SSH) プロトコルを使用して、ターゲット vSnap サーバーのコンソールに ID `serveradmin` でログインします。

次のコマンドを入力します。\$ `ssh serveradmin@MGMT_ADDRESS`

例: \$ `ssh serveradmin@10.10.10.2`

2. コマンド・プロンプトを開き、次のコマンドを入力して、障害を起こしたソース vSnap サーバーの ID を取得します。

\$ `vsnap partner show`

出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
API PORT: 8900
SSH PORT: 22
```

3. 「MGMT ADDRESS」が障害を起こしたソース vSnap サーバーのアドレスであることを確認します。障害を起こしたソース vSnap サーバーの ID 番号を書き留めます。
4. ソース vSnap サーバーが置かれている環境で、障害を起こしたソース vSnap サーバーと同じタイプとバージョンの新規の vSnap サーバーを同じストレージ割り振りでインストールします。

vSnap サーバーのインストール手順については、[物理 vSnap サーバーのインストール](#)を参照してください。

重要: 新規の vSnap サーバーを IBM Spectrum Protect Plus に登録しないでください。「ディスク・ストレージの追加」ウィザードを使用しないでください。

- a) 最初に、次のコマンドを使用して、vSnap サーバーを初期化する必要があります。

\$ `vsnap system init ----skip_pool id partner_id`

例: \$ `vsnap system init --skip_pool --id 12345678901234567890123456789012`
(障害を起こしたソース vSnap のパートナー ID を使用します)。初期化が完了すると、それを示すメッセージが表示されます。

注: このコマンドは、IBM Knowledge Center と Blueprints にリストされている vSnap 初期化コマンドとは異なります。

5. Blueprints の『Chapter 5: vSnap Server Installation and Setup』に概要が示されている vSnap サーバーとプールの作成プロセスを実行します。

6. 次のコマンドを入力して、新規のソース vSnap サーバーを保守モードにします。

```
$ vsnap system maintenance begin
```

vSnap サーバーを保守モードにすると、スナップショット作成、データ・リストア・ジョブ、複製操作などの操作が中断されます。

7. 障害を起こしたソース vSnap サーバーのパートナー ID を使用して新規のソース vSnap サーバーを初期化します。以下のコマンドを入力します。

```
$ vsnap system init --id partner_id
```

コマンドの例: `$ vsnap system init --id 12345678901234567890123456789012`

8. 新規のソース vSnap サーバーで、パートナー vSnap サーバーを追加します。各パートナーを個別に追加する必要があります。パートナーを追加するには、次のコマンドを入力します。

```
$ vsnap partner add --remote_addr remote_ip_address --local_addr local_ip_address
```

ここで、`remote_ip_address` にはソース vSnap サーバーの IP アドレスを指定し、`local_ip_address` には新規のソース vSnap サーバーの IP アドレスを指定します。

以下にコマンド例を示します。

```
$ vsnap partner add --remote_addr 10.10.10.2 --local_addr 10.10.10.1
```

9. プロンプトが表示されたら、ターゲット vSnap サーバーのユーザー ID とパスワードを入力します。パートナーの作成と更新が正常に行われると、それを示す通知メッセージが表示されます。

10. 次のコマンドを入力して、新規のソース vSnap サーバーで修復タスクを作成します。

```
$ vsnap repair create --async
```

このコマンドの出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDING
MESSAGE: The repair has been scheduled
```

11. 次のコマンドを入力して、修復操作に関与するボリュームの数をモニターします。

```
$ vsnap repair show
```

このコマンドの出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Created 0 volumes. There are 3 primary volumes that have recoverable snapshots,
the latest snapshot of each will be restored. Restoring 3 snapshots: 3 active, 0 pending, 0
completed, and 0 failed
```

修復操作に関与するボリュームの数は、「TOTAL VOLUMES」フィールドに示されます。

12. 新規のソース vSnap サーバーのディレクトリー /opt/vsnap/log/repair.log にある repair.log ファイルを表示して、修復タスクの状況をモニターします。あるいは、次のコマンドを入力することもできます。

```
$ vsnap repair show
```

このコマンドの出力は、上記の例のようになります。修復プロセス中に以下の状況メッセージが表示されることがあります。

- ・「STATUS: PENDING」は、修復ジョブがまもなく実行されることを示します。
- ・「STATUS: ACTIVE」は、修復ジョブがアクティブであることを示します。
- ・「STATUS: COMPLETED」は、修復ジョブが完了したことを示します。
- ・「STATUS: FAILED」は、修復ジョブが失敗したため、再実行依頼する必要があることを示します。

13. 修復操作中に、vSnap repair show コマンドを実行して、いつ状況が「COMPLETED」になるかを確認します。

```
$ vsnap repair session show
```

このコマンドの出力は、以下の例のようになります。

```
ID: 1 RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ACTIVE
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
Created 0 volumes.
There are 3 replica volumes whose snapshots will be restored on next replication.
```

修復操作に参与する各ボリュームのセッションが表示されます。

\$ vsnap repair session show コマンドを定期的に行って、各ボリュームについて送信されているデータの量が徐々に増えていることを確認します。セッションが終了すると、状況が「COMPLETED」に変わります。すべてのセッションが終了したら、\$ vsnap repair session show コマンドを実行して、全体の状況が「COMPLETED」であることを確認します。スナップショットがリストアされたボリュームの数を示す最終メッセージが表示されます。メッセージ出力は、以下の例のようになります。

```
Created 0 volumes.
There are 3 primary volumes that have recoverable snapshots, the latest snapshot of each
will be restored.
Restored 3 snapshots.
```

14. リストアされず、「FAILED」状況が示されているスナップショットがある場合は、次のコマンドを入力して、修復プロセスを再実行依頼します。

```
$ vsnap repair create --async --retry
```

15. 修復プロセスで「COMPLETED」状況が報告されたら、vSnap サーバーの保守モードを終了して通常の操作を再開することができます。通常の処理を再開するには、次のコマンドを入力します。

```
$ vsnap system maintenance complete
```

16. 保存した SSH ホスト鍵を、修復したソース vSnap サーバーとターゲット vSnap サーバーから削除します。

ソースとターゲットの両方の vSnap サーバーで次のコマンドを実行します。

```
$ sudo rm -f /home/vsnap/.ssh/known_hosts
```

```
$ sudo rm -f /root/.ssh/known_hosts
```

SSH 鍵を削除すると、後続の複製の転送で、修復された vSnap サーバーの変更されたホスト鍵に起因するエラーが発生しなくなります。

17. 次のコマンドを入力して、交換したサーバーで vSnap サービスを再開します。

```
$ sudo systemctl restart vsnap
```

18. 「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、次のように新規の vSnap サーバーが正しく登録されていることを確認します。

- 新規の vSnap サーバーで登録に同じホスト名または IP アドレスが使用されている場合は、変更は不要です。
- 新規の vSnap サーバーで登録に別のホスト名または IP アドレスが使用されている場合は、鉛筆アイコンを選択して登録を更新する必要があります。

19. ソース vSnap サーバーで使用できなくなったリカバリー・ポイントを削除するには、IBM Spectrum Protect Plus ユーザー・インターフェースからメンテナンス・ジョブを開始します。

手順については、[Creating jobs and job schedules](#) を参照してください。

ヒント： 次の例のような通知メッセージが表示されることがあります。

```
CTGGA1843 storage snapshot spp_1004_2102_2_16de41fc3 not found on live Storage2101  
Snapshot Type vsnap
```

20. vSnap サーバーが使用不可になった後で失敗したジョブを再開するには、ストレージ・サーバー・イベントリ・ジョブを実行します。手順については、[Creating jobs and job schedules](#) を参照してください。

タスクの結果

ソース vSnap サーバーが最後のリカバリー・ポイントのみで修復されました。SLA の一環として実行される次のバックアップ・ジョブによってデータが差分バックアップされます。リストア・ジョブを作成する場合、最後のリカバリー・ポイントのみをバックアップ・リポジトリで使用できます。その他のすべてのリカバリー・ポイントは、複製リポジトリと、ご使用の環境に該当する場合はオブジェクト・ストレージおよびアーカイブ・ストレージのリポジトリで使用できます。

IBM Spectrum Protect Plus 環境で障害を起こしたターゲット vSnap を修復するにはどうすればよいですか？

IBM Spectrum Protect Plus 環境の vSnap サーバーは、バックアップ・プロセスと複製プロセスを通してデータを保護するためのディスク・ストレージを提供します。IBM Spectrum Protect Plus 環境で構成されている、障害を起こした vSnap サーバーを、バックアップと複製のサービスのターゲットの役割を果たすように修復して交換することができます。バックアップと複製のサービスを再開できるようにするために、ソース vSnap サーバーを修復する必要があります。

始める前に

重要： 環境のすべての vSnap サーバーが複製によって保護されていることを想定しています。vSnap サーバーが複製されていない状態で障害を起こした場合は、ソースまたはターゲットのディスク・ストレージとしての役割を果たし続けられる状態にリカバリーすることはできません。複製プロセスが行われていない場合は、新規の vSnap サーバーを作成して、SLA ポリシーをセットアップする必要があります。ポリシーを実行すると、新規の vSnap サーバーに対して新規のフルバックアップ・プロセスが実行されます。

このタスクについて

重要： 障害を起こした vSnap サーバーを IBM Spectrum Protect Plus から登録抹消したり、削除したりしないでください。交換手順が正しく機能するためには、障害を起こした vSnap サーバーが登録されたままになっている必要があります。

この手順では、IBM Spectrum Protect Plus 環境で、障害を起こしたターゲット vSnap サーバーに取って代わる新規のターゲット vSnap サーバーを設定します。新規のターゲット vSnap サーバーには、データがまったく格納されていませんが、スケジュールされている次の複製操作時に最後のリカバリー・ポイントが取り込まれます。

注: 新規の vSnap サーバーのバージョンは、デプロイされている IBM Spectrum Protect Plus アプライアンスのバージョンと一致している必要があります。

どのタイプの修復プロセスがご使用の vSnap サーバーに適用されるかを判断するには、[技術情報 1103847](#) を参照してください。

手順

1. セキュア・シェル (SSH) プロトコルを使用して、機能している vSnap サーバーのコンソールに ID serveradmin でログインします。

次のコマンドを入力します。\$ ssh serveradmin@MGMT_ADDRESS

例: \$ ssh serveradmin@10.10.10.1

2. コマンド・プロンプトを開き、次のコマンドを入力して、障害を起こした vSnap サーバーの ID を取得します。

```
$ vsnap partner show
```

出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.2
API PORT: 8900
SSH PORT: 22
```

3. 「MGMT ADDRESS」が障害を起こした vSnap サーバーのアドレスであることを確認します。障害を起こした vSnap サーバーの ID 番号を書き留めます。
4. ターゲット vSnap サーバーが置かれている環境で、障害を起こしたターゲット vSnap サーバーと同じタイプとバージョンの新規の vSnap サーバーを同じストレージ割り振りでインストールします。

vSnap サーバーのインストール手順については、[物理 vSnap サーバーのインストール](#)を参照してください。

重要: 新規の vSnap サーバーを IBM Spectrum Protect Plus に登録しないでください。「ディスク・ストレージの追加」ウィザードを使用しないでください。

- a) 最初に、次のコマンドを使用して、vSnap サーバーを初期化する必要があります。

```
$ vsnap system init --skip_pool --id <partner_id>
```

例: \$ vsnap system init --skip_pool --id 12345678901234567890123456789012 (障害を起こしたソース vSnap のパートナー ID を使用します)。初期化が完了すると、それを示すメッセージが表示されます。

注: このコマンドは、IBM Knowledge Center と Blueprints にリストされている vSnap 初期化コマンドとは異なります。

5. Blueprints の『*Chapter 5: vSnap Server Installation and Setup*』に概要が示されている vSnap サーバーとプールの作成プロセスを実行します。
6. 次のコマンドを入力して、新規の vSnap サーバーを保守モードにします。

```
$ vsnap system maintenance begin
```

vSnap サーバーを保守モードにすると、スナップショット作成、データ・リストア・ジョブ、複製操作などの操作が中断されます。

7. 障害を起こしたターゲット vSnap サーバーのパートナー ID を使用して新規のターゲット vSnap サーバーを初期化します。以下のコマンドを入力します。

```
$ vsnap system init --id <partner_id>
```

以下にコマンド例を示します。

```
$ vsnap system init --id 12345678901234567890123456789012
```

8. 新規のターゲット vSnap サーバーで、パートナー vSnap サーバーを追加します。各パートナーを個別に追加する必要があります。パートナーを追加するには、次のコマンドを入力します。

```
$ vsnap partner add --remote_addr <remote_ip_address> --local_addr <local_ip_address>
```

ここで、<remote_ip_address> にはソース vSnap サーバーの IP アドレスを指定し、<local_ip_address> には新規のターゲット vSnap サーバーの IP アドレスを指定します。

以下にコマンド例を示します。

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

9. プロンプトが表示されたら、ソース vSnap サーバーのユーザー ID とパスワードを入力します。パートナーの作成と更新が正常に行われると、それを示す通知メッセージが表示されます。
10. 次のコマンドを入力して、新規のソース vSnap サーバーで修復タスクを作成します。

```
$ vsnap repair create --async
```

このコマンドの出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: N/A
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: PENDING
MESSAGE: The repair has been scheduled
```

11. 次のコマンドを入力して、複製操作に参与するボリュームの数をモニターします。

```
$ vsnap repair show
```

このコマンドの出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
PARTNER ID: abcdef7890abcdef7890abcdef7890ab
TOTAL VOLUMES: 3
SNAPSHOTS RESTORED: N/A
RETRY: No
CREATED: 2019-11-01 15:49:31 UTC
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Creating 3 volumes for partner 670d61a10f78456bb895b87c45e20999
```

複製操作に参与するボリュームの数は、「TOTAL VOLUMES」フィールドに示されます。

12. 新規のソース vSnap サーバーのディレクトリー /opt/vsnap/log/repair.log にある repair.log ファイルを表示して、修復タスクの状況をモニターします。あるいは、次のコマンドを入力することもできます。

```
$ vsnap repair show
```

このコマンドの出力は、上記の例のようになります。修復プロセス中に以下の状況メッセージが表示されることがあります。

- ・「STATUS: PENDING」は、修復ジョブがまもなく実行されることを示します。
- ・「STATUS: ACTIVE」は、修復ジョブがアクティブであることを示します。
- ・「STATUS: COMPLETED」は、修復ジョブが完了したことを示します。
- ・「STATUS: FAILED」は、修復ジョブが失敗したため、再実行依頼する必要があることを示します。

13. 修復操作中に、vSnap repair show コマンドを実行して、いつ状況が「COMPLETED」になるかを確認します。

```
$ vsnap repair session show
```

次のように、最終メッセージに、スナップショットが次回の複製でリストアされるボリュームの数が示されます。

```
Created 0 volumes.  
There are 3 replica volumes whose snapshots will be restored on next replication.
```

14. リストアされず、「FAILED」状況が示されているスナップショットがある場合は、次のコマンドを入力して、修復プロセスを再実行依頼します。

```
$ vsnap repair create --async --retry
```

15. 修復プロセスで「COMPLETED」状況が報告されたら、vSnap サーバーの保守モードを終了して通常の操作を再開することができます。通常の処理を再開するには、次のコマンドを入力します。

```
$ vsnap system maintenance complete
```

16. 保存した SSH ホスト鍵を、修復したソース vSnap サーバーとターゲット vSnap サーバーから削除します。

ソースとターゲットの両方の vSnap サーバーで次のコマンドを実行します。

```
$ sudo rm -f /home/vsnap/.ssh/<known_hosts>
```

```
$ sudo rm -f /root/.ssh/<known_hosts>
```

SSH 鍵を削除すると、後続の複製の転送で、修復された vSnap サーバーの変更されたホスト鍵に起因するエラーが発生しなくなります。

17. 次のコマンドを入力して、交換したサーバーで vSnap サービスを再開します。

```
$ sudo systemctl restart vsnap
```

18. 「システム構成」 > 「バックアップ・ストレージ」 > 「ディスク」を起こしたターゲットクリックして、次のように新規の vSnap が正しく登録されていることを確認します。

- 新規の vSnap サーバーで登録に同じホスト名または IP アドレスが使用されている場合は、変更は不要です。
- 新規の vSnap サーバーで登録に別のホスト名または IP アドレスが使用されている場合は、鉛筆アイコンを選択して登録を更新する必要があります。

19. ソース vSnap サーバーで使用できなくなったリカバリー・ポイントを削除するには、IBM Spectrum Protect Plus ユーザー・インターフェースからメンテナンス・ジョブを開始します。

ヒント：次の例のような通知メッセージが表示されることがあります。

```
CTGGA1843 storage snapshot spp_1004_2102_2_16de41fcbc3 not found on live Storage2101  
Snapshot Type vsnap
```

20. vSnap サーバーが使用不可になった後で失敗したジョブを再開するには、ストレージ・サーバー・インベントリー・ジョブを実行します。

タスクの結果

ターゲット vSnap サーバーが修復されました。新規のターゲット vSnap サーバーで後続のアクションを実行する前に、ソース vSnap サーバーで新規のバックアップ・ジョブを実行する必要があります。

新規ターゲット vSnap サーバーで複製ジョブが試行された場合は、以下のようなメッセージが表示されます。

```
CTGGA0289 - Skipping volume <volume_id> because there are no new snapshots since last backup
```

ソース vSnap サーバーで新規のバックアップ・ジョブが実行された後、スケジュールされている次の複製ジョブにより、バックアップ・ジョブによって作成されたリカバリー・ポイントが複製されます。この時点では、リストア・ジョブを作成する場合、最後のリカバリー・ポイントのみを複製リポジトリで使用できます。ターゲット vSnap サーバーがオブジェクトまたはアーカイブ・ストレージに対するコピー・ソースとしても機能していた場合は、後続のコピー操作を正常に実行できるように、その前にまず、ターゲット vSnap サーバーで複製ジョブを実行する必要があります。オブジェクト・ストレージへのデータの最初のコピーは、フルコピーになります。

IBM Spectrum Protect Plus 環境で障害を起こした二重役割の vSnap サーバーを修復するにはどうすればよいですか？

IBM Spectrum Protect Plus 環境で構成されている、障害を起こした vSnap サーバー、バックアップと複製のサービスのソース とターゲット の両方の役割を果たすように修復して交換することができます。

このタスクについて

重要: 障害を起こした vSnap サーバーを IBM Spectrum Protect Plus から登録抹消したり、削除したりしないでください。交換手順が正しく機能するためには、障害を起こした vSnap サーバーが登録されたままになっている必要があります。

この手順では、IBM Spectrum Protect Plus 環境で、障害を起こした vSnap サーバーに取って代わる新規の vSnap サーバーを設定します。修復プロセスが完了すると、新規の vSnap サーバーは、バックアップ・ジョブで差分変更のバックアップを続行でき (フルバックアップは不要)、複製ジョブを続行できるポイントにリカバリーされます。

どのタイプの修復プロセスがご使用の vSnap サーバーに適用されるかを判断するには、[技術情報 1103847](#) を参照してください。

注: 新規の vSnap サーバーのバージョンは、デプロイされている IBM Spectrum Protect Plus アプライアンスのバージョンと一致している必要があります。

手順

1. セキュア・シェル (SSH) プロトコルを使用して、環境で機能している vSnap サーバーのコンソールに ID serveradmin でログインします。

次のコマンドを入力します。\$ ssh serveradmin@MGMT_ADDRESS

例: \$ ssh serveradmin@10.10.10.2

2. コマンド・プロンプトを開き、次のコマンドを入力して、障害を起こした vSnap サーバーの ID を取得します。

\$ vsnap partner show

出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012
PARTNER TYPE: vsnap
MGMT ADDRESS: 10.10.10.1
API PORT: 8900
SSH PORT: 22
```

3. 「MGMT ADDRESS」が障害を起こした vSnap サーバーのアドレスであることを確認します。障害を起こした vSnap サーバーの ID 番号を書き留めます。
4. ターゲット vSnap サーバーで、障害を起こしたソース vSnap サーバーと同じタイプとバージョンの新規の vSnap サーバーを同じストレージ割り振りでインストールします。

vSnap サーバーのインストール手順については、[物理 vSnap サーバーのインストール](#)を参照してください。

重要: 新規の vSnap サーバーを IBM Spectrum Protect Plus に登録しないでください。「ディスク・ストレージの追加」ウィザードを使用しないでください。

- a) 最初に、次のコマンドを使用して、vSnap サーバーを初期化する必要があります。


```
$ vsnap system init ----skip_pool id partner_id
```

例: \$ vsnap system init --skip_pool --id 12345678901234567890123456789012
(障害を起こしたソース vSnap のパートナー ID を使用します)。初期化が完了すると、それを示すメッセージが表示されます。

注: このコマンドは、IBM Knowledge Center と Blueprints にリストされている vSnap 初期化コマンドとは異なります。

5. [Blueprints](#) の『*Chapter 5: vSnap Server Installation and Setup*』に概要が示されている vSnap サーバーとプールの作成プロセスを実行します。

6. 次のコマンドを入力して、新規の vSnap サーバーを保守モードにします。

```
$ vsnap system maintenance begin
```

vSnap サーバーを保守モードにすると、スナップショット作成、データ・リストア・ジョブ、複製操作などの操作が中断されます。

7. 障害を起こしたターゲット vSnap サーバーのパートナー ID を使用して新規のターゲット vSnap サーバーを初期化します。次のコマンドを入力して、vSnap を初期化します。

```
$ vsnap system init --id partner_id
```

コマンドの例: \$ vsnap system init--id 12345678901234567890123456789012

8. 新規のターゲット vSnap サーバーで、パートナー vSnap サーバーを追加します。複数のパートナー・サーバーがある場合は、各パートナーを個別に追加する必要があります。パートナーを追加するには、次のコマンドを入力します。

```
$ vsnap partner add --remote_addr remote_ip_address --local_addr  
local_ip_address
```

ここで、remote_ip_address にはソース vSnap サーバーの IP アドレスを指定し、local_ip_address には新規のターゲット vSnap サーバーの IP アドレスを指定します。

以下にコマンド例を示します。

```
$ vsnap partner add --remote_addr 10.10.10.1 --local_addr 10.10.10.2
```

9. プロンプトが表示されたら、ソース vSnap サーバーのユーザー ID とパスワードを入力します。パートナーの作成と更新が正常に行われると、それを示す通知メッセージが表示されます。

10. 次のコマンドを入力して、新規のソース vSnap サーバーで修復タスクを作成します。

```
$ vsnap repair create --async
```

このコマンドの出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012  
PARTNER TYPE: vsnap  
PARTNER ID: abcdef7890abcdef7890abcdef7890ab  
TOTAL VOLUMES: N/A  
SNAPSHOTS RESTORED: N/A  
RETRY: No  
CREATED: 2019-11-01 15:49:31 UTC  
UPDATED: 2019-11-01 15:49:31 UTC  
ENDED: N/A  
STATUS: PENDING  
MESSAGE: The repair has been scheduled
```

11. 次のコマンドを入力して、複製操作に関与するボリュームの数をモニターします。

```
$ vsnap repair show
```

このコマンドの出力は、以下の例のようになります。

```
ID: 12345678901234567890123456789012  
PARTNER TYPE: vsnap  
PARTNER ID: abcdef7890abcdef7890abcdef7890ab  
TOTAL VOLUMES: 6  
SNAPSHOTS RESTORED: N/A  
RETRY: No  
CREATED: 2019-11-01 15:49:31 UTC
```

```
UPDATED: 2019-11-01 15:49:31 UTC
ENDED: N/A
STATUS: ACTIVE
MESSAGE: Created 0 volumes
There are 3 replica volumes whose snapshots will be restored on next replication.
There are 3 primary volumes that have recoverable snapshots, the latest snapshot of each
will be restored.
The number of volumes that are involved in the repair operation are indicated in the TOTAL
VOLUMES field
```

12. 新規のソース vSnap サーバーのディレクトリー /opt/vsnap/log/repair.log にある repair.log ファイルを表示して、修復タスクの状況をモニターします。あるいは、次のコマンドを入力することもできます。

```
$ vsnap repair show
```

13. 修復操作の状況が「ACTIVE」状態である場合、次のコマンドを入力して、個々の修復セッションの状況を表示することができます。

```
$ vsnap repair session show
```

出力は、以下の例のようになります。

```
ID: 1
RELATIONSHIP: 72b19f6a9116a46aae6c642566906b31
PARTNER TYPE: vsnap
LOCAL SNAP: 1313
REMOTE SNAP: 311
STATUS: ACTIVE
SENT: 102.15GB
STARTED: 2019-11-01 15:51:18 UTC
ENDED: N/A
```

修復操作の各ソース・ボリュームのセッションを表示します。プロセスが完了するまで、ボリュームごとに送信されるデータの量として示される値は徐々に増えます。次の例のように、最終メッセージに、スナップショットが次の複製操作でリストアされるボリュームの数が示されます。

```
Created 0 volumes. There are 3 replica volumes whose snapshots will be restored on next
replication.
```

14. リストアされず、「FAILED」状況が示されているスナップショットがある場合は、次のコマンドを入力して、修復プロセスを再実行依頼します。

```
$ vsnap repair create --async --retry
```

15. 修復プロセスで「COMPLETED」状況が報告されたら、vSnap サーバーの保守モードを終了して通常の操作を再開することができます。通常の処理を再開するには、次のコマンドを入力します。

```
$ vsnap system maintenance complete
```

16. オプション: 修復操作中にリストアされた合計ボリューム数とスナップショットの数を表示するには、vSnap サーバーに対して show コマンドを実行します。

出力には、以下の情報が含まれています。

- ・「Total volumes」には、修復操作中に検査されたボリュームの総数がリストされます。このリストには、最後のリカバリー・ポイントのバックアップがリストアされたソース・ボリューム (1 次ボリューム) と、SLA でスケジュールされている次の複製操作時に再び取り込まれるターゲット・ボリューム (レプリカ・ボリューム) が示されます。
- ・「SNAPSHOTS RESTORED」には、リストアされたソース・ボリュームの数がリストされます。

17. 保存した SSH ホスト鍵を、修復したソース vSnap サーバーとターゲット vSnap サーバーから削除します。

ソースとターゲットの両方の vSnap サーバーで次のコマンドを実行します。

```
$ sudo rm -f /home/vsnap/.ssh/known_hosts
```

```
$ sudo rm -f /root/.ssh/known_hosts
```

SSH 鍵を削除すると、後続の複製の転送で、修復された vSnap サーバーの変更されたホスト鍵に起因するエラーが発生しなくなります。

18. 次のコマンドを入力して、交換したサーバーで vSnap サービスを再開します。

```
$ sudo systemctl restart vsnap
```

19. 「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、次のように新規の vSnap サーバーが正しく登録されていることを確認します。

- 新規の vSnap サーバーで登録に同じホスト名または IP アドレスが使用されている場合は、変更は不要です。
- 新規の vSnap サーバーで登録に別のホスト名または IP アドレスが使用されている場合は、鉛筆アイコンを選択して登録を更新する必要があります。

20. ソース vSnap サーバーで使用できなくなったリカバリー・ポイントを削除するには、IBM Spectrum Protect Plus ユーザー・インターフェースからメンテナンス・ジョブを開始します。

そのためには、[Creating jobs and job schedules](#) の手順に従ってください。

ヒント：次の例のような通知メッセージが表示されることがあります。

```
CTGGA1843 storage snapshot spp_1005_2102_2_16de41fc3 not found on live Storage2101  
Snapshot Type vsnap
```

21. vSnap サーバーが使用不可になった後で失敗したジョブを再開するには、ストレージ・サーバー・インベントリー・ジョブを実行します。手順については、[Creating jobs and job schedules](#) を参照してください。

タスクの結果

修復された vSnap サーバーに保管されている 1 次バックアップ・データでは、1 次バックアップ・データの最後のリカバリー・ポイントを使用できるようになります。修復された vSnap サーバーへの後続のバックアップでは、引き続き、最後のバックアップ以降の差分変更のみが送信されます。修復された vSnap サーバーに保管されている複製データについては、修復直後に使用できる複製データはありません。パートナー vSnap サーバーからの後続の複製ジョブにより、修復プロセスの完了後にパートナー vSnap サーバーで作成されたバックアップが再び取り込まれます。パートナー vSnap サーバーでバックアップが完了する前にパートナー vSnap サーバーで複製ジョブが試行された場合は、最後のバックアップ以降の新規スナップショットがないことを示す警告メッセージが表示されます。

```
CTGGA0289 - Skipping volume <volume_id> because there are no new snapshots since last backup
```

修復された vSnap サーバーがオブジェクトまたはアーカイブ・ストレージに対するコピー・ソースとして機能していた場合は、後続のコピー操作を正常に実行できるように、その前にまず、修復された vSnap サーバーでバックアップ・ジョブを実行する必要があります。オブジェクト・ストレージへのデータの最初のコピーは、フルコピーになります。

第 5 章 Kubernetes Backup Support のインストール

コンテナ内の永続ボリュームを保護するには、バックアップ管理者が Kubernetes 環境で Kubernetes Backup Support をインストールして構成する必要があります。

Kubernetes Backup Support の前提条件

Kubernetes Backup Support をインストールする前に、すべてのシステム要件および前提条件が満たされていることを確認してください。

Kubernetes Backup Support のシステム要件については、[51 ページの『Kubernetes Backup Support の要件』](#)を参照してください。

次に、Kubernetes Backup Support の前提条件を満たすために、Kubernetes 環境で以下のアクションを実行します。

- [143 ページの『VolumeSnapshotDataSource フィーチャーの有効化』](#)
- [144 ページの『Metrics Server が稼働していることの確認』](#)
- [145 ページの『アプリケーションと Persistent Volume Claim の関係の定義』](#)
- [145 ページの『外部レジストリーで使用するイメージ・プル・シークレットの作成』](#)

VolumeSnapshotDataSource フィーチャーの有効化

Kubernetes 1.16 のみ: コピー・バックアップおよびスナップショットのリストア 操作をサポートするために、**VolumeSnapshotDataSource** のアルファ版のフィーチャーを有効にする必要があります。

アルファ版のフィーチャーについて詳しくは、[Feature Gates](#) を参照してください。

VolumeSnapshotDataSource のアルファ版のフィーチャーを有効にするには、次のようにして、Kubernetes のスケジューラー、コントローラー、および API サーバーにパッチを適用する必要があります。

1. **sudo** コマンドを使用して、以下の YAML ファイルを編集します。

```
/etc/kubernetes/manifests/kube-apiserver.yaml
/etc/kubernetes/manifests/kube-controller-manager.yaml
/etc/kubernetes/manifests/kube-scheduler.yaml
```

2. 各 YAML ファイルで、コマンド・セクション内に次のステートメントを追加します。

```
- --feature-gates=VolumeSnapshotDataSource=true
```

重要: 必ず、YAML ファイルを直接編集してください。これらのファイルのバックアップ・コピーを同じディレクトリーに作成しないでください。/etc/kubernetes/manifests ディレクトリーにバックアップ・コピーが存在していると、**VolumeSnapshotDataSource** フィーチャー・ゲートを有効にするために行った変更が無効になる可能性があります。

変更が Kubernetes によって検出されるまで 1 分から 2 分待たなければならない場合があります。

3. 以下のコマンドを実行して、フィーチャーが有効になっているか確認します。

```
ps aux | grep apiserver | grep feature-gates
```

```
ps aux | grep scheduler | grep feature-gates
```

```
ps aux | grep controller-manager | grep feature-gates
```

上記のコマンドの 1 つの出力は、次の例のようになります。

```

root      13121  7.4  2.5 518276 305424 ?          Ssl  Sep06 120:37 kube-apiserver --
authorization-mode=Node,RBAC --advertise-address=192.0.2.0
--allow-privileged=true --client-ca-file=/etc/kubernetes/pki/ca.crt --enable-admission-
plugins=NodeRestriction --enable-bootstrap-token-auth=true
--etcd-cafile=/etc/kubernetes/pki/etcd/ca.crt --etcd-certfile=/etc/kubernetes/pki/apiserver-
etcd-client.crt --etcd-keyfile=/etc/kubernetes/pki/apiserver-etcd-client.key
--etcd-servers=https://127.0.0.1:2379 --insecure-port=0 --kubectl-client-certificate=/etc/
kubernetes/pki/apiserver-kubectl-client.crt
--kubectl-client-key=/etc/kubernetes/pki/apiserver-kubectl-client.key --kubectl-preferred-
address-types=InternalIP,ExternalIP,Hostname
--proxy-client-cert-file=/etc/kubernetes/pki/front-proxy-client.crt --proxy-client-key-
file=/etc/kubernetes/pki/front-proxy-client.key
--requestheader-allowed-names=front-proxy-client --requestheader-client-ca-file=/etc/
kubernetes/pki/front-proxy-ca.crt
--requestheader-extra-headers-prefix=X-Remote-Extra- --requestheader-group-headers=X-Remote-
Group --requestheader-username-headers=X-Remote-User
--secure-port=6443 --service-account-key-file=/etc/kubernetes/pki/sa.pub --service-cluster-
ip-range=198.51.100.0/24 --tls-cert-file=/etc/kubernetes/pki/apiserver.crt
--tls-private-key-file=/etc/kubernetes/pki/apiserver.key --feature-
gates=VolumeSnapshotDataSource=true

```

Metrics Server が稼働していることの確認

オプション: 製品のパフォーマンスとスケーラビリティを最適化するには、Kubernetes Metrics Server v0.3.5 以降がクラスターで適切にインストールおよび実行されていることを確認してください。Metrics Server は、Kubernetes Backup Support スケジューラーによって、同時データ・ムーバー・インスタンスで使用されているリソースを判別するために使用されます。

Metrics Server がデータを返さない場合、バックアップ操作に使用されるデータ・ムーバーの数が制限され、そのためにパフォーマンスに悪影響を及ぼす可能性があります。

Metrics Server をデプロイする手順については、<https://github.com/kubernetes-sigs/metrics-server> の README.md ファイルを確認してください。Kubernetes Metrics Server については、[Resource metrics pipeline](#) を参照してください。

以下のステップを実行して、Metrics Server がインストールされていて、メトリックを返していることを確認できます。

1. 次のコマンドを実行して、インストールを確認します。

```
kubectl get deploy,svc -n kube-system | egrep metrics-server
```

出力は、以下の例のようになります。

```

deployment.extensions/metrics-server 1/1      1      1      3d4h
service/metrics-server ClusterIP 198.51.100.0 <none> 443/TCP 3d4h

```

2. 次のコマンドを実行して、Metrics Server がすべてのノードのデータを返していることを確認します。

```
kubectl get --raw "/apis/metrics.k8s.io/v1beta1/nodes"
```

出力は、以下の例のようになります。

```

{"kind": "NodeMetricsList", "apiVersion": "metrics.k8s.io/v1beta1", "metadata": {"selfLink": "/
apis/metrics.k8s.io/v1beta1/nodes"}, "items": [{"metadata":
{"name": "cirrus12", "selfLink": "/apis/metrics.k8s.io/v1beta1/nodes/cirrus12",
"creationTimestamp": "2019-08-08T23:59:49Z"}, "timestamp": "2019-08-08T23:59:08Z",
"window": "30s", "usage": {"cpu": "1738876098n", "memory": "8406880Ki"}}]}

```

ヒント: コマンドが失敗して、「items」キーの空の出力を返す可能性があります。このエラーの原因として、自己署名証明書を使用して Metrics Server をインストールしたことが考えられます。この問題を解決するには、クラスターによって認識されている、正しく署名された証明書を使用して Metrics Server をインストールしてください。

アプリケーションと Persistent Volume Claim の関係の定義

オプションで、所有者依存関係を使用して、ステートフル・アプリケーションを Persistent Volume Claim (PVC) に結合することができます。この関係を定義することにより、アプリケーションに対してカスタード・アクションを有効にします。

例えば、アプリケーションのスケールアップおよびスケールダウンにより、その PVC のスケジュール済みバックアップが停止されも再開されることがあります。同様に、アプリケーションを削除すると、PVC が削除され、バックアップの削除がトリガーされます。

アプリケーションが永続データを保管するために PVC の使用を開始した後、所有者アプリケーションで PVC 定義を再構成することができます。

次の例は、アプリケーションと PVC オブジェクトの間の所有者依存関係を示す PVC のサンプル構成ファイルです。PVC オブジェクトには、所有者のデプロイメントの詳細が含まれています。

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: demo-pvc
  ownerReferences:
    - apiVersion: apps/v1beta1
      blockOwnerDeletion: true
      kind: Deployment
      name: Dept10-deployment
      uid: 3b760e89-7da5-11e9-8c5a-0050568ba59c
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-rbd
```

外部レジストリーで使用するイメージ・プル・シークレットの作成

外部の Docker レジストリーまたはリポジトリからイメージをプルする予定の場合は、イメージ・プル・シークレットを作成する必要があります。デプロイメント時に、Kubernetes は、外部レジストリーから必要なコンテナをプルして、Kubernetes Backup Support 用にポッドをプロビジョンします。

イメージ・プル・シークレットは、Kubernetes が外部レジストリーから Docker イメージをプルするために必要な資格情報を提供するために使用されます。

作成するイメージ・プル・シークレットの名前は、`baas_config.cfg` 構成ファイルの `PRODUCT_IMAGE_REGISTRY_SECRET_NAME` パラメーターの値と一致している必要があります。

イメージ・プル・シークレットは、Kubernetes Backup Support によって保護される PVC のすべての名前空間になければなりません。

内部の Docker レジストリーを使用する場合は、この手順は不要です。内部レジストリーの場合は、`PRODUCT_IMAGE_REGISTRY_SECRET_NAME` パラメーターに空ストリング ("") を指定してください。

ヒント : IBM Helm Chart Repository および IBM Entitled Registry から Kubernetes Backup Support をインストールする場合は、IBM Helm Chart Repository および IBM Entitled Registry で使用するイメージ・プル・シークレットの作成方法について、<https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod> にある製品の README ファイルを参照してください。

始めに:

- 次のコマンドを実行して、製品の名前空間 `baas` が存在していることを確認します。

```
kubectl get namespace baas
```

- `baas` 名前空間が存在していない場合は、次のコマンドを実行して作成します。

```
kubectl create namespace baas
```

Docker レジストリー用のイメージ・プル・シークレットを作成するには、次のようにします。

1. 次のコマンドを実行して、イメージ・プル・シークレットを作成します。

```
kubectl create secret docker-registry secret_name --namespace namespace_name --docker-server=registry_name --docker-username=docker_user or "token" --docker-password=password/token --docker-email=email
```

2. 次のコマンドを実行して、保護する永続ボリュームの PVC の名前空間を判別します。

```
kubectl get pvc --all-namespaces
```

3. 保護する PVC ごとに、シークレットをその PVC の名前空間にコピーします。例えば、baas 名前空間用に作成した baas-registry-secret シークレットを namespace1 名前空間にコピーするには、次のコマンドを実行します。

```
kubectl get secret "baas-registry-secret" --namespace="baas" --export -o yaml | kubectl apply --namespace="namespace1" -f -
```

Kubernetes 環境での Kubernetes Backup Support イメージのインストールとデプロイメント

Kubernetes クラスター環境内のコンテナに接続されている永続ボリュームをバックアップおよびリストアするには、事前に Kubernetes Backup Support イメージをインストールしてデプロイしておく必要があります。

始める前に

Kubernetes Backup Support は、以下のいずれかの方法を使用してインストールできます。

IBM Helm Charts Repository および IBM Entitled Registry からの Helm パッケージのダウンロードおよびインストール

Helm パッケージの方がサイズが小さいため、ダウンロードに要する時間が短くなります。デプロイメント時にコンテナをプルするには、インターネット・アクセスが必要です。ibm-spectrum-protect-plus-prod-1.0.0.tgz という名前の Helm パッケージ・ファイルを <https://github.com/IBM/charts/tree/master/repo/entitled> でダウンロードできます。

Helm チャートのインストール手順については、<https://github.com/IBM/charts/tree/master/entitled/ibm-spectrum-protect-plus-prod> で製品の README ファイルを参照してください。

IBM Passport Advantage®・オンラインからの製品パッケージのダウンロードおよびインストール

IBM パスポート・アドバンテージからのインストール・パッケージの方が大きいものの、自己完結型のパッケージです。デプロイメント時にインターネット・アクセスは不要です。このトピックでは、このパッケージのダウンロードおよびインストールの手順について説明します。

IBM パスポート・アドバンテージからインストール・パッケージをダウンロードするには、以下のタスクを実行します。

- ご使用のシステム環境が、51 ページの『Kubernetes Backup Support の要件』および 143 ページの『Kubernetes Backup Support の前提条件』に記載されている要件を満たしていることを確認します。
- インストール・ファイル SPP_V10.1.6_for_Containers.tar.gz 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 5693313](#) を参照してください。
- 以下のいずれかの方法を使用して、ダウンロードしたファイルを検証します。
 - ダウンロードしたインストール・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。
 - 以下のコマンドを発行して、インストール・パッケージに関連付けられている署名済みファイルを検証します。

```
openssl dgst -sha256 -verify IBMSPSignCertificatePublic -signature ./SPP_V10.1.6_for_Containers.tar.gz.sig ./SPP_V10.1.6_for_Containers.tar.gz
```

制約事項:

- 前のバージョンの Kubernetes Backup Support へのロールバックはサポートされていません。つまり、Kubernetes Backup Support V10.1.5 を使用して、Kubernetes Backup Support V10.1.6 によってバックアップされたデータをリストアすることはできません。
- Kubernetes Backup Support V10.1.5 からの製品のアップグレードはサポートされていません。
- BaasReq オブジェクトの基本的な変更のため、Kubernetes Backup Support V10.1.6 を使用して、Kubernetes Backup Support V10.1.5 によってバックアップされたデータをリストアすることはできません。

このタスクについて

インストールおよびデプロイメント手順時に、`baas_config.cfg` 構成ファイルをご使用の環境の仕様で更新してから、インストール・スクリプト `baas_install.sh` を実行する必要があります。インストール・スクリプトを実行すると、ご使用の環境に Kubernetes Backup Support をデプロイするために適切な Helm チャートが自動的に呼び出されます。

手順

Kubernetes 環境のコマンド・ラインで、以下のステップを実行します。

1. `cluster-admin` 特権を持つユーザーとしてターゲット・クラスターにログインします。
2. 以下のコマンドを入力して、インストール・パッケージ (`SPP_V10.1.6_for_Containers.tar.gz`) を解凍します。

```
tar -xvf SPP_V10.1.6_for_Containers.tar.gz
```

このコマンドは、`installer` という名前のフォルダーを解凍します。

3. 次のコマンドを入力して、`installer` ディレクトリーに移動します。

```
cd installer
```

4. 以下のコマンドを実行して、クラスターのクラスレス・ドメイン間ルーティング (CIDR) 方式を取得します。これらの値は、ステップ [147 ページの『6』](#) で使用されます。

```
kubectl cluster-info dump | grep -m 1 cluster-cidr
```

CIDR は、以下のフォーマットで出力に表示されます。

```
--cluster-cidr=xxx.yyy.0.0/zz
```

ヒント: コマンドが CIDR を返さない場合は、**grep** 式を変更して「cluster」と「CIDR」の組み合わせを検索し、再度コマンドを実行します。

CIDR は、以下の例のようになります。

```
198.51.0.0/24
```

5. 以下のコマンドを実行して、クラスター、およびクラスター API サーバーの IP アドレスとポートを取得します。これらの値は、ステップ [147 ページの『6』](#) で使用されます。

```
kubectl config view|awk '/cluster\:\/\/server\:\/\/' | grep server\: | awk '{print $2}'
```

結果は、以下の例に示されているように、IP アドレスとポート番号で構成される URL です。

```
https://192.0.2.0:6443
```

ここで、`192.0.2.0` はクラスター API サーバーの IP アドレスで、`6443` はポート・アドレスです。

6. テキスト・エディターを使用して `baas_config.cfg` ファイルを編集し、ご使用の環境に適切な値を指定して構成パラメーターを変更します。以下の例に示されているように、値を引用符で囲みます。

```
BAAS_ADMIN="sppadmin"
```

以下の表には、変更する必要があるパラメーターが記載されています。

表 54. <i>baas_config.cfg</i> 構成ファイルの仕様	
パラメーター	説明
BAAS_ADMIN	IBM Spectrum Protect Plus 管理者のユーザー ID。
BAAS_PASSWORD	IBM Spectrum Protect Plus パスワード。 セキュリティを強化するには、空ストリング("")を指定してください。 デプロイメント・スクリプトの実行時に、パスワードを求めるプロンプトが出されます。自動テスト・デプロイメントのために構成ファイルでパスワードを指定する必要がある場合は、そのファイルが安全な場所に保管されていることを確認してください。
CLUSTER_NAME	アプリケーション・ホストを IBM Spectrum Protect Plus サーバーに登録するのに使用される固有のクラスター名。
CLUSTER_CIDR	クラスターの CIDR。ステップ 147 ページの『4』で取得した CIDR を入力します。
CLUSTER_API_SERVER_IP_ADDRESS	クラスター API サーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)。ステップ 147 ページの『5』で取得した IP アドレスまたは FQDN を入力します。
CLUSTER_API_SERVER_PORT	クラスター API サーバーのポート・アドレス。ステップ 147 ページの『5』で取得したポート・アドレスを入力します。
LICENSE	Kubernetes Backup Support の製品ライセンス。英語のライセンス・ファイルは、インストール・パッケージに含まれている <code>installer/licenses/LA_en</code> ディレクトリーにあります。その他の言語のライセンスのバージョンは、 License Information documents で入手できます。 ライセンス情報を確認し、ACCEPTED を指定して、プロンプトが出されることなくインストール中にライセンスを受け入れます。 デフォルト値は NOTACCEPTED です。デフォルト値を変更しない場合は、インストール中にライセンスの受け入れを求めるプロンプトが出されます。そうしないと、インストールが失敗します。
SPP_AGENT_SERVICE_NODEPORT	IBM Spectrum Protect Plus から Kubernetes Backup Support エージェント・コンテナ・サービスへの接続のための SSH ポート。 このポートに値を指定しない場合、NodePort 範囲内のランダム・ポートが、Kubernetes の NodePort サービスによって割り当てられます。デフォルトの範囲は 30000 から 32767 です。 このポートに値を指定する場合は、Kubernetes 管理者によってセットアップされている NodePort 範囲内のポート番号を使用します。ポートがクラスターによってまだ使用されていないことを確認してください。ポートが既に使用されている場合、インストール・プロセスは失敗し、どの NodePorts が既に使用されているかを示すエラーが出されます。
SPP_IP_ADDRESSES	IBM Spectrum Protect Plus サーバーの IP アドレスまたは FQDN。
PRODUCT_IMAGE_REGISTRY	コンテナをホストする Docker レジストリーのアドレスとポート。 <i>ip_address:port</i> フォーマットでアドレスを入力してください。
PRODUCT_IMAGE_REGISTRY_NAMESPACE	コンテナをホストする Docker レジストリーの名前空間。

表 54. *baas_config.cfg* 構成ファイルの仕様 (続き)

パラメーター	説明
PRODUCT_IMAGE_REGISTRY_SECRET_NAME	<p>レジストリーの資格情報を含む、Kubernetes イメージ・プル・シークレットの名前。このシークレットは、PRODUCT_IMAGE_REGISTRY_NAMESPACE パラメーターで指定された名前空間内になければなりません。</p> <p>内部レジストリーを使用している場合は、空ストリング("")を入力してください。</p> <p>データ・ムーバー・コンテナを実行するには、バックアップおよびリストアされる各 Persistent Volume Claim (PVC) のすべての名前空間に、イメージ・プル・シークレットが存在する必要があります。</p> <p>イメージ・プル・シークレットの作成手順については、145 ページの『外部レジストリーで使用するイメージ・プル・シークレットの作成』を参照してください。</p>
PRODUCT_LOGLEVEL	<p>Kubernetes Backup Support トランザクション・マネージャー、コントローラー、およびスケジューラー・コンポーネントの問題をトラブルシューティングするためのトレース・レベル。トレース・レベル INFO、WARNING、DEBUG、または ERROR が使用可能です。</p> <p>デフォルト: INFO</p>

制約事項:

- 以下のパラメーターおよび値は Kubernetes Backup Support 用に予約されています。そのまま保持してください。

```
PRODUCT_NAMESPACE="baas"
OPERATOR_NAMESPACE="default"
PRODUCT_TARGET_PLATFORM="K8S"
```

- SPP_PORT 値は、IBM Spectrum Protect Plus ユーザー・インターフェースのポートを指定します。デフォルト値 443 を変更しないでください。
- Kubernetes Backup Support は、IBM Spectrum Protect Plus V10.1.6 で英語でのみ使用可能です。そのため、PRODUCT_LOCALIZATION="en_US" の設定を変更しないでください。

仕様は、デプロイメント中に ConfigMap (baas-configmap) に自動的に挿入されます。

- 以下のコマンドを発行して、インストールとデプロイメントを開始します。

```
./baas_install.sh -i
```

プロンプトが出されたら、yes と入力して続行します。

- インストール・プロセス中に、以下の情報を求めるプロンプトが出されます。

a) プロンプトが出されたら、IBM Spectrum Protect Plus 管理者 ID とパスワードを入力します。

b) IBM Spectrum Protect Plus サーバーとの接続を確認するように求めるプロンプトが出されたら、yes と入力して続行します。

no と入力すると、IBM Spectrum Protect Plus サーバーとの接続を確認せずにインストールが続行します。

yes と入力したときに、接続テストが失敗した場合、インストールは次のエラー・メッセージを出して終了します。

```
ERROR: Could not connect to IBM Spectrum Protect Plus server with provided credentials.
```

ご使用の環境によっては、パッケージをロードしてデプロイするまでに数分かかる場合があります。

9. Kubernetes Backup Support コンポーネントが正しくインストールされていることを確認するには、次のコマンドを発行します。

```
./baas_install.sh -s
```

インストールが失敗した場合は、欠落しているコンポーネントが出力の MISSING セクションにリストされます。

ヒント: `./helm status baas` コマンドを使用してインストールの状況を確認することもできます。

タスクの結果

すべてのポッドが実行されている場合、デプロイメントは完了しました。すべてのポッドが Running 状態にあり、コンポーネントが欠落していないことを確認するには、以下のコマンドを発行します。

```
kubectl get pods -n baas
```

または

```
kubectl describe pod pod_name -n baas
```

出力は、以下の例のようになります。

```
kubecttl get pods -n baas
NAME                                READY   STATUS    RESTARTS   AGE
baas-controller-768869468c-crttd4   1/1     Running   0           4m24s
baas-kafka-68d7ff8455-m96cc         1/1     Running   0           4m24s
baas-scheduler-656978d87f-thqv2     1/1     Running   1           4m24s
baas-spp-agent-cdb784466-v9tnz      1/1     Running   0           4m24s
baas-transaction-manager-657db7bb8b-6dgqb 1/1     Running   2           4m24s
-----
All pods are running.
All resources are installed successfully.
Installation is completed.
Product release >>baas<< version 10.1.6 has been installed in namespace >>baas<< at Wed May 20
17:58:02 MST 2020.
Script baas_install.sh finished at Wed May 20 17:58:02 MST 2020. A log of this transaction has
been written to /tmp
/baas_installation.sh_20200520-175605.log .
```

データ・ムーバー・コンテナが出力にリストされていない場合、データ・ムーバー・コンテナは実行時にデプロイされます。

以下のコマンドを発行して、セットアップされた Kubernetes Backup Support サービスを表示することができます。

```
kubectl get services -n baas
```

出力は、以下の例のようになります。

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
baas-kafka-svc	ClusterIP	10.110.116.210	<none>	9092/TCP,2181/TCP	4m27s
baas-scheduler	ClusterIP	10.96.38.170	<none>	8000/TCP	4m27s
baas-spp-agent	NodePort	10.110.164.151	<none>	22:30412/TCP	4m27s
baas-transaction-manager	ClusterIP	10.108.42.194	<none>	5000/TCP	4m27s

baas-datamover サービスは、TCP プロトコルを使用する ClusterIP の範囲ではなく、NodePort タイプで実行時にデプロイされます。

以下のコマンドを発行して、デプロイされた Kubernetes Backup Support ネットワーク・ポリシーを表示することができます。

```
kubectl get networkpolicies -n baas
```

出力は、以下の例のようになります。

NAME SELECTOR	POD
------------------	-----


```
AGE
baas-ctl-networkpolicy    app.kubernetes.io/component=controller,app.kubernetes.io/
name=baas,app.kubernetes.io/version=10.1.6    4m30s
baas-kafka                app.kubernetes.io/component=kafka,app.kubernetes.io/
name=baas,app.kubernetes.io/version=10.1.6    4m30s
baas-scheduler            app.kubernetes.io/component=scheduler,app.kubernetes.io/
name=baas,app.kubernetes.io/version=10.1.6    4m30s
baas-spp-agent            app.kubernetes.io/component=spp-agent,app.kubernetes.io/
name=baas,app.kubernetes.io/version=10.1.6    4m30s
baas-transaction-manager  app.kubernetes.io/component=transaction-manager,app.kubernetes.io/
name=baas,app.kubernetes.io/version=10.1.6    4m30s
```

データ・ムーバーのネットワーク・ポリシーは、ポッド・セクター `app.kubernetes.io/name=baas,app.kubernetes.io/component=datamover,version=10.1.6` を使用して実行時にデプロイされます。

次のタスク

デプロイメントが完了したら、Kubernetes Backup Support コンテナのアプリケーション・ホストは、Kubernetes のクラスター・ホストの始動時に自動的に登録されます。ただし、自動登録が失敗した場合、IBM Spectrum Protect Plus ユーザー・インターフェースを使用して手動でクラスターを登録することができます。手順については、[314 ページの『Kubernetes クラスターの登録』](#)を参照してください。

既存の構成を更新する場合、または Kubernetes Backup Support の既存のインストール済み環境をアップグレードする場合は、ご使用の環境で必要に応じて `baas_config.cfg` ファイル内のパラメーターを変更し、以下のコマンドを発行します。

```
./baas_install.sh -u
```

関連概念

[520 ページの『Kubernetes Backup Support のトラブルシューティング』](#)

Kubernetes Backup Support の問題のトラブルシューティングを行うために、デバッグ・ログ・ファイルを収集して、トレース・ログを表示することができます。問題を診断するための手順に従うこともできます。

関連タスク

[521 ページの『ログ・ファイルのトレース・レベルの設定』](#)

ローカル・ログ・ファイルのトレース・レベルを設定すると、Kubernetes Backup Support で発生する可能性がある問題のトラブルシューティングに役立ちます。

Kubernetes Backup Support のアンインストール

すべての構成およびバックアップを含むすべてのコンポーネントが Kubernetes 環境から削除されるように、Kubernetes Backup Support を完全にアンインストールすることができます。

始める前に

アンインストールを開始する前に、以下のアクションを実行してください。

- スケジュールされたすべてのバックアップを停止します。手順については、[PVC の SLA バックアップの中止](#)または [YAML ファイル内のパラメーターの変更](#)を参照してください。
- 実行中のすべてのバックアップ・ジョブとリストア・ジョブが終了するまで待ちます。

手順

ログインしているクラスターから Kubernetes Backup Support を完全にアンインストールするには、コマンド・ラインで以下のステップを実行します。

- destroy** 要求を使用して、すべてのスナップショット・バックアップおよびコピー・バックアップを破棄します。手順については、[345 ページの『コンテナ・バックアップの削除』](#)を参照してください。
- コピー・バックアップに使用された Persistent Volume Claim (PVC) をすべて削除します。

ヒント: バックアップされた PVC の名前を検索できます。

3. 以下のコマンドを発行して、**baas** カスタム・リソース定義 (CRD) を削除します。

```
kubectl delete crd baasreqs.baas.io
```

このコマンドは、すべての **BaasReq** 要求オブジェクトも削除します。

4. **installer** ディレクトリーから次のコマンドを発行して、**Kubernetes Backup Support** をアンインストールします。

```
./baas_install.sh -d
```


プロンプトが出されたら、**yes** と入力して続行します。

このコマンドは、すべてのデータ・ムーバー・ポッド、デプロイメント、およびネットワーク・ポリシーを削除します。**Kubernetes Backup Support** の **Kubernetes** シークレットも削除されます。


5. オプション: アンインストールの進行状況を確認するには、以下のコマンドを入力します。

```
kubectl get pod -n baas
```

6. **IBM Spectrum Protect Plus** ユーザー・インターフェースを使用して、**Kubernetes** クラスターの登録を抹消します。

- ナビゲーション・ペインで、「**保護の管理**」 > 「**コンテナ**」 > 「**Kubernetes**」をクリックします。
- 「**Kubernetes**」ページで「**クラスターの管理 (Manage clusters)**」をクリックします。
- ホスト・アドレスのリストで、登録抹消したいクラスターの横にある削除アイコン  をクリックします。
- 「**確認**」ウィンドウで、表示された確認コードを入力し、「**登録抹消**」をクリックします。

7. **Kubernetes** クラスターの登録に使用されるアカウント ID を削除します。

- 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。
- クラスタ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。
- 「**はい**」をクリックして ID を削除します。

8. **VolumeSnapshotDataSource** 機能がなくなった場合は、使用不可にします。

9. **baas** 名前空間を削除することにより、SLA ポリシーおよびその他のカスタマイズを削除します。次のコマンドを発行します。

```
kubectl delete namespace baas
```

10. 外部レジストリーで使用するためのイメージ・プル・シークレットを手動で作成した場合は、そのシークレットが存在していたすべての名前空間で **kubectl delete secret** コマンドを使用してシークレットを削除します。

11. オプション: インストールおよび構成情報を確認し、前提条件ステップをすべて元に戻します。

次のタスク

Kubernetes Backup Support が正常にアンインストールされなかった場合は、523 ページの『[トラブルシューティングのクイック・リファレンス](#)』で「**Kubernetes Backup Support** が正常にアンインストールされなかった」を参照してください。

第6章 クイック・スタート

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) の作成などの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。データのコピー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 [1 ページの『IBM Spectrum Protect Plus のデプロイメント・ストーリーボード』](#) 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、リソースのバックアップ・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	説明
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	<p>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。</p> <p>初期起動後、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。</p>

アクション	所有者	説明
156 ページの『管理サイト』	インフラストラクチャー管理者	<p>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。</p> <p>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。</p> <p>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。</p>
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	<p>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・データをコピーするオプションがあります。</p> <p>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。</p> <p>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。</p>
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	<p>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。</p>
保護するリソースの追加	アプリケーション管理者	<p>リソースは、保護したいエンティティです。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ます。</p>

アクション	所有者	説明
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-SysXyz` 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。

新規パスワードの作成時には、次の規則が適用されます。

- パスワード長は 15 文字以上にします。
- 新規パスワードには、前のパスワードには存在しない、8 文字を指定する必要があります。
- 新規パスワードには、各クラス (数字、英大文字、英小文字、およびその他) から最低 1 文字ずつ指定する必要があります。
- 新規パスワードで指定可能な同一の連続文字は 3 文字までです。
- 新規パスワードで指定可能な同一クラスの連続文字は 4 文字までです。

- ・ 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

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。	<ol style="list-style-type: none"> 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、198 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コピー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。	<ol style="list-style-type: none"> 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、199 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コピー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

[5 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。

[198 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

IBM Spectrum Protect Plus には、225 ページの『第9章 バックアップ操作の SLA ポリシーの管理』で説明されているデフォルトの SLA ポリシーが含まれています。デフォルト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。

例を挙げる目的で、以下のステップは、VMware 用の SLA ポリシーを作成する方法を示しています。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・ストレージへのデータのコピー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、228 ページの『ハイパーバイザー、データベース、およびファイル・システムの 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. 「**VMware、Hyper-V、Exchange、Office365、SQL、Oracle、Db2、MongoDB および Windows ファイル・システム (VMware, Hyper-V, Exchange, Office365, SQL, Oracle, Db2, MongoDB and Windows File Systems)**」をクリックします。
5. 「**バックアップ・ポリシー**」セクションで、以下のバックアップ操作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

制約事項:「**週**」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

バックアップ操作の頻度を入力します。「**分**」、「**時間**」、「**日**」、「**週**」、「**月**」、または「**年**」から選択します。「**週**」が選択されている場合、1 つ以上の曜日を選択できます。「**開始時刻**」は、選択した曜日に適用されます。

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。

タイム・ゾーンには、ブラウザーの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「**ヨーロッパ/ダブリン**」)。フィールドをクリックして、「**検索**」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

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、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。

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。

The screenshot shows a web interface for creating a new SLA Policy. The title is 'Policy Overview' and the subtitle is 'New SLA Policy'. The form includes the following fields and options:

- Name:** A text box containing 'Copper'.
- Platform Selection:** Three radio buttons are shown:
 - ☒ VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB, Catalog, and Windows File Systems
 - ☐ Kubernetes
 - ☐ Amazon EC2
- Backup Policy:**
 - Retention:** A dropdown menu set to '1' and a unit dropdown set to 'Months'.
 - ☐ Disable Schedule
 - Frequency:** A dropdown menu set to '3' and a unit dropdown set to 'Days'.
 - Start Time:** Three fields: '06/02/2020', '00:00', and 'America/Los_Angeles'.
 - Target Site:** A dropdown menu set to 'Primary'.
 - ☐ Only use encrypted disk storage.
- Replication Policy:**
 - ☐ Backup Storage Replication
- Buttons:** 'Cancel' and 'Save' buttons at the bottom.

図 12. SLA ポリシーの作成

6. 「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 ([163 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

[10 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。

11 ページの『2 次バックアップ・ストレージへのコピー・スナップショット』

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・ストレージにコピーできます。

225 ページの『バックアップ操作の SLA ポリシーの管理』

サービス・レベル契約 (SLA) ポリシーは、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コピーするオプションがあります。事前定義された SLA ポリシーを使用できます。また、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リソース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、512 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、504 ページの『リソース・グループの作成』および 509 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。

User

Add User - User Information and Role

Select the type of user or group you want to add. Individual new user

Username
Username must not be 'root', 'admin' or 'test'.

Password [Show](#)
Password must contain at least 8 characters.

ASSIGN ROLE

- ☐ Application Admin
- ☐ Backup Only
- ☐ Restore Only
- ☐ SYSADMIN
- ☐ Self Service
- ☒ VM Admin

PERMISSION GROUPS

- [Certificate](#)
- [Cloud](#)

[Cancel](#) [Continue >](#)

図 13. 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。

User

Add User - Assign Resources

vmadmin

VM Administrator

Choose resource groups to assign

☒ All Resources

☐ Hypervisor All Resource Group

Add resources

Selected Resources

All Resources

Cancel

< Back to user role

Create user

図 14. 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

503 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

リソースは、保護したいエンティティです。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、以下のセクションでリソース・タイプ別の説明を参照してください。

- 241 ページの『第 10 章 仮想化システムの保護』
- 291 ページの『第 11 章 ファイル・システムの保護』
- 309 ページの『第 12 章 コンテナの保護』
- 347 ページの『第 13 章 クラウド・システム上のデータの保護』
- 353 ページの『第 14 章 データベースの保護』

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」 > 「仮想化システム (Virtualized Systems)」 > 「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」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。

The screenshot displays the 'VMware' configuration window. At the top, there are 'Manage vCenter' and 'Create job' buttons. The main section is titled 'Manage vCenter'. Under 'vCenter Properties', the following fields are visible: 'Hostname/IP' with the value '192.0.2.0', 'Use existing user' which is unchecked, 'Username' with the value 'admin_192.0.2.0', 'Password' which is masked with dots, and 'Port' with the value '443'. Below these, the 'Use SSL' checkbox is checked. The 'Options' section contains a field for 'Maximum number of VM's to process concurrently per ESX server' with the value '3'. At the bottom of the configuration area are 'Cancel' and 'Save' buttons. The footer of the window reads 'VMware Backup'.

図 15. 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。

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」 > 「仮想化システム (Virtualized Systems)」 > 「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」、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。

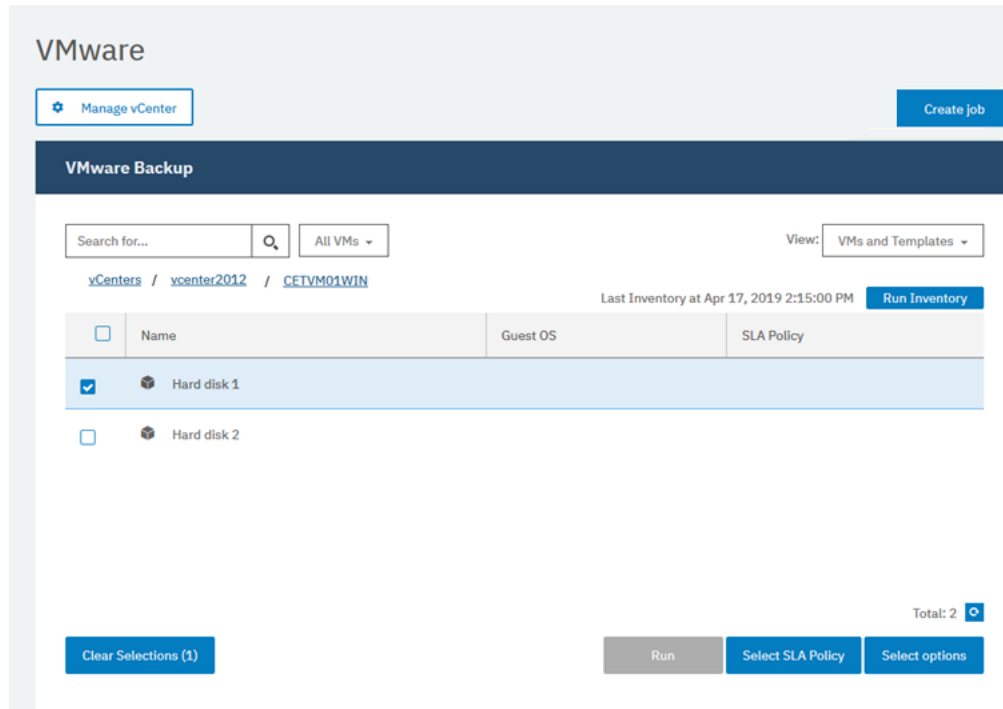



図 16. バックアップ用のリソースの選択

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。

Search Policy by name... 			
	SLA Policy	Frequency	Retention
<input type="checkbox"/>	Gold	Every 4 Hours	1 Weeks
<input type="checkbox"/>	Silver	Every 1 Days at 10:10:00 PM	1 Months
<input type="checkbox"/>	Bronze	Every 1 Days at 10:10:00 PM	1 Weeks
<input checked="" type="checkbox"/>	Copper	Every 3 Days at 12:00:00 AM	1 Months

Save


Total: 98 

図 17. SLA ポリシーの選択

- 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。このサンプル・ジョブでは、vmware_Copper という名前が作成されます。
- 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、[245 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。
- 「**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。[250 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、[164 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

[475 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、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。

- 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。
- 次の例に示すように、実行するジョブを選択して、「**開始**」アクションをクリックします。

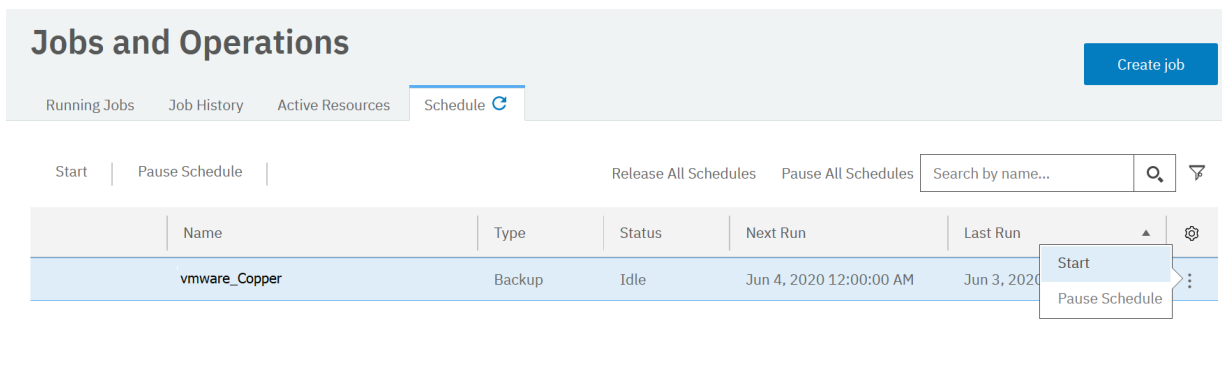


図 18. ジョブの開始

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

479 ページの『[ジョブと操作の管理](#)』

「**ジョブと操作**」ウィンドウでジョブを管理して、モニターすることができます。ジョブの実行前または実行後に実行するスクリプトを構成することもできます。

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**」タブをクリックします。












































Reports			
Reports		Custom Reports	
		Filter by category: All	
	Name (job title)	Category	Schedule
 	Configuration	System	
 	Container Persistent Volume Backup History	Protection	
 	Container Persistent Volume Backup Utilization	Backup Storage Utilization	
 	Container SLARPOComplianceDisplay/Name	Protection	
 	Database Backup History	Protection	
 	Database Backup Utilization	Backup Storage Utilization	
 	Database SLA Policy RPO Compliance	Protection	
 	Job	System	
 	License	System	
 	Protected and Unprotected Container Persistent Volumes	Protection	
 	Protected and Unprotected Databases	Protection	
 	Protected and Unprotected VMs	Protection	
 	VM Backup History	Protection	
 	VM Backup Utilization	Backup Storage Utilization	
 	VM Datastores	VM Environment	
 	VM LUNs	VM Environment	
 	VM SLA Policy RPO Compliance	Protection	
 	VM Snapshot Sprawl	VM Environment	
 	VM Sprawl	VM Environment	
 	VM Storage	VM Environment	
 	vSnap Storage Utilization	Backup Storage Utilization	

図 19. 実行するレポートの選択

- レポートの横にある「**レポートの実行**」() アイコンをクリックして、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、「**レポートの実行**」ウィンドウ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

491 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 7 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・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 5693313](#) 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、475 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。

更新の管理

IBM Spectrum Protect Plus 環境には、IBM Spectrum Protect Plus サーバー、1 つ以上の vSnap サーバー、そしてオプションで 1 つ以上の VADP プロキシが含まれています。IBM Spectrum Protect Plus を正常に移働させるには、環境内のすべてのコンポーネントが同じバージョン・レベルでなければなりません。手順を確認して、更新処理を慎重に計画および実行します。

始める前に

以下のステップを実行してください。

1. 更新処理のメンテナンスと検証の期間について計画します。必要な時間は、更新する必要がある環境内のコンポーネント数に基づいて推定できます。

IBM Spectrum Protect Plus 環境をアップグレードする処理は、環境内のコンポーネントの数、および関連する場所のネットワーク速度によって異なります。以下の表には、3 つの IBM Spectrum Protect Plus コンポーネントと、更新の適用およびシステムの正常な再始動に要する平均時間 (分単位) が記載されています。

表 55. IBM Spectrum Protect Plus コンポーネントとアップグレード時間

コンポーネント	更新にかかる時間	再始動にかかる時間	合計
IBM Spectrum Protect Plus サーバー	10	15	25
vSnap サーバー (vSnap server)	15	10 - 30	25 - 45
VADP プロキシ・サーバー	15	必要なし。	15

2. ご使用の環境内のコンポーネントに関するバージョン情報を収集し、更新処理のためにバージョン・レベルを判別します。アップグレード処理の一環として vSnap サーバーを更新する必要があるかどうかを判別します。

3. スケジュールされたインベントリー・ジョブまたはメンテナンス・ジョブがメンテナンスと検証の期間の完了後に実行されるように、開始時刻を調整します。

4. オブジェクト・ストレージ・リストア・ジョブなど、リストア・ジョブまたは再使用ジョブを終了します。これらのジョブは、必要に応じて、メンテナンスと検証の期間の完了後にスケジュールします。

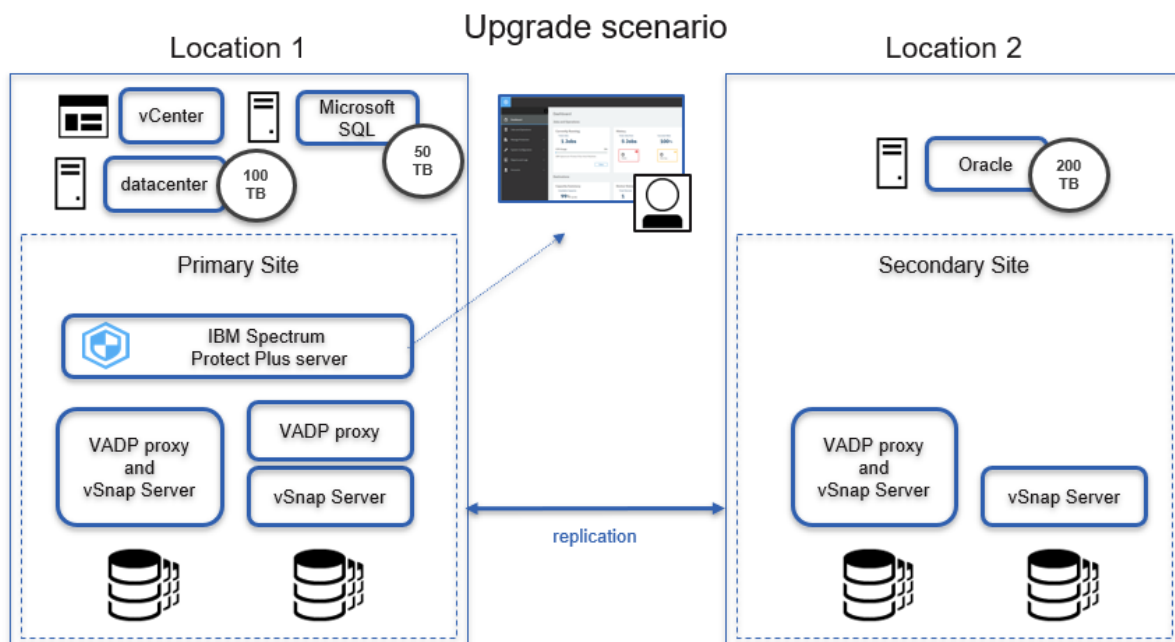
5. 残りのジョブがあればそれも一時停止し、メンテナンスと検証の期間中に実行されないようにします。

このタスクについて

ここでの手順は、以下のコンポーネントが含まれた環境例に基づいています。

- IBM Spectrum Protect Plus サーバー 1 つ
- 組み込み vSnap サーバー 2 つと、スタンドアロン vSnap サーバー 2 つ (4 つすべてのサーバーに複製関係がある)
- 2 つの vSnap サーバーと同時にインストールされている 2 つの VADP プロキシ
- 1 つのスタンドアロン VADP プロキシ

以下の図では、ロケーション 1 とロケーション 2 のそれぞれのサイトのコンポーネントが表示されています。



手順

1. 更新処理に際してシステム環境を準備するには、以下のステップを実行します。
 - a) 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、「**SLA ポリシーの追加**」ボタンをクリックします。
 - b) 「**新規 SLA ポリシー**」ペインで、ポリシー名を入力し、用語「**カタログ**」が含まれているラジオ・ボタンをクリックします。「**保存**」をクリックします。
 - c) 「**スケジュールを無効にする**」チェック・ボックスを選択し、適切な保存期間を指定します。「**ターゲット・サイト**」リストから、カタログ・バックアップが含まれるサイトを選択します。
 - d) オプションで、他のオプションをバックアップ・ジョブ用に指定します。「**保存**」をクリックします。
 - e) 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。
 - f) 「**SLA ポリシー**」ペインで、作成したポリシーを選択します。「**保存**」をクリックします。
 - g) ポリシーが「**SLA ポリシーのステータス**」ペインに表示されます。自動的に表示されない場合は、最新表示ボタンをクリックします。
 - h) カatalog・バックアップを開始するには、「**アクション**」をクリックしてから「**開始**」をクリックします。
 - i) カatalog・バックアップ・ジョブが完了したことを確認します。ナビゲーション・ペインで、「**ジョブと操作**」をクリックして、カタログ・バックアップ・ジョブが正常に完了したことを確認します。
 - j) すべてのスケジュール済みジョブを一時停止します。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。「**すべてのスケジュールを一時停止 (Pause All Schedules)**」をクリックします。すべてのスケジュール済みジョブの状況が「**保留**」に変わります。
 - k) 実行中のジョブがないことを確認するには、「**実行中のジョブ**」タブをクリックします。ジョブが実行中の場合は、ジョブが処理を完了できるようにします。
2. vSnap サーバーの更新を準備するには、IBM Spectrum Protect Plus Blueprints (<https://www.ibm.com/support/pages/node/1119489>) を参照してください。環境内のすべての vSnap サーバーを、同じ IBM Spectrum Protect Plus バージョン・レベルに更新する必要があります。vSnap サーバーを更新するには、次のステップを完了します。
 - a) 171 ページの『仮想 vSnap サーバー用のオペレーティング・システムの更新』の説明に従って、vSnap サーバー用のオペレーティング・システムを更新するステップを実行します。

重要: オペレーティング・システムを更新する場合は、手順の説明に従って、ダウンロードされた ISO ファイルの名前を変更し、vSnap サーバー上の /tmp ディレクトリーにファイルを移動する必要があります。
 - b) 172 ページの『vSnap サーバーの更新』の説明に従って、vSnap サーバーを更新するステップを実行します。


ヒント: vSnap サーバーの更新後、vSnap サーバーの再始動に要する時間は旧バージョンよりも 15 分長くなる可能性があります。詳しくは、<https://www.ibm.com/support/pages/node/3531159> を参照してください。
3. 以下のステップを実行して、IBM Spectrum Protect Plus サーバーを更新します。
 - a) オプション: IBM Spectrum Protect Plus サーバーが仮想的にデプロイされる場合は、適切なハイパーバイザー・インターフェースでアプライアンスのスナップショットを取得します。
 - b) IBM Spectrum Protect Plus サーバーを更新します。173 ページの『IBM Spectrum Protect Plus 仮想アプライアンスの更新』トピックのステップ 1 から 6 までを実行します。ただし、最後の 2 のステップで示されているように、保留されているスケジュールやジョブを解除しないでください。
 - c) IBM Spectrum Protect Plus サーバーに再度ログインします。
4. VADP プロキシを更新します。IBM Spectrum Protect Plus サーバーを更新すると VADP プロキシも自動的に更新されます。ただし、プロキシがすぐに更新されない場合があります。

VADP プロキシをすぐに更新するには、175 ページの『VADP プロキシの更新』トピックのステップを実行します。

5. 以下のステップを実行して、すべてのコンポーネントが正常に更新されたことを確認します。
- a) serveradmin アカウントを使用して IBM Spectrum Protect Plus 管理コンソールにログオンします。204 ページの『管理コンソールへのログオン』のステップに従います。
 - b) 「製品管理 (Product Management)」をクリックします。表で、以下の項目が同じバージョン・レベルであることを確認します。 spp-release、vsnap、vsnap-dist、vadp、および vadp-dist。
 - c) IBM Spectrum Protect Plus 管理コンソールからログアウトします。
 - d) サポート対象ブラウザを開き、以下の URL を入力して IBM Spectrum Protect Plus スプラッシュ画面を読み込みます。

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

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。

- e) スプラッシュ画面上のバージョンとビルドが、管理コンソールの「製品管理 (Product Management)」セクションに表示されていた spp-release と一致していることを確認してください。
 - f) 更新された環境でメンテナンス・ジョブが正常に実行できることを確認するには、ナビゲーション・ペインで、「ジョブと操作」 > 「スケジュール」をクリックします。メンテナンス・ジョブの横にあるオプション・アイコン  をクリックして、「開始」を選択します。「ジョブと操作」ペインでジョブの進行状況をモニターします。
6. スケジュールされたジョブを保留解除し、オプションでスナップショットを削除します。以下のステップを実行してください。
- a) すべてのスケジュールを保留解除します。ナビゲーション・ペインで、「ジョブと操作」 > 「スケジュール」をクリックします。「すべてのスケジュールを保留解除 (Release All Schedules)」をクリックします。
 - b) オプション: IBM Spectrum Protect Plus 仮想アプライアンスのスナップショットを取得していた場合は、ハイパーバイザー・インターフェースを使用して IBM Spectrum Protect Plus サーバーのスナップショットを削除できます。ハイパーバイザーの資料に示された手順に従ってください。

次のタスク

必要に応じて、保守および検査期間中に停止または一時停止されたジョブを再始動してください。

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 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ているジョブは、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があります。オペレーティング・システム要件については、21 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

172 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

ISO ファイルを使用して vSnap サーバー・オペレーティング・システムを更新すると、使用可能な最新のパッチとセキュリティ更新が提供されます。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・ソフトウェアを更新する必要があります。バージョン 7.5 または 7.6 ではオペレーティング・システムの更新はオプションです。ISO ファイルをダウンロードして、仮想 vSnap サーバーのアップグレードに使用します。

始める前に

更新処理を始める前に、475 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。ISO ファイルの取得方法について詳しくは、173 ページの『[IBM Spectrum Protect Plus 仮想アプライアンスの更新](#)』を参照してください。

制約事項: Red Hat Enterprise Linux 物理サーバーを更新する場合は、ISO を使用しないでください。ISO は、OVA デプロイメントでのみ使用することが必要です。

手順

1. ISO ファイルの `<part_number>.iso` をダウンロードします。ISO ファイルを vSnap サーバー上の `/tmp` ディレクトリーに移動し、ファイルを `spp_with_os.iso` に名前変更します。

```
$mv <part_number>.iso /tmp/spp_with_os.iso
```

重要: オペレーティング・システムを更新する場合は、前述のステップで説明されているようにダウンロードされた ISO ファイルの名前を変更し、vSnap サーバー上の `/tmp` ディレクトリーに移動することが重要です。

2. 172 ページの『[vSnap サーバーの更新](#)』トピックに記載されている指示に従って続行します。`<part_number>.run` ファイルが実行される際に、`/tmp/spp_with_os.iso` が存在すると、インストーラーはオプションでオペレーティング・システムを更新します。

以下の 2 つのシナリオは、ISO ファイルが存在するかしないかによってどちらか 1 つが実施されます。

- ISO ファイルが存在する場合、オペレーティング・システム・パッケージはアップグレードされ、vSnap ソフトウェアがアップグレードされます。
- ファイルが存在しない場合は、次のようなメッセージが表示されます。

```
File /tmp/spp_with_os.iso is not present, skipping update of OS packages.  
To update OS packages, download the ISO file to /tmp/spp_with_os.iso and rerun this  
installer.
```

その後 vSnap ソフトウェアがアップグレードされます。

インストーラーが完了すると、`/tmp/spp_with_os.iso` を削除できます。

関連タスク

172 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. 475 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. vSnap 更新ファイル `<part_number>.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 5693313](#) 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. `<part_number>.run` ファイルが置かれているディレクトリーから、以下のコマンドを実行してファイルを実行可能にします。

```
$ chmod +x <part_number>.run
```

3. 以下のコマンドを実行して、インストーラーを実行します。

```
$ sudo ./<part_number>.run
```

あるいは、`noprompt` オプションを使用して vSnap の非対話式のインストールまたは更新を開始することができます。このオプションが使用されると、vSnap インストーラーでは応答のプロンプトをスキップし、以下のプロンプトに対して応答として「はい」を想定します。

- ご使用条件
- カーネルをインストールして更新する
- インストールの終了時にリブートするか、必要な場合は更新する

`noprompt` オプションを使用するには、次のコマンドを発行します。次のように 2 つ並んだダッシュの前後に意図的にスペースを挿入します。

```
$ sudo ./<part_number>.run -- noprompt
```

vSnap パッケージがインストールされます。

4. vSnap パッケージのインストール後に、更新バージョンの vSnap サーバーを開始します。
5. 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。
6. 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。

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

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、[475 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。
2. オフライン更新の場合、`<part_number>.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 5693313](#) 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	SUPERUSER 特権を持つ IBM Spectrum Protect Plus ユーザーとしてログインするには、管理者ユーザー名とパスワードを入力します。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-SysXyz 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。

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する場合にオフライン・モードしか表示されないときは、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: 更新が使用可能になると、リポジトリに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。一度に 1 つの更新ファイルしか選択できません。

重要: IBM Spectrum Protect Plus サーバーの /tmp ディレクトリーには使用可能な 4.2 GB 以上のディスク・スペースがなければなりません。

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・サーバーおよび VADP プロキシ・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

170 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。

Hyper-V Replica 環境で仮想マシンを更新するための追加のステップ

IBM Spectrum Protect Plus バージョン 10.1.5 以降では、Hyper-V Replica 機能が使用可能になっている仮想マシン (VM) を保護できます。

IBM Spectrum Protect Plus は、VM のソースと複製されたインスタンスでデータを個別に処理します。例えば、VM1 という名前の VM が Host1 という名前の Hyper-V ホストにあり、この VM が Host2 に複製される場合、IBM Spectrum Protect Plus は、ID VM1@Host1 および VM1@Host2 を VM に割り当てます。その後、データ保護のために、一方または両方の VM を選択できます。

既存の SLA ポリシーで定義されている VM に関する考慮事項

IBM Spectrum Protect Plus を更新する場合、現在、SLA ポリシーに含まれている VM でデータ保護が継続されるように追加のステップを実行する必要がある可能性があります。

SLA ポリシーには、複製された VM が暗黙的または明示的に含まれている場合があります。IBM Spectrum Protect Plus V10.1.5 以降に更新する際、SLA ポリシーの更新が必要になることがあります。

複製された VM が暗黙的に含まれている SLA ポリシーの例として、VM VM1 が含まれている Host1 のすべての VM がポリシーによって保護されるシナリオが挙げられます。VM1 が Host2 に複製されます。このシナリオでは、IBM Spectrum Protect Plus の更新後に SLA ポリシーを変更する必要はありません。SLA ポリシーにより、VM1 のインスタンスのフルバックアップが Host2 で作成され、VM1 のインスタンスの新規

のフルバックアップが Host1 で作成されます。Host1 で更新前に作成された VM1 の既存のバックアップは、SLA ポリシーの保存設定に基づいて期限切れになります。

複製された VM が明示的に含まれている SLA ポリシーの例としては、Host1 の VM1 がポリシーによって保護されていて、VM1 が Host2 に複製されるシナリオが挙げられます。このシナリオでは、IBM Spectrum Protect Plus の更新後に、各ホスト上の VM のインスタンスを SLA ポリシーに再び追加する必要があります。

VADP プロキシの更新

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、475 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。

注： IBM Spectrum Protect Plus に登録されている VADP プロキシのみが更新されます。VADP プロキシが IBM Spectrum Protect Plus に登録されていない場合、VADP コンポーネントは更新されません。

手順

VADP プロキシ更新が、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 プロキシに自動的に適用されます。VADP プロキシを ID に関連付けるには、「システム構成」 > 「VADP プロキシ」にナビゲートします。省略符号アイコン *** をクリックし、「編集」を選択します。「既存ユーザーの使用」を選択し、VADP プロキシ・サーバーの「ユーザーの選択」で以前に入力した ID を選択します。

VADP プロキシ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」ページにナビゲートします。
2. 「VADP プロキシ」ページに、各プロキシ・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・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・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。	<p>245 ページの『VMware データのバックアップ』を参照してください。</p> <p>プロキシは、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。</p> <p>Run remote vmdkbackup of MicroService: http://<proxy nodename, IP:proxy_IP_address</p>

関連タスク

252 ページの『[VADP プロキシの作成](#)』

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 プロキシを作成できます。

関連資料

99 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・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・トラフィックを、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 8 章 システム環境の構成

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。



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・サーバーにコピーできます。

2 次ストレージへのスナップショット・データのコピーについては、[11 ページの『2 次バックアップ・ストレージへのコピー・スナップショット』](#)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・ストレージにスナップショット・データをコピーすることができます。

クラウドにデータをコピーまたはアーカイブするための構成

長期保存またはスナップショット・ストレージのためにクラウド・ストレージに IBM Spectrum Protect Plus データをコピーまたはアーカイブする 予定の場合は、2 次ストレージを構成する必要があります。

クラウド・ストレージを構成するためのタスク

表 1 に示すように、クラウド・ストレージへのバックアップ操作とリストア操作用に IBM Spectrum Protect Plus を構成する必要があります。

ユーザー・シナリオ	目的	ステップ
重複排除されたデータと重複排除されていないデータをクラウド・コンテナ・ストレージ・プールに保管して、必要に応じてデータをリストアします。	クラウド・ストレージにデータをコピーします。最初のコピー操作では、フルバックアップ・コピーが作成されます。以降のコピーは差分です。	<p>以下のいずれかのプロバイダーを選択してください。</p> <ul style="list-style-type: none"> • 178 ページの『Amazon S3 オブジェクト・ストレージの追加』 • 179 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』 • 181 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』 • 182 ページの『S3 互換オブジェクト・ストレージの追加』

Amazon S3 オブジェクト・ストレージの追加

Amazon Simple Storage Service (S3) をバックアップ・ストレージ・プロバイダーとして IBM Spectrum Protect Plus に追加すると、Amazon S3 ストレージへのコピー操作を可能にすることができます。

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、[205 ページの『アクセス・キーの追加』](#)を参照してください。

クラウド・ストレージ・バケットが IBM Spectrum Protect Plus データ用に作成されていることを確認してください。バケットの作成手順については、[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・オブジェクト・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」 > 「オブジェクト・ストレージ」をクリックします。
2. 「オブジェクト・ストレージの追加」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. 「オブジェクト・ストレージの登録」フォームのフィールドに入力します。

名前

クラウド・ストレージの識別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

ストレージ用に以前入力されたキーを選択する場合にこのオプションを有効にします。次にそのキーを「**キーの選択**」リストから選択します。

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。

Deep Archive を有効にする

オプションとして、このオプションを選択すると、Amazon S3 Glacier Deep Archive ストレージ・クラスが有効になります。

5. 「**バケットの取得**」をクリックして IBM Spectrum Protect Plus を AWS に接続して、使用可能なバケットのリストを取得します。
6. コピー・ターゲットとして使用する予定のバケットを選択します。
「**標準オブジェクト・ストレージ・バケット**」フィールドと「**アーカイブ・オブジェクト・ストレージ・バケット**」フィールドが表示されます。
7. 「**標準オブジェクト・ストレージ・バケット**」フィールドで、コピーのターゲットにするバケットを選択します。
8. オプション: 「**アーカイブ・オブジェクト・ストレージ・バケット**」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、[11 ページの『2 次バックアップ・ストレージへのコピー・スナップショット』](#)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。
9. 「**Deep Archive**」を選択して、Amazon S3 Glacier Deep Archive バケットを長期アーカイブ用に登録します。
10. 「**登録**」をクリックして、操作を完了します。
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、 228 ページの『ハイパーバイザー、データベース、およびファイル・システムの 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、 239 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 にコピー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、[205 ページの『アクセス・キーの追加』](#)および [206 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。

IBM Cloud Object Storage (COS) にバケットを作成する場合、コピーまたはアーカイブに使用されるバケットを作成するときに、「**アーカイブ・ルールの追加**」および「**有効期限ルールの追加**」の両方が選択されていないことを確認してください。これは、ジョブが IBM Spectrum Protect Plus で実行しようとしたときに、「バケットのライフサイクル構成がサポートされていません (bucket has an unsupported lifecycle configuration)」というエラーを出して失敗する可能性があります。「**保存ポリシーの追加**」オプションは、コピーに使用されるバケットに対して設定できますが、アーカイブに使用されるバケットには設定しないでください。

コールド・ボールト・バケットのタイプを使用する必要があるのは、アーカイブ時のみです。これは最も低コストのオプションであり、アクセスが最小限であるデータの長期保存に最適であると記述されているためです。

IBM Cloud Object Storage (COS) を追加する場合、アクセス・キーと秘密鍵を取得する方法は、デプロイメント・モデルによって異なります。オンプレミスの場合、鍵は IBM COS Manager Console から取得できます。IBM COS IaaS の場合、鍵は、サービス・アカウントの作成時に作成され、SoftLayer ポータルから取得できます。IBM COS (COS as a Service) を使用する場合、デフォルトではアクセス・キーと秘密鍵は作成されません。サービス・アカウントが作成されるときに、「**HMAC 資格情報を含める**」ボックスにチェック・マークを付け、「**インラインの構成パラメーターの追加**」テキスト域に `{"HMAC":true}` を追加します。

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」 > 「オブジェクト・ストレージ」をクリックします。
2. 「オブジェクト・ストレージの追加」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. 「オブジェクト・ストレージの登録」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、「**キーの選択 (Select a key)**」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、コピー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、「**標準オブジェクト・ストレージ・バケット**」フィールドと「**アーカイブ・オブジェクト・ストレージ・バケット**」フィールドが表示されます。
6. 「**標準オブジェクト・ストレージ・バケット**」フィールドで、コピー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・オブジェクト・ストレージ・バケット**」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、[11 ページの『2 次バックアップ・ストレージへのコピー・スナップショット』](#)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、 228 ページの『ハイパーバイザー、データベース、およびファイル・システムの 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、 239 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 ストレージにコピー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」 > 「オブジェクト・ストレージ」をクリックします。
2. 「オブジェクト・ストレージの追加」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. 「オブジェクト・ストレージの登録」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、「**キーの選択 (Select a key)**」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、コピー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、「**標準オブジェクト・ストレージ・バケット**」フィールドと「**アーカイブ・オブジェクト・ストレージ・バケット**」フィールドが表示されます。
6. 「**標準オブジェクト・ストレージ・バケット**」フィールドで、コピー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・オブジェクト・ストレージ・バケット**」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、[11 ページの『2 次バックアップ・ストレージへのコピー・スナップショット』](#)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、 228 ページの『ハイパーバイザー、データベース、およびファイル・システムの 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、 239 ページの『SLA ポリシーの編集』 を参照してください。

S3 互換オブジェクト・ストレージの追加

データを Amazon Simple Storage Service (S3) オブジェクト・ストレージおよび IBM Cloud Object Storage にバックアップするのに加えて、他の S3 互換オブジェクト・ストレージ・プロバイダーにデータをバックアップすることもできます。実稼働環境で他の S3 互換オブジェクト・ストレージにデータをバックアップする前に、そのオブジェクト・ストレージが IBM Spectrum Protect Plus での使用を検証済みであることを確認してください。

始める前に

ヒント:

互換オブジェクト・ストレージ・プロバイダーについては、[技術情報 108714](#) を参照してください。

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、[205 ページの『アクセス・キーの追加』](#)を参照してください。

クラウド・ストレージ・バケットが使用可能であることを確認します。クラウド・ストレージ・バケットについて詳しくは、[S3 互換ストレージ・プロバイダーの資料](#)を参照してください。

手順

S3 互換クラウド・ストレージをバックアップ・ターゲット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**」 > 「**オブジェクト・ストレージ**」をクリックします。
2. 「**オブジェクト・ストレージの追加**」をクリックします。
3. 「**プロバイダー**」リストから「**S3 互換ストレージ (S3 Compatible Storage)**」を選択します。

4.「オブジェクト・ストレージの登録」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入力します。

既存のアクセス・キーを使用する

ストレージ用に以前入力されたキーを選択する場合にこのオプションを有効にします。次にそのキーを「**キーの選択**」リストから選択します。

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の分かりやすい名前を入力します。

アクセス・キー

S3 互換アクセス・キーを入力します。アクセス・キーの取得方法については、S3 互換ストレージ・プロバイダーの資料を参照してください。

秘密鍵

S3 互換秘密鍵を入力します。アクセス・キーの取得方法については、S3 互換ストレージ・プロバイダーの資料を参照してください。

証明書

該当するオプションを選択して、S3 互換ストレージ用の証明書を追加します。

アップロード

証明書をアップロードするには、「**参照**」をクリックして証明書を見つけて選択します。「**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、その証明書をテキスト域に貼り付けます。「**作成**」をクリックします。

既存の使用

証明書が存在する場合、その証明書を「**証明書の選択**」リストから選択します。

5.「**バケットの取得**」をクリックして、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、「**標準オブジェクト・ストレージ・バケット**」フィールドと「**アーカイブ・オブジェクト・ストレージ・バケット**」フィールドが表示されます。

6.「**標準オブジェクト・ストレージ・バケット**」フィールドで、バックアップ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・オブジェクト・ストレージ・バケット**」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、[11 ページの『2 次バックアップ・ストレージへのコピー・スナップショット』](#)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 互換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、 228 ページの『ハイパーバイザー、データベース、およびファイル・システムの 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、 239 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」 > 「オブジェクト・ストレージ」をクリックします。
2. オブジェクト・ストレージ・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。「オブジェクト・ストレージの更新 (Update Object Storage)」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」 > 「オブジェクト・ストレージ」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・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・サーバーにデータをコピー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・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。データを磁気テープにコピーするには、IBM Spectrum Protect サーバー バージョン 8.1.8 以降が必要です。

IBM Spectrum Protect サーバーにコピーされた IBM Spectrum Protect Plus データをターゲット・サーバーに複製できます。ただし、IBM Spectrum Protect Plus は、後続の IBM Spectrum Protect サーバーの複製操作を認識しないため、複製されたデータをターゲットの IBM Spectrum Protect サーバーから IBM Spectrum Protect Plus にリストアすることはできません。

IBM Spectrum Protect にデータをコピーまたはアーカイブするための構成

IBM Spectrum Protect Plus データを IBM Spectrum Protect サーバーにコピーまたはアーカイブする予定の場合、3 種類の構成が考えられます。どの構成を選択するかは、どのシナリオがデータ保護のニーズに当てはまるかによって決まります。それぞれのシナリオに、セットアップを完了するために IBM Spectrum Protect Plus と IBM Spectrum Protect サーバーの両方の環境で実行する必要があるステップがあります。

IBM Spectrum Protect を構成するためのタスク

IBM Spectrum Protect サーバーは、IBM Spectrum Protect Plus サーバーと通信して、バックアップ操作とリストア操作の要求を処理できるように構成する必要があります。Amazon Simple Storage Service (S3) プロトコルにより、2 つのサーバー間の通信が可能になります。

ユーザー・シナリオ	目的	ステップ
1 日に 1 回以下の頻度で標準オブジェクト・ストレージへのコピーを実行する場合の標準オブジェクト・ストレージへのコピー。	標準オブジェクト・ストレージにデータをコピーします。最初のコピー操作では、フルバックアップ・コピーが作成されます。以降のコピーは差分です。バックアップおよびリカバリーの時間を比較的短くして、長期的な保護、コスト、テープ・ストレージによって提供されるセキュリティ上のメリットは必要でない場合は、標準オブジェクト・ストレージにデータをコピーすると便利です。	データを IBM Spectrum Protect サーバーの標準オブジェクト・ストレージにコピーするには、クラウド・コンテナまたはディレクトリー・コンテナのストレージ・プールを作成して、IBM Spectrum Protect のオブジェクト・エージェント・コンポーネントをセットアップする必要があります。オブジェクト・エージェントの追加は必須のステップです。必要なストレージ・プールのセットアップのほか、 ここにリストされているステップ 2 から 4 に従ってください 。
週に 1 回以下の頻度でテープ・ストレージへのデータのフルコピーを作成する場合のテープへのコピー。 重要: 週に 1 回未満の頻度でテープにデータをアーカイブすることはできません。この理由から、アーカイブ・データを災害復旧に役立つコピーとは見なさないでください。	テープにデータをコピーすると、コピー・プロセスの時点でデータのフルコピーが作成されます。テープにデータをコピーすると、セキュリティ上のメリットが増えます。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。ただし、これらのストレージ・タイプへのコピーには完全なデータ・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。	テープにデータをコピーするには、テープ用のクラウド・コンテナまたはディレクトリー・コンテナのストレージ・プールと IBM Spectrum Protect サーバー上のコールド・データ・キャッシュ・ストレージ・プールを作成する必要があります。オブジェクト・エージェントの追加は必須のステップです。 ここにリストされているステップ 1 から 4 に従ってください 。
標準オブジェクト・ストレージと長期のテープへのコピーの両方の組み合わせ。	IBM Spectrum Protect サーバー上の差分バックアップでデータを保護するとともに、長期的なセキュリティのためにテープにデータを保存します。	これは上記のケースの組み合わせです。データはテープに保管され、データは IBM Spectrum Protect サーバー上の標準オブジェクト・ストレージにも保管されます。両方のシナリオに必要なデータ・ストレージ・プールのセットアップのほか、オブジェクト・エージェントの作成が必須です。

IBM Spectrum Protect Plus と IBM Spectrum Protect サーバーの間のデータ転送通信のセットアップと構成に必要な 4 つのステップは以下のとおりです。

1. テープにデータをコピーするためのストレージ・プールをセットアップする場合は、ステップ 1 に従います。IBM Spectrum Protect Operations Center を使用して、IBM Spectrum Protect サーバー上にストレージ・プールを作成します。手順については、[186 ページの『ステップ 1: テープにデータをコピーするためのテープ・ストレージ・プールおよびコールド・データ・キャッシュ・ストレージ・プールの作成』](#)を参照してください。このステップが必要になるのは、週に 1 回以下の頻度でコピーを使用してアーカイブするために IBM Spectrum Protect を設定する場合のみです。

2. 1つ以上のストレージ・プールを指すポリシー・ドメインを作成します。ポリシー・ドメインは、IBM Spectrum Protect Plus のバックアップ・サービスを制御するルールを定義します。手順については、[188 ページの『ステップ 2: オブジェクト・ポリシー・ドメインの構成』](#)を参照してください。
3. 標準ストレージ・プールまたはテープにデータをコピーする場合は、IBM Spectrum Protect サーバーに標準ストレージ・プールを追加する必要があります。手順については、[190 ページの『ステップ 3: 標準オブジェクト・ストレージのセットアップ』](#)を参照してください。
4. IBM Spectrum Protect サーバーにオブジェクト・エージェントを追加します。オブジェクト・エージェントは、IBM Spectrum Protect Plus サーバーと IBM Spectrum Protect サーバー の間のゲートウェイを提供します。手順については、[193 ページの『ステップ 4: データをコピーするためのオブジェクト・エージェントの追加』](#)を参照してください。
5. セットアップを完了するには、IBM Spectrum Protect サーバーにオブジェクト・クライアントを追加する必要があります。オブジェクト・クライアントは、IBM Spectrum Protect Plus サーバーを識別して、IBM Spectrum Protect サーバーでオブジェクトを保管できるようにします。IBM Spectrum Protect Plus に使用したのと同じ資格情報がオブジェクト・クライアントに使用されます。このオブジェクト・クライアントは、ステップ 2 でセットアップしたポリシー・ドメインに関連付けられます。オブジェクト・クライアントをセットアップする 手順については、[194 ページの『ステップ 5: データをコピーするためのオブジェクト・クライアントの追加および構成』](#)を参照してください。

ヒント: あるいは、以下のトピックで説明しているように、**DEFINE STGPOOL** コマンドを入力してストレージ・プールを作成します。

次の作業

1. IBM Spectrum Protect ストレージに必要なタスクを完了した後、IBM Spectrum Protect サーバーを IBM Spectrum Protect Plus に追加する必要があります。その方法については、[196 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・サーバーの登録』](#)の手順を参照してください。
2. その手順が完了した後、IBM Spectrum Protect サーバーをバックアップ・ストレージ・ターゲットとして定義する SLA ポリシーを作成できます。必要なタイプのポリシーを選択するための詳細情報については、[184 ページの『IBM Spectrum Protect にデータをコピーまたはアーカイブするための構成』](#)を参照してください。

ステップ 1: テープにデータをコピーするためのテープ・ストレージ・プールおよびコールド・データ・キャッシュ・ストレージ・プールの作成

アーカイブの目的で IBM Spectrum Protect Plus から IBM Spectrum Protect サーバーにデータをコピーする前に、オブジェクト・エージェント・サービスを構成する必要があります。データの長期アーカイブの場合は、コールド・データ・ストレージ・プールを構成する必要があります。IBM Spectrum Protect サーバー上のテープにデータをアーカイブする 予定がない場合は、このステップをスキップできます。

このタスクについて

始める前に、サイジング・ツールと Blueprints を使用して、コールド・キャッシュ・ストレージ必要量のサイズを設定したことを確認してください。それを行う方法については、[Blueprints](#) を参照してください。その他の有用なリンクとビデオについては、[1 ページの『IBM Spectrum Protect Plus のデプロイメント・ストーリーボード』](#)を参照してください。

S3 Glacier ストレージ・クラスが指定されたオブジェクト・クライアント・データは頻繁にアクセスされません。コールド・データ と呼ばれることが多いこのデータをテープ・ストレージにコピーできるようにするために、オブジェクト・データを処理するための要件を満たすストレージ・プールにデータが一時的に書き込まれます。その後、データはテープ装置または VTL に移動されます。このストレージ・プールは、コールド・データ・キャッシュ・ストレージ・プール と呼ばれ、オブジェクト・クライアントにポリシー・ドメインに割り当てられます。コールド・データ・キャッシュ・ストレージ・プールへの書き込みまたはコールド・データ・キャッシュ・ストレージ・プールからのリストアを行えるのは、オブジェクト・クライアントからのデータのみです。

手順

Operations Center を使用しない場合は、**define stgpool** コマンドを使用できます。このコマンドは、次のように定義できます。

```
define stgpool NAME
stgtype=colddatacache
```

注：オブジェクト・ストレージ用に標準プールを構成するには、以下のステップに従ってください。ただし、ストレージ・プールのタイプを定義する際、「Standard」を選択してください。

オブジェクト・クライアントから物理テープ・メディアまたは VTL にデータをコピーするように IBM Spectrum Protect サーバー を構成するには、以下の構成ステップを実行します。

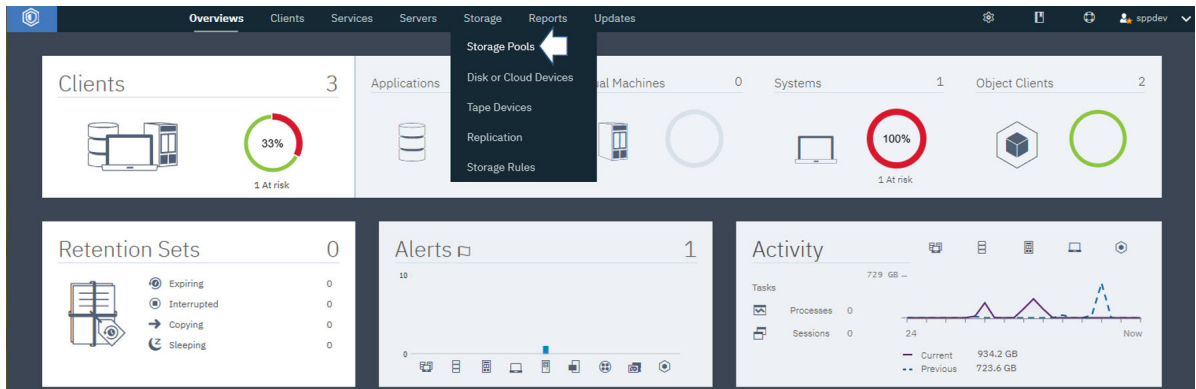
1. IBM Spectrum Protect サーバー で、テープ装置または VTL を表す 1 次ストレージ・プールを構成します。この 1 次ストレージ・プールは、コピーするオブジェクト・データの宛先となります。

後で、コールド・データ・キャッシュ・ストレージ・プールを定義するときに、このテープ・プールをコールド・データ・キャッシュ・プールの次のストレージ・プールとして指定する必要があります。

制約事項：テープ・ストレージ・プールには、以下の制約事項が適用されます。

- ・テープ・ストレージ・プールとの間でオブジェクト・クライアント・データを複製することはできません。
- ・テープ・ストレージ・プールを重複排除することはできません。
- ・次のストレージ・プールをテープ・ストレージ・プールに指定することはできません。

- a) Operations Center メニュー・バーで、「ストレージ」 > 「ストレージ・プール」をクリックします。



- b) 「ストレージ・プール」 ページで、「ストレージ・プール」  をクリックします。

- c) 「ストレージ・プールの追加」ウィザードで、「オブジェクト・クライアント」を選択して、オブジェクト・クライアントがデータをテープにコピーできるようにします。

2. ウィザードのステップに従って、コールド・データ・キャッシュ・ストレージ・プールを構成します。コールド・データ・キャッシュ・ストレージ・プールは、ディスク上の 1 つ以上のファイル・システム・ディレクトリで構成されます。これは、オブジェクト・クライアントとテープ装置または VTL の間の中間ストレージ・プールであり、テープ装置または VTL を表す 1 次順次アクセス・ストレージ・プールにリンクされます。一時ディスク・ストレージ用の 1 つ以上の既存のファイル・システム・ディレクトリと、テープ装置または VTL を表す 1 次順次アクセス・ストレージ・プールを識別します。
3. 「コールド・データ・キャッシュ」 ページで、ディスク・ストレージ用に 1 つ以上の既存のファイル・システム・ディレクトリを指定します。サーバーのオペレーティング・システムで 사용되는構文に適合した完全修飾パス名を入力します。

例えば、c:\¥temp¥dir1¥ (Microsoft Windows の場合) または /tmp/dir1/ (UNIX の場合) のように入力します。

オブジェクト・データは、ファイル・システム・ディレクトリ内の順次ボリュームに保管されます。オブジェクト・クライアントは、アクセス頻度の低いデータ、つまりコールド・データを物理磁気テープ・メディアまたは VTL にコピーすることができます。オブジェクト・クライアントがコールド・デー

データをコピーするときに、データは最初にコールド・データ・キャッシュに保管されます。その後、データは、マイグレーション遅延なしで、物理磁気テープ・メディアまたは VTL を表す 1 次テープ・ストレージ・プールにマイグレーションされます。データがテープにマイグレーションされた後、そのデータはコールド・データ・キャッシュから削除されます。コールド・データ・キャッシュは、コールド・データをオブジェクト・クライアントにリストアするためのステージング領域として使用されます。リストア操作中に、データはコールド・データ・キャッシュにコピーされます。データは、オブジェクト・クライアントによって指定された期間、コールド・データ・キャッシュに残ります。データは、テープまたは VTL から直接ではなく、コールド・データ・キャッシュからオブジェクト・クライアントにリストアされます。

パフォーマンス向上のために複数のディレクトリーを指定する場合は、それらのディレクトリーが別個の物理ボリュームに対応していることを確認してください。コールド・データ・キャッシュは一時ストレージとして使用されますが、データをテープにマイグレーションする前に、オブジェクト・クライアントからコピーされたデータを保持できるだけの大きさが必要です。また、オブジェクト・クライアントによって指定された期間、リストア操作中にデータを保持できるだけの大きさでなければなりません。

次のタスク

コールド・データ・キャッシュ・ストレージ・プールの構成が完了したら、オブジェクト・ドメインを作成します。それを行う方法については、[188 ページの『ステップ 2: オブジェクト・ポリシー・ドメインの構成』](#)を参照してください。

ステップ 2: オブジェクト・ポリシー・ドメインの構成

IBM Spectrum Protect Plus から IBM Spectrum Protect サーバーにデータをコピーする前に、オブジェクト・ポリシー・ドメインを作成して構成する必要があります。ポリシー・ドメインは、IBM Spectrum Protect Plus のバックアップ・サービスを制御するルールを定義します。ディレクトリー・コンテナー・ベースまたはクラウド・コンテナー・ベースのストレージをコピーに使用する標準ストレージ・プールを追加して、テープへのデータのコピーまたはデータのアーカイブを行う場合にはコールド・プールを追加する必要があります。

手順

1. データをコピーするために使用する予定のポリシー・ドメインの設定を確認します。IBM Spectrum Protect サーバー V8.1.8 以降で定義または更新されたオブジェクト・クライアントは、**DEFINE OBJECTDOMAIN** コマンドを使用して作成されたポリシー・ドメインに割り当てする必要があります。オブジェクト・クライアント・ノードは、ノードが **REGISTER NODE** コマンドまたは **UPDATE NODE** コマンドを使用して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。

制約事項: IBM Spectrum Protect サーバー V8.1.8 以降、すべての新規のオブジェクト・クライアント・ノードをオブジェクト・ポリシー・ドメインに割り当てする必要があります。

V8.1.8 より前の非オブジェクト・ポリシー・ドメインに割り当てられたオブジェクト・クライアント・ノードの場合は、サーバーを IBM Spectrum Protect サーバー V8.1.8 にアップグレードした後、割り当てを更新する必要はありません。ただし、オブジェクト・クライアント・ノードのドメインを更新する必要がある場合は、ノードをオブジェクト・ポリシー・ドメインに割り当てする必要があります。

2. コピー操作用のポリシー・ドメインを指定する場合の以下の考慮事項を確認してください。
 - IBM Spectrum Protect サーバー の場合、ポリシー・ドメインには、標準ストレージ・プール (クラウド・コンテナーまたはディレクトリー・コンテナーのストレージ・プール)、コールド・データ・キャッシュ・ストレージ・プール、あるいは標準とコールド・データ・キャッシュの両方のストレージ・プールの管理クラスを指定できます。

ただし、IBM Spectrum Protect Plus からデータをコピーするには、クラウド・コンテナーまたはディレクトリー・コンテナーのストレージ・プールにデータをコピーするのか、あるいは物理テープ・メディアまたは仮想テープ・ライブラリー (VTL) に保管するためにコールド・データ・キャッシュ・ストレージ・プールにデータをコピーするのかに応じて、以下の管理クラスを指定する必要があります。

- クラウド・コンテナまたはディレクトリー・コンテナのストレージ・プールにデータをコピーするには、次の例に示すように、**STANDARDPOOL** パラメーターを使用して、ポリシー・ドメインに対してストレージ・プールを定義します。

```
define objectdomain mydomain standardpool=hotpool
```

- コールド・データ・キャッシュ・ストレージ・プールにデータをコピーするには、ポリシー・ドメインに標準プールとコールド・プールの両方を指定する必要があります。標準プールは、リストア操作およびその他の IBM Spectrum Protect Plus 操作に使用されるメタデータを保管するために必要です。ポリシー・ドメインに対してコールド・データ・キャッシュ・ストレージ・プールを定義するには、次の例に示すように、**COLDPOOL** パラメーターを使用します。

```
define objectdomain mydomain standardpool=hotpool coldpool=coldpool
```

- 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。ポリシー・ドメインを定義する際、以下のストレージ管理ポリシーが自動的に指定されます。
 - 「データが存在するバージョン」フィールドは 1 に設定されます。
 - 「非活動バックアップ・バージョン保存」フィールドおよび「バックアップ・バージョンのみ保存」フィールドは 0 に設定されます。
- IBM Spectrum Protect Plus 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。

例: IBM Spectrum Protect Plus コピー操作のポリシー・ドメインに関する詳細情報の表示

ポリシー・ドメインは、作成時に管理クラスおよびコピー・グループが割り当てられています。**QUERY COPYGROUP** コマンドを使用して、ポリシー・ドメインの宛先ストレージ・プールに関する情報を表示できます。次の例で、ポリシー・ドメイン名は XYZ です。宛先ストレージ・プールは、HOTPPOOL および COLDPOOL です。

```
query copygroup xyz standard f=d
```

```

Policy Domain Name: XYZ
Policy Set Name: STANDARD
Mgmt Class Name: COLD
Copy Group Name: STANDARD
Copy Group Type: Backup
Versions Data Exists: 1
Versions Data Deleted: 1
Retain Extra Versions: 0
Retain Only Version: 0
Copy Mode: Modified
Copy Serialization: Shared Static
Copy Frequency: 0
Copy Destination: COLDPOOL
Table of Contents (TOC) Destination:
Last Update by (administrator): SERVER_CONSOLE
Last Update Date/Time: 05/22/20 17:03:46
Managing profile:
Changes Pending: No

Policy Domain Name: XYZ
Policy Set Name: STANDARD
Mgmt Class Name: STANDARD
Copy Group Name: STANDARD
Copy Group Type: Backup
Versions Data Exists: 1
Versions Data Deleted: 1
Retain Extra Versions: 0
Retain Only Version: 0
Copy Mode: Modified
Copy Serialization: Shared Static
Copy Frequency: 0
Copy Destination: HOTPOOL
Table of Contents (TOC) Destination:
Last Update by (administrator): SERVER_CONSOLE
Last Update Date/Time: 03/05/20 22:15:18
Managing profile:
Changes Pending: No

```

次のタスク

オブジェクト・ドメインを作成した後、次のステップの [190 ページの『ステップ 3: 標準オブジェクト・ストレージのセットアップ』](#)に進みます。

ステップ 3: 標準オブジェクト・ストレージのセットアップ

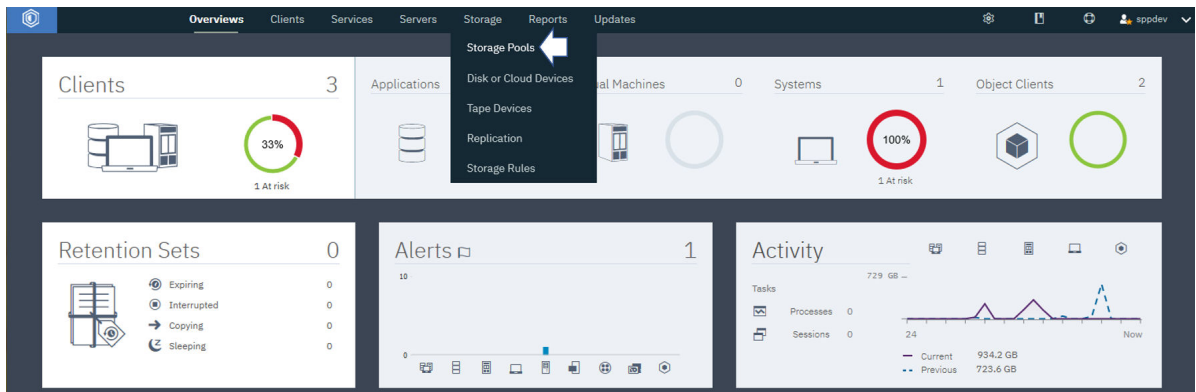
IBM Spectrum Protect Plus から IBM Spectrum Protect サーバーにデータをコピーするための標準オブジェクト・ストレージをセットアップするには、Operations Center にログインして、ストレージ・プールをセットアップするための手順に従います。Operations Center のウィザードを使用して、オブジェクト・エージェント・サービスを作成するための手順に従い、プロセスを完了してください。

始める前に

始める前に、標準ストレージ用またはテープへのコピー用にストレージ・プールをセットアップする必要があります。テープにコピーする場合は、コールド・データ・キャッシュ・ストレージ・プールをセットアップする必要があり、標準オブジェクト・ストレージの場合は、必要に応じてストレージ・プールを作成して構成する必要があります。コールド・データ・キャッシュ・ストレージ・プールのセットアップ方法については、[186 ページの『ステップ 1: テープにデータをコピーするためのテープ・ストレージ・プールおよびコールド・データ・キャッシュ・ストレージ・プールの作成』](#)を参照してください。

手順

1. 以下の手順を実行して、ディレクトリー・コンテナ・ストレージ・プールを作成します。
 - a) Operations Center メニュー・バーで、「ストレージ」 > 「ストレージ・プール」をクリックします。



b) 「ストレージ・プール」 ページで、「ストレージ・プール」  をクリックします。

c) 「ストレージ・プールの追加」ウィザードのステップを実行します。

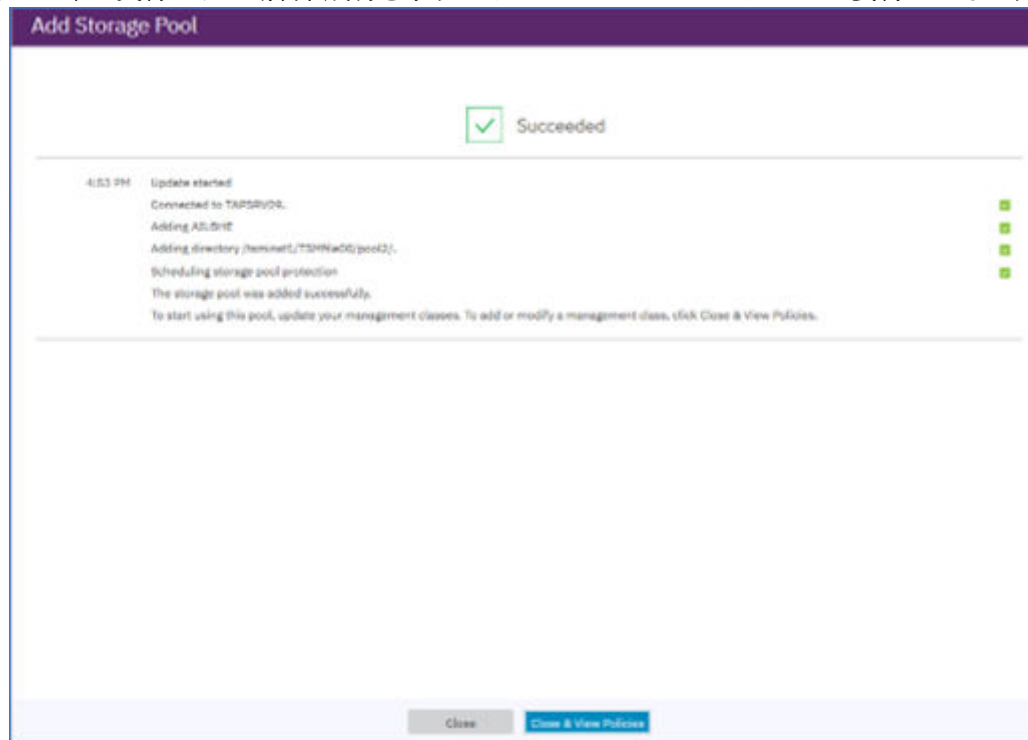
ヒント：コンテナー・ベースのストレージのタイプとして「ディレクトリー」を選択し、+ アイコンを使用してディレクトリーを追加します。「次へ」をクリックして先に進みます。

d) 「保護プール」の要約を確認して、「次へ」をクリックします。

e) 必要なオーバーフロー・プールを指定します。

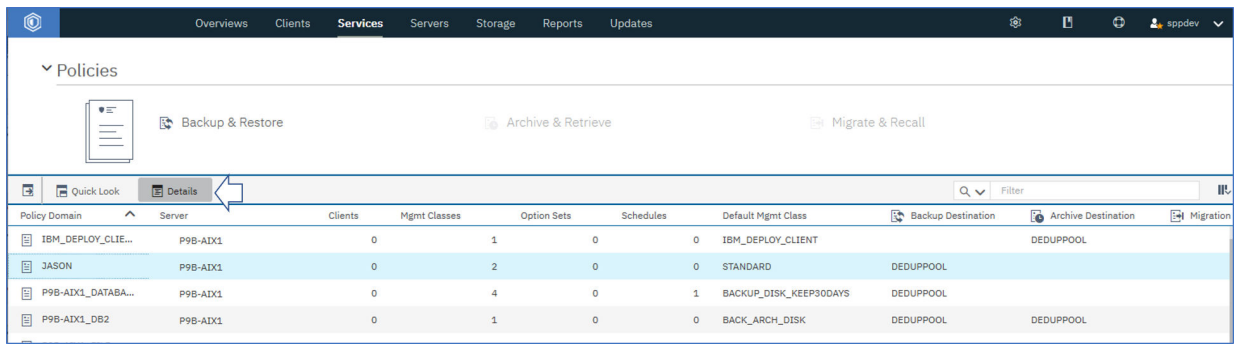
f) 「ストレージ・プールの追加」をクリックして、ストレージ・プールの作成を完了します。

操作が正常に実行された場合、成功を示すアイコンがストレージ・プールの要約とともに表示されま

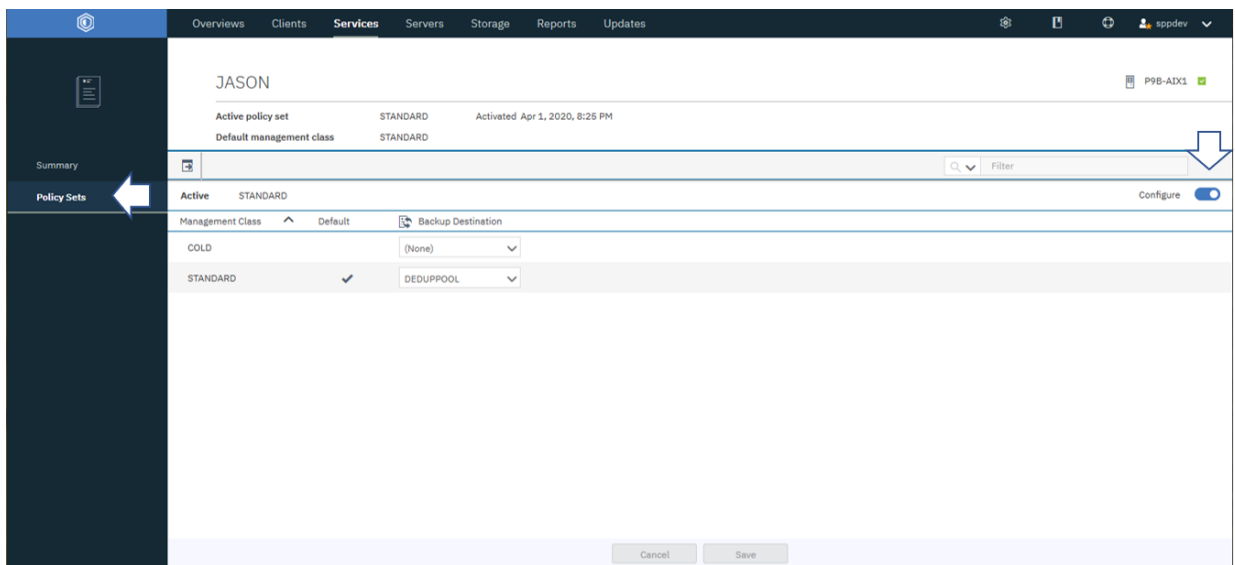


す。

2. 「サービス」 > 「ポリシー」 ページで、ポリシーを選択して、「詳細」をクリックします。



- 以下のステップを実行して、既存のドメイン・ポリシーを編集することができます。
 - a) 表の「バックアップの宛先」フィールドを編集することにより、新規プールを使用するように1つ以上の管理クラスを更新します。
 - b) 「保存」をクリックします。
- あるいは、**define objectdomain** コマンドを実行して、新規ドメインを作成することができます。詳しくは、前のステップの [188 ページ](#) の『ステップ 2: オブジェクト・ポリシー・ドメインの構成』を参照してください。
- 3. 「詳細」 ページで、「ポリシー・セット」をクリックします。「構成」トグルをクリックして、ポリシー・セットを編集可能にします。



4. 「バックアップの宛先」を新しく作成したストレージ・プールに変更するか、新規のストレージ・プー

ルを指定するために新規管理クラス  **Management Class** を追加します。

5. 「活動化」をクリックします。
アクティブ・ポリシー・セットを変更すると、データ損失が起こる可能性があります。変更が行われる前に、アクティブ・ポリシー・セットと新規ポリシー・セットの相違点の概要が表示されます。
6. 2つのポリシー・セットの中に対応する管理クラスの相違点を確認して、クライアント・ファイルに対する影響を検討します。現在のアクティブ・ポリシー・セットの管理クラスにバインドされているクライアント・ファイルは、活動化の後、新規ポリシー・セット内の同じ名前を持つ管理クラスにバインドされます。
7. 現在のアクティブ・ポリシー・セットの中で、新規ポリシー・セットに対応するものがない管理クラスを特定して、クライアント・ファイルに対する影響を検討します。これらの管理クラスにバインドされているクライアント・ファイルは、活動化の後、新規ポリシー・セット内のデフォルト管理クラスによって管理されます。

8. ポリシー・セットによって実装される変更内容を許容できる場合は、「これらの更新がデータ損失を引き起こす可能性があることを理解している (I understand that these updates can cause data loss)」チェック・ボックスを選択して、「活動化」をクリックします。

次のタスク

作成した 1 つ以上のストレージ・プール用のオブジェクト・クライアントを作成して構成します。詳しくは、194 ページの『ステップ 5: データをコピーするためのオブジェクト・クライアントの追加および構成』を参照してください。

ステップ 4: データをコピーするためのオブジェクト・エージェントの追加

IBM Spectrum Protect Plus から IBM Spectrum Protect サーバー にデータをコピーする前に、オブジェクト・エージェントを追加および構成する必要があります。このステップは、オブジェクト・ストレージへのデータのアーカイブまたはデータのコピーを行うための IBM Spectrum Protect サーバーでの IBM Spectrum Protect Plus のセットアップにおける 4 番目のステップです。

始める前に

オブジェクト・クライアントの作成を開始する前に、以下のステップが完了していることを確認してください。

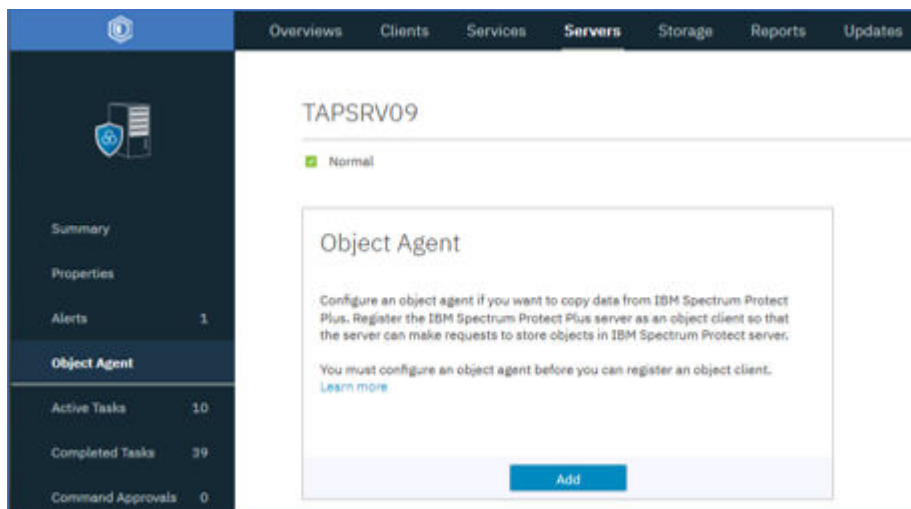
1. インスタンス・ユーザー ID を使用して IBM Spectrum Protect サーバーにログインしていることを確認します。
2. 標準ストレージ用またはテープへのコピー用にストレージ・プールをセットアップしてあることを確認します。手順については、186 ページの『ステップ 1: テープにデータをコピーするためのテープ・ストレージ・プールおよびコールド・データ・キャッシュ・ストレージ・プールの作成』または 190 ページの『ステップ 3: 標準オブジェクト・ストレージのセットアップ』を参照してください。
3. オブジェクト・ドメインを作成してあることを確認します。

このタスクについて

この手順は、IBM POWER8® 以降のサーバーで稼働している IBM AIX オペレーティング・システムの AIX バージョン 7.2 TL 1 および SP 4 以降に IBM Spectrum Protect サーバーがインストールされている環境に基づいています。(旧バージョンへのリンク)

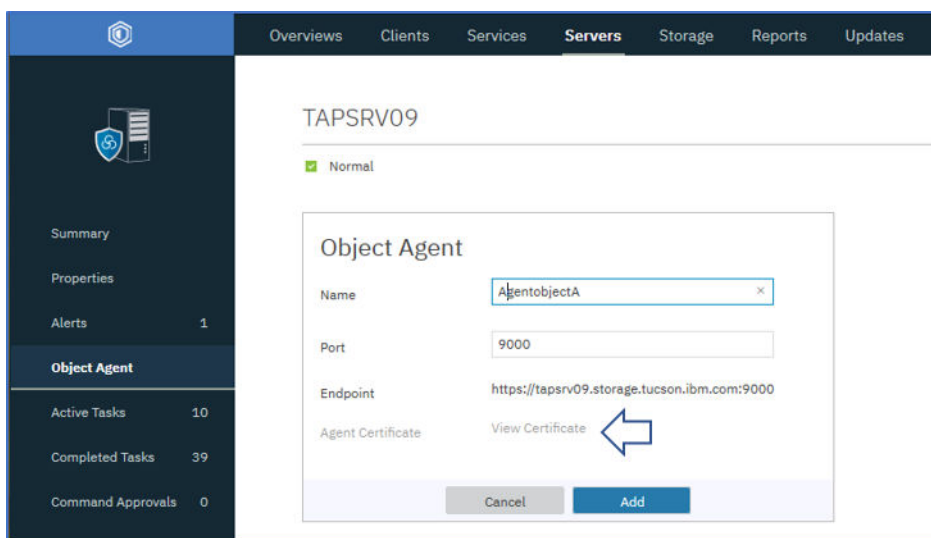
手順

1. Operations Center メニュー・バーで、「サーバー」 **Servers** をクリックします。
2. サーバーを選択して、「詳細」をクリックします。
3. ナビゲーション・ペインで、「オブジェクト・エージェント」をクリックして、「追加」をクリックし、オブジェクト・エージェントを追加します。



ヒント: コマンド・ラインを使用している場合は、**DEFINE SERVER** コマンドを実行して、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。コマンドの出力の指示に従います。これらのアクションが完了すると、IBM Spectrum Protect サーバー をホスティングしているシステムでオブジェクト・エージェント・サービスが自動的に開始されます。

- 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。



- 次の例のように、ウィザードからコピーできるコマンドを実行して、オブジェクト・エージェント・サービスをインストールします。

```
[root@servername-os: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPP0BJAGENT/spObjectAgent_SPP0BJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Installed and started system service as
nameportnumberobjectagentname
```

以下に例を示します。

```
[root@p9b-aix1: /]# /opt/tivoli/tsm/server/bin/spObjectAgent service install
/home/tsminst1/tsminst1/SPP0BJAGENT/spObjectAgent_SPP0BJAGENT_1500.config
2020-03-31 15:50:07.631021 I | Installed and started system service as spoa9000SPP0BJAGENT
```

- startObjectAgent** コマンドを実行して、オブジェクト・エージェント・サービスを開始し、構成を完了します。以下に、AGENTOBJECTA オブジェクト・エージェントの例を示します。

```
"/opt/tivoli/tsm/server/bin/spObjectAgent" service install
"/home/tsminst1/tsminst1/AGENTOBJECTA/spObjectAgent_AGENTOBJECTA_1500.config"
```

- AIX 向けの次のようなコマンドを実行して、オブジェクト・エージェント・サービスを始動時に自動的に開始するようにセットアップします。

```
spobj:2:once:/usr/bin/startsrc -s nameportnumberobjectagentname
```

以下に例を示します。

```
spobj:2:once:/usr/bin/startsrc -s spoa9000SPP0BJAGENT
```

ステップ 5: データをコピーするためのオブジェクト・クライアントの追加および構成

IBM Spectrum Protect Plus から IBM Spectrum Protect サーバー にデータをコピーする前に、オブジェクト・クライアントを構成する必要があります。このステップは、Operations Center でデータのアーカイブおよびコピーを行うための IBM Spectrum Protect サーバーのセットアップにおける最後のステップです。

始める前に

オブジェクト・クライアントの作成を開始する前に、以下のステップが完了していることを確認してください。

1. インスタンス・ユーザー ID を使用して IBM Spectrum Protect サーバーにログインしていることを確認します。
2. 標準ストレージ用またはテープへのコピー用にストレージ・プールがセットアップされ、準備ができていることを確認します。手順については、[186 ページの『ステップ 1: テープにデータをコピーするためのテープ・ストレージ・プールおよびコールド・データ・キャッシュ・ストレージ・プールの作成』](#)または [190 ページの『ステップ 3: 標準オブジェクト・ストレージのセットアップ』](#)を参照してください。
3. 開始する前にオブジェクト・ドメインおよびオブジェクト・エージェントが作成されていることを確認します。

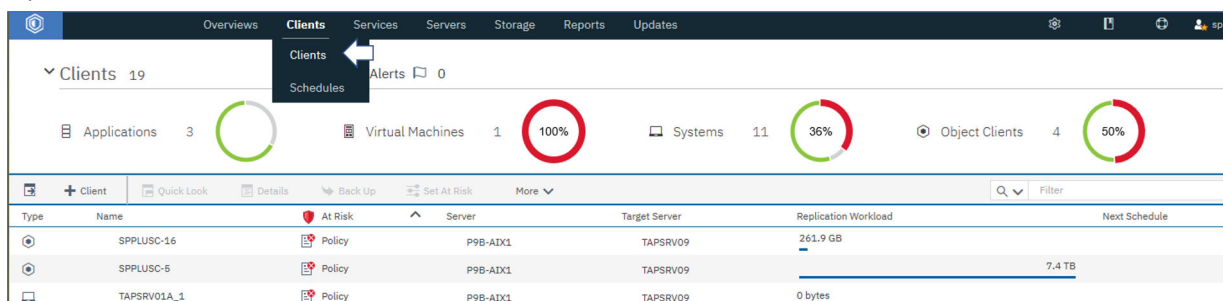
ヒント: 対応するオブジェクト・エージェントを作成する前にオブジェクト・クライアントを作成すると、対応するオブジェクト・エージェントを作成する場合、「クライアントの追加」ウィザードによりオブジェクト・エージェントの作成が強制されます。

このタスクについて

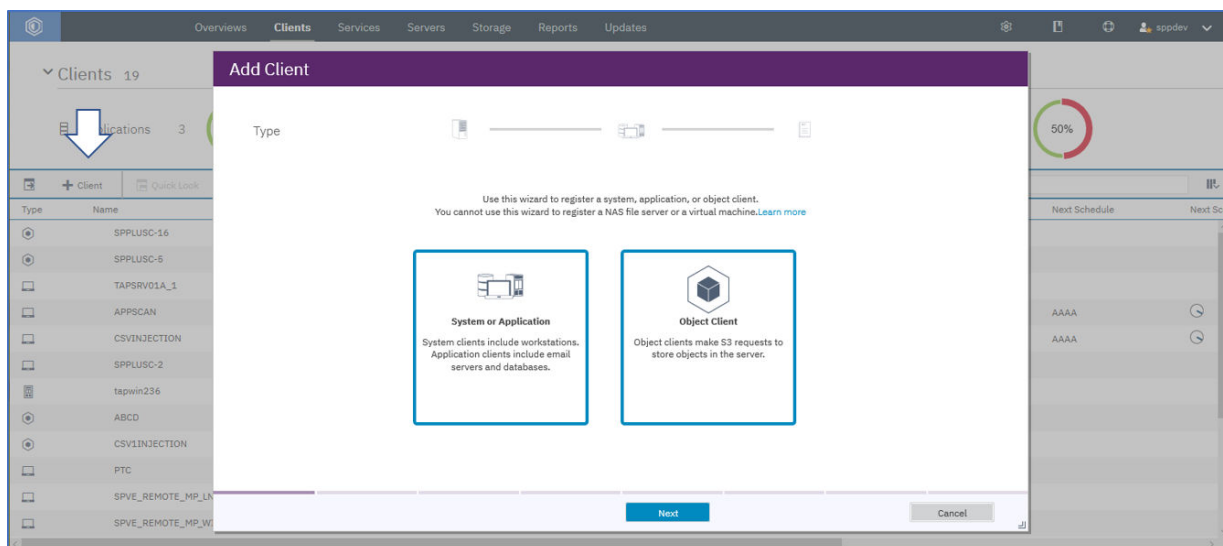
この手順は、IBM POWER8 以降のサーバーで稼働している IBM AIX オペレーティング・システムの AIX バージョン 7.2 TL 1 および SP 4 以降に IBM Spectrum Protect サーバーがインストールされている環境に基づいています。

手順

1. Operations Center メニュー・バーで、「クライアント」をクリックします。



2. 「クライアント」をクリックして、示されているようにクライアントを追加します。



3. 「オブジェクト・クライアント」を選択して、「次へ」をクリックし、「クライアントの追加」ウィザードを開始します。

ウィザードの画面では、セットアップしているクライアントに対して以下の選択と定義を行うよう求められます。

- このクライアントに対して複製を有効にすることもできます。

- ・クライアント名および連絡先名と、ウィザードの最後のステップで定義するレポート用の E メール・アドレスを割り当てる必要があります。
- ・ステップ 2 の [188 ページ](#)の『[ステップ 2: オブジェクト・ポリシー・ドメインの構成](#)』でセットアップしたポリシー・ドメインを割り当てる必要があります。
- ・指定した E メール・アドレスへの 1 日 1 回のレポートなど、クライアントに関する危険レポートを定義できます。

4. 「クライアントの追加」をクリックします。

注:

プロセスが終了した後、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、秘密アクセス・キー、および証明書が提供されます。IBM Spectrum Protect Plus は、オブジェクト・クライアントである場合は、そのエンドポイントに要求を送信し、アクセス・キー ID、秘密アクセス・キー、およびセキュア証明書の形式でこの情報を使用します。

重要: 各資格情報のコピーは安全な場所に保管するようにしてください。

ヒント: コマンド・ラインを使用する場合、**REGISTER NODE** コマンドを実行して、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。このスクリプトは、インスタンス・ユーザー ID で実行されます。

次のタスク

次のステップでは、IBM Spectrum Protect サーバーをリポジトリ・サーバーとして登録する必要があります。その方法については、[196 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・サーバーの登録](#)』を参照してください。その手順が完了すると、SLA ポリシー・ジョブを作成して、標準ストレージ用またはテープへのアーカイブ用にデータを IBM Spectrum Protect サーバーにコピー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リポジトリ・サーバーの登録

IBM Spectrum Protect Plus がデータをサーバーにコピーできるようにリポジトリ・サーバーを追加および登録します。

始める前に

リポジトリ・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、[205 ページ](#)の『[アクセス・キーの追加](#)』および [206 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・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、コピー・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。

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。

コピー保存設定は、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、コピー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および登録するには、以下のステップを実行します。

1. ナビゲーション・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・サーバー」をクリックします。

2. 「リポジトリ・サーバーの追加」をクリックします。
3. 「リポジトリ・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・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・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・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・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・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・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、 228 ページの『ハイパーバイザー、データベース、およびファイル・システムの 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、 239 ページの『SLA ポリシーの編集』 を参照してください。

関連概念

[184 ページの『IBM Spectrum Protect にデータをコピーまたはアーカイブするための構成』](#)


IBM Spectrum Protect Plus データを IBM Spectrum Protect サーバーにコピーまたはアーカイブする予定の場合、3 種類の構成が考えられます。どの構成を選択するかは、どのシナリオがデータ保護のニーズに当てはまるかによって決まります。それぞれのシナリオに、セットアップを完了するために IBM Spectrum Protect Plus と IBM Spectrum Protect サーバーの両方の環境で実行する必要があるステップがあります。

リポジトリ・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・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・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・サーバー」をクリックします。
2. 目的のリポジトリ・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・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・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・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・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・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・サーバー」をクリックします。
2. 目的のリポジトリ・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。

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」 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・アクティビティを管理するには、サイト複製操作およびコピー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 20. 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、毎日のスロットルを行う時間、またはスロットルを行う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曜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」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・アクティビティを管理するには、サイト複製操作およびコピー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。

Site

Site Properties

Name:

☒ Enable Throttle

Rate:

Schedule

	12	1	2	3	4	5	6	7	8	9	10	11	12
All													
Sunday													
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													

Sunday from 7:00 AM to 7:59 AM; Monday through Wednesday from 8:00 AM to 8:59 AM; Thursday from 1:00 AM to 1:59 AM, from 8:00 AM to 8:59 AM; Friday from 8:00 AM to 8:59 AM; Saturday from 4:00 AM to 4:59 AM, from 8:00 AM to 8:59 AM

図 21. 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、毎日のスロットルを行う時間、またはスロットルを行う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曜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

512 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 では、Lightweight Directory Access Protocol (LDAP) サーバーを使用してユーザーを管理できます。LDAP ユーザー・アカウントを作成すると、そのユーザー・アカウントをユーザー・グループに追加できます。

500 ページの『レポートのスケジューリング』

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 sAMAccountName 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

[512 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 では、Lightweight Directory Access Protocol (LDAP) サーバーを使用してユーザーを管理できます。LDAP ユーザー・アカウントを作成すると、そのユーザー・アカウントをユーザー・グループに追加できます。

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)。

送信者アドレス

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

500 ページの『[レポートのスケジューリング](#)』


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。

管理コンソールへのログイン

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インします。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、およびプロキシ設定が含まれます。

手順

管理コンソールにログインするには、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	SUPERUSER 特権を持つ IBM Spectrum Protect Plus ユーザーとしてログインするには、管理者ユーザー名とパスワードを入力します。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	システム・ユーザーとしてログインするには、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-SysXyz です。初回ログイ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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、 155 ページの『IBM Spectrum Protect Plus の始動』 でパスワード要件の規則を参照してください。

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

[21 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。

[507 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。

鍵と証明書の管理

クラウド・リソースとリポジトリ・サーバーは、コピー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・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、コピー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。一部のコピー宛先には、データ・セキュリティを強化するために証明書も必要です。

コピー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・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・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**」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・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・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・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・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・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」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・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・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 のほか、vCenter および Hyper-V 各アプリケーション・サーバーにより管理される仮想マシン上で、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 鍵を追加できます。SSH 鍵は、ファイルの索引付けとリストア操作のために IBM Spectrum Protect Plus リソースとターゲット・リソースの間のセキュア接続を提供します。

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。
- SSH 鍵ペアを生成するために使用されるターゲット・リソースのユーザー・アカウントには、**sudo** 特権が必要です。このアカウントは、IBM Spectrum Protect Plus に割り当てられます。このアカウントは、IBM Spectrum Protect Plus ユーザー・エージェント (sppagent) と呼ばれます。
- vCenter によって管理される仮想マシンが環境に含まれている場合は、最新の VMware Tools をインストールするようにしてください。

手順

鍵を追加するには、以下のステップを実行します。

1. ターゲット・リソースで、`ssh-keygen` コマンドを使用して SSH 鍵を生成します。このコマンドは、IBM Spectrum Protect Plus に割り当てられるユーザー・アカウントを使用して実行されます。このアカウントには **sudo** 特権が必要です。例えば、Oracle サーバーでは、端末に以下のコマンドを入力し、指示に従ってください。

```
ssh-keygen
```

デフォルト設定を使用する場合、指定されたディレクトリーに 2 つのファイル (`id_rsa.pub` は公開鍵で `id_rsa` は秘密鍵) が作成されます。

2. プロンプトが出されたら、鍵が保存されるファイル名を入力し、ディレクトリーとファイル名を入力します。ディレクトリーとファイル名を指定しないと、デフォルトが使用されます。

```
/home/privileged_user/.ssh/id_rsa
```

ここで `privileged_user` は、IBM Spectrum Protect Plus、`sppagent` に割り当てられたアカウントです。デフォルト名の鍵がすでに存在している場合、以下に表示するメッセージで示されます。既存の鍵が使用中の場合は、上書きしないように注意してください。鍵を保存する別のファイルを入力する場合は、「**N**」を押します。

```
/home/<privileged user>/.ssh/id_rsa already exists.  
Overwrite (y/n)?
```

この手順は、デフォルトのファイル名 (`id_rsa`) を使用して鍵がデフォルト・ロケーションに保存されていることを前提としています。鍵ファイルが別のファイル名を使用して作成されている場合は、以下のステップでそのファイル名を使用してください。

3. パスフレーズを入力して、Enter キーを押してください。それ以外の場合は、パスフレーズを入力しないで単に Enter キーを押します。
4. パスフレーズが指定された場合は、再入力します。Enter キーを押します。
5. `id_rsa.pub` 鍵のコンテンツを `authorized_keys` ファイルにコピーします。ファイルがすでに存在する場合、公開鍵を `authorized_keys` ファイルに追加します。

```
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
```

6. `chmod 600` コマンドを発行して、`authorized_keys` ファイルに必要な特権を割り当てます。

```
chmod 600 ~/.ssh/authorized_keys
```

7. テキスト・エディターを使用して `/etc/ssh/sshd_config` ファイルを編集して、`PubkeyAuthentication` 設定値を `yes` に設定します。設定をコメント化しないように、番号記号 (#) が行の先頭に表示されている場合は削除してください。

```
sudo vi /etc/ssh/sshd_config
```

```
...  
PubkeyAuthentication yes  
...
```

8. ターゲット・リソース上で SSH サービスを再始動します。

```
systemctl restart sshd
```

9. 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。
10. 「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。
11. 「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 鍵の識別するための分かりやすい名前を入力します。

ユーザー

ターゲット・リソースと SSH 鍵に関連付けられているユーザー・アカウントを入力します。これは、前のステップで公開鍵と秘密鍵を生成する際に使用したユーザー・アカウントです。

暗号化

公開鍵と秘密鍵の生成時にパスフレーズを指定した場合は、このボックスにチェック・マークを付けます。

パスフレーズ

このボックスは、「暗号化」チェック・ボックスを選択した場合のみ表示されます。公開鍵と秘密鍵の生成時にパスフレーズを指定した場合は、このボックスにパスフレーズを入力します。

秘密鍵

秘密鍵をコピーしてこのボックスに貼り付けます。これは、ターゲット・リソース上の `id_rsa` ファイルに含まれている鍵です。ファイルは、以下の例のようになります。

```
cat ~/.ssh/id_rsa

-----BEGIN OPENSSH PRIVATE KEY-----
ZRYtuinjaHx2mKgW4LnfqzlyAIIq5Amasi/J8/AAAFiFiP4GZYj+BmAAAAB3NzaC1yc2
...
...
Q5ZqZ1Ec8N7dsAAANdG9vckBVYnVudHVWQgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

12. 「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」オプションでリソースにアクセスするため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。

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。

始める前に

証明書が使用可能であることを確認します。以下の技術情報は、IBM Spectrum Protect Plus の証明書を使用するための概要について説明します。

HTTPS

[技術情報 739663](#) は、Microsoft 認証局が発行する HTTPS 証明書の使用方法について説明します。一方で、別の認証局 (CA) を使用することもできます。

LDAP

[技術情報 791677](#) は LDAP 証明書の使用方法を説明します。

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 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。

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. サポート対象ブラウザから、以下の管理コンソールの URL を入力します。

`https://HOSTNAME:8090/`

ここで、HOSTNAME は、管理コンソール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	SUPERUSER 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-SysXyz 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、 155 ページの『IBM Spectrum Protect Plus の始動』

3. 「**証明書管理**」をクリックします。
4. 証明書タイプ「**HTTP**」または「**LDAP/Hyper-V**」をクリックします。
5. 「**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。
6. 「**certificate type の SSL 証明書のアップロード**」をクリックします。
7. アップロードが完了したら、「**システム管理**」 > 「**IBM Spectrum Protect Plus の再始動**」をクリックしてください。

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	SUPERUSER 特権を持つ IBM Spectrum Protect Plus ユーザーとしてログインするには、管理者ユーザー名とパスワードを入力します。

認証タイプ	ログイン情報
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-SysXyz 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、 155 ページの『IBM Spectrum Protect Plus の始動』 のパスワード要件の規則を参照してください。

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. 管理コンソールから IBM Spectrum Protect Plus アプライアンスを再始動します。
6. IBM Spectrum Protect Plus アプライアンスが再開されたら、現在のタイム・ゾーンを確認します。管理コンソールのメイン・ページから「製品情報」を選択して、更新されたタイム・ゾーンを確認します。

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-SysXyz** 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#)でパスワード要件の規則を参照してください。

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-SysXyz` 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#)でパスワード要件の規則を参照してください。

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・ラインにアクセスします。以下のコマンドを実行します。

```
# sudo bash
```

2. 以下のコマンドを実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. 以下のコマンドを実行してツールを実行します。

```
# java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxddd.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、「実行」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実行して、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。次のコマンドを実行します。

```
# 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・ルール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 の「iptables を使用するファイアウォール構成」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-SysXyz` 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、155 ページの『IBM Spectrum Protect Plus の始動』のパスワード要件の規則を参照してください。

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。

```
sudo bash
```

Enter キーを押します。

```
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-SysXyz` 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。新規パスワードの作成時には、特定の規則が適用されます。詳しくは、[155 ページの『IBM Spectrum Protect Plus の始動』](#) のパスワード要件の規則を参照してください。

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、**pvccreate /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
```

グローバル設定の構成

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構成できます。

始める前に

グローバル設定を構成するには、管理者資格情報が必要です。

「**他のストレージ製品との統合 (Integrations with other storage products)**」カテゴリの設定は、いつでも変更できます。



重要: 「**他のストレージ製品との統合 (Integrations with other storage products)**」カテゴリの設定を変更できますが、その他のすべての設定を変更するのは、絶対に必要な場合のみで、IBM サポートの指示による場合のみにしてください。グローバル設定を変更すると、ストレージ環境に影響を与える可能性があります。IBM サポートとの協議が必要な設定のカテゴリは、「**アプリケーション**」、「**一般**」、「**ジョブ**」、「**ロギング**」、「**保護**」、および「**セキュリティー**」です。

このタスクについて

パラメーターのデフォルト値に対して行った変更は、変更を保存するときにすべての IBM Spectrum Protect Plus 操作に適用されます。

手順


設定の値を編集してグローバルに適用するには、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」 > 「グローバル設定」をクリックします。
2. IBM Spectrum Protect Plus から IBM Spectrum Protect Operations Center へのアクセスを有効にするには、「他のストレージ製品との統合 (Integrations with other storage products)」カテゴリの設定を編集します。次の図に、設定のデフォルト値を示します。

以下の設定を編集できます。

IBM Spectrum Protect Operations Center URL

IBM Spectrum Protect Operations Center の IP アドレス。Operations Center では、IBM Spectrum Protect 環境に関する情報状況への Web およびモバイル・アクセスが提供されています。

この設定が指定される場合、IBM Spectrum Protect Plus メニュー・バーで IBM Spectrum Protect アイコン  がアクティブになります。この設定の URL を最初に設定する場合、または URL を変更する場合は、ユーザー・インターフェースで設定を有効にするために、いったんログオフしてから再度ログインする必要があります。

この URL は、Operations Center のインストール・プロセス中に作成されます。Operations Center の URL を取得するには、IBM Spectrum Protect システム 管理者にお問い合わせください。

3. グローバル・アプリケーション設定を適用するには、「アプリケーション」カテゴリの設定を編集します。次の図に、設定のデフォルト値を示します。

Application

Enable SQL Server databases restored in test mode eligible for backup

☐

Maximum volume size for backup target LUNs on Windows (TB)

Maximum backup retries(k8s)

Maximum concurrent servers running backups

Allow SQL database backup when transaction log backup chain is broken

☐

Rename SQL data and log files when database is restored in production mode with new name

☐

以下のアプリケーション設定を編集できます。

適格なテスト・モードでリストアされた SQL Server データベースのバックアップを有効にする (Enable SQL Server databases restored in test mode eligible for backup)

テスト・モードでリストアされた SQL Server データベースをバックアップします。このオプションを選択すると、テスト・モードでリストアされた SQL Server データベースが「SQL バックアップ」ペインまたは「アドホック・バックアップ (Ad hoc backup)」ウィザードで選択できるようになります。

Windows 上のバックアップ・ターゲット LUN の最大ボリューム・サイズ (TB) (Maximum volume size for backup target LUNs on Windows (TB))

バックアップ・ターゲット用のストレージの最大サイズ。

最大バックアップ再試行回数 (k8s) (Maximum backup retries (k8s))

複数の Persistent Volume Claim (PVC) を含むコピー・バックアップ・ジョブのバックアップ・セッションを IBM Spectrum Protect Plus が再試行する最大回数。

複数の PVC が同じコピー・バックアップ・ジョブに関係している場合、IBM Spectrum Protect Plus はバックアップ操作を並行ジョブとして実行します。バックアップ・セッションが接続の問題のためにタイムアウトにならないように、IBM Spectrum Protect Plus が接続を再試行する最大回数を指定してください。

最大再試行回数に達したときに、接続障害がまだ存在している場合は、失敗したセッションに含まれていた PVC バックアップのみが失敗として報告されます。

バックアップを実行する並行サーバーの最大数

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。

トランザクション・ログ・バックアップ・チェーンが壊れたときに SQL データベース・バックアップを許可する (Allow SQL database backup when transaction log backup chain is broken)

IBM Spectrum Protect Plus がデータベースのログ・バックアップ・チェーン内の切断を検出すると、データベース・バックアップ・ジョブを実行します。

データベースが新しい名前を実動モードでリストアされるときに、SQL データおよびログ・ファイルの名前を変更する (Rename SQL data and log files when database is restored in production mode with new name)

実動またはテストのリストア・ジョブ中に、関連した SQL データベース・データおよびログ・ファイルの名前を変更します。このフィールドは、SQL データベースのリストア・ジョブ中に新規データベース名が指定される場合にのみ適用されます。

4. 一般設定を適用するには、「一般」カテゴリの設定を編集します。次の図に、設定のデフォルト値を示します。

General	
Access log retention (days)	<input type="text" value="30"/>
Tools working folder on Linux guest	<input type="text" value="/tmp"/>
Tools working folder on Windows guest	<input type="text" value="c:\ProgramData"/>
Linux/AIX Clients Port (SSH) used for application and file indexing	<input type="text" value="22"/>
Windows Clients Port (WinRM) used for application and file indexing	<input type="text" value="5985"/>
IBM Spectrum Protect Plus Server IP Address	<input type="text"/>

以下の一般設定を編集できます。

アクセス・ログ保存(日数) (Access log retention (days))

アクセス・ログを保存する日数を入力します。

Linux ゲスト上のツール作業フォルダー (Tools working folder on Linux guest)

Linux VM ゲスト上のツール用の作業フォルダー。

Windows ゲスト上のツール作業フォルダー (Tools working folder on Windows guest)

Windows VM ゲスト上のツール用の作業フォルダー。

アプリケーションおよびファイル索引付けに使用される Linux/AIX クライアント・ポート (SSH) (Linux/AIX Clients Port (SSH) used for application and file indexing)

Linux および AIX クライアント上のアプリケーションおよびファイル索引付けに使用される SSH ポート。

アプリケーションおよびファイル索引付けに使用される Windows クライアント・ポート (WinRM) (Windows Clients Port (WinRM) used for application and file indexing)

Windows クライアント上でのアプリケーションおよびファイル索引付けに使用される Windows リモート管理 (WinRM) ポート。

IBM Spectrum Protect Plus サーバー IP アドレス (IBM Spectrum Protect Plus Server IP Address)

IBM Spectrum Protect Plus サーバーの使用可能な IP アドレスのリスト。これらの IP アドレスは、VADP プロキシと IBM Spectrum Protect Plus サーバーの間の通信に使用されます。また、これらのアドレスは、リモート・エージェント通信にも使用されます。

5. ジョブまたはロギングの設定を適用するには、「**ジョブ**」カテゴリまたは「**ロギング**」カテゴリの値を編集します。次の図に、設定のデフォルト値を示します。

Job	
Job log retention (days)	60
Job notification status	failed

Logging	
Enable logging IBM Spectrum Protect Plus alerts to the system log	<input type="checkbox"/>

以下のジョブおよびロギングの設定を編集できます。

ジョブ・ログ保存(日数)

ログが削除されるまでにジョブ・ログを保存する日数。

ジョブ通知状況

アラートを送信するための状況レベル。指定された状況でジョブが完了すると、アラートが送信されます。例えば、ジョブ通知状況が **failed** の場合、ジョブに対して **failed** 状況が報告されると、アラートが送信されます。

システム・ログへの IBM Spectrum Protect Plus アラートのロギングを有効にする (Enable logging IBM Spectrum Protect Plus alerts to the system log)

IBM Spectrum Protect Plus によって生成されたアラートをシステム・ログに組み込みます。この機能を有効にすると、アラートを見つけるためにシステム・ログを検索することができます。

6. 保護設定を適用するには、「**保護**」カテゴリの設定を編集します。次の図に、設定のデフォルト値を示します。

Protection	
Number of seconds to wait before checking connection	1000
Number of times to check for valid connection	0
Temporary folder for file index zip files	/data2/filecatalog
Temporary folder for file indexing on Windows server	
Group VMs by	Count
Number of VMs in group	1
Force the removal of replication relationship for last remaining snapshot	<input type="checkbox"/>
Target free space error (percentage)	20
Target free space warning (percentage)	30
Catalog object update count	50
Virtual machine backup status update interval (seconds)	300
VADP proxy uses only HotAdd transport mode	<input type="checkbox"/>
VM group size (GB)	5120
vSnap auto disable deduplication when DDT size reaches resource limit	<input checked="" type="checkbox"/>
vSnap DDT size limit as percentage of total memory cache	80
vSnap DDT size limit in GB	50
Used space threshold on datastore or a volume before backup cannot take snapshots of a VM (percentage)	95
Backup wait timeout (seconds)	600
VMware communication timeout (seconds)	300

以下の保護設定を編集できます。

接続を検査するまでの待機秒数

クラウド・オブジェクトとの接続を確認するまでに IBM Spectrum Protect Plus が待機する時間。

有効な接続を調べる回数

IBM Spectrum Protect Plus が使用可能な接続を検査する回数。

ファイル索引 zip ファイルの一時フォルダー (Temporary folder for file index zip files)

索引付け用のメタデータを含む圧縮 (.zip) ファイルを保管するための一時フォルダー。索引付けが完了すると、ファイルが削除されます。

Windows サーバー上のファイル索引付け用の一時フォルダー (Temporary folder for file indexing on Windows server)

Windows サーバーの索引付け用のメタデータが含まれている圧縮 (.zip) ファイルを保管するための一時フォルダー。索引付けが完了すると、このフォルダーは削除されます。

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、グループに含まれる VM の数またはグループに含まれる VM のサイズで定義できます。

グループ内の VM の数

VM グループ化の場合、4 つの VM グループが使用可能であり、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) をグループ化することができます。

最後に残ったスナップショットの複製関係の削除を強制する (Force the removal of the replication relationship for last remaining snapshot)

期限切れが設定され、ロックされている最後の残りのスナップショットの既存の複製関係を削除します。

ターゲットのフリー・スペース・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。

ターゲットのフリー・スペース警告 (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。

カタログ・オブジェクトの更新カウント (Catalog object update count)

カタログ内で照会および更新されるオブジェクトの数を制限するために設定できるカウント。例えば、カタログに 100 個のオブジェクトが含まれており、更新カウントが 20 である場合、IBM Spectrum Protect Plus は 5 回の反復でカタログを更新します。

仮想マシンのバックアップ状況更新間隔 (秒) (Virtual machine backup status update interval (seconds))

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。

VADP プロキシは HotAdd トランスポート・モードのみを使用する (VADP proxy uses only HotAdd transport mode)

HotAdd 仮想ディスク・トランスポート方式を使用して、VMware IBM Spectrum Protect Plus 仮想アプライアンスを VADP プロキシに接続します。このオプションが有効になっている場合、VADP プロキシは、代替トランスポート・モードにフォールバックせずに、HotAdd のみを使用します。

VM グループのサイズ (GB)

VM グループのサイズ (ギガバイト (GB))。

DDT サイズがリソース限界に達する場合の vSnap 重複排除の自動無効化 (vSnap auto disable deduplication when DDT size reaches resource limit)

重複排除テーブル (DDT) はデフォルトで有効になっています。ディスク・スペース (ギガバイト) またはパーセンテージによって定義されているいずれかのしきい値を超えると、vSnap データ重複排除が無効になり、アラートが表示されます。

vSnap DDT サイズ制限 (合計メモリー・キャッシュのパーセンテージとして) (vSnap DDT size limit as percentage of total memory cache)

合計メモリー・キャッシュと比較した、vSnap 重複排除テーブル (DDT) のパーセンテージとしてのしきい値。vSnap 自動無効化オプションが選択されているときに、定義されたしきい値を超えると、DDT が無効になります。

vSnap DDT サイズ制限 (GB) (vSnap DDT size limit in GB)

vSnap DDT のしきい値 (ギガバイト (GB))。vSnap 自動無効化オプションが選択されているときに、定義されたしきい値を超えると、DDT が無効になります。

バックアップが VM のスナップショットを取ることができなくなるまでの、データ・ストアまたはボリュームの使用スペースしきい値 (パーセンテージ) (Used space threshold on datastore or a volume before backup cannot take snapshots of a VM (percentage))

バックアップのために VM のスナップショットが取得できなくなるまでのしきい値である、データ・ストアまたはボリューム上の使用スペースのパーセンテージ。

バックアップ待ちのタイムアウト (秒)

IBM Spectrum Protect Plus が別のバックアップ・ジョブを開始するまでにバックアップ・ジョブが終了するのを待機する時間の長さ。バックアップ・ジョブが待機時間内に終了しない場合、そのジョブはタイムアウトになり、次のジョブが始まります。

VMware 接続タイムアウト (秒) (VMware connection timeout (seconds))

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。

7. セキュリティー設定を適用するには、「セキュリティ」カテゴリーの設定を編集します。次の図に、設定のデフォルト値を示します。

Set Minimum Password Length (characters)

8

以下のセキュリティ設定を編集できます。

パスワードの最小長の設定 (文字) (Set Minimum Password Length (characters))

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。

デモ環境の削除

IBM Spectrum Protect Plus アプライアンスには、ローカル・ホストという名前のオンボード vSnap サーバー、デモという名前のデモンストレーション用のサイト、およびデモという名前の関連 SLA ポリシーが含まれています。もっと大きい実稼働環境には、オンボード vSnap サーバーを使用しないでください。代わりに、1 つ以上のスタンドアロン vSnap サーバーを使用します。デモ SLA ポリシー、デモ・サイト、およびオンボード vSnap サーバー (デモ環境と総称されます) は、ディスク・スペースを節約するために安全に除去することができます。

始める前に

稼働中の IBM Spectrum Protect Plus アプライアンスの場合、IBM Spectrum Protect Plus アプリケーションをバックアップします。手順については、475 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。新規デプロイメントの場合、アプリケーションのバックアップは不要です。

ローカル・ホスト vSnap サーバー上のデータが必要ないことを確認します。


少なくとも 1 つのスタンドアロン vSnap サーバーがバックアップの宛先としてデプロイされていることを確認します。





このタスクについて

デプロイすると、IBM Spectrum Protect Plus アプライアンスには 6 つの仮想ハード・ディスクがあります。IBM Spectrum Protect Plus アプライアンスからデモ構成およびローカル・ホスト vSnap サーバーを削除すると、関連する 2 つの仮想ハード・ディスクを除去することにより、ストレージを解放することができます。

このトピックの手順は、IBM Spectrum Protect Plus からデモ環境を除去するために実行する必要があります。

手順

- 以下のステップを実行して、デモ環境に割り当てられている SLA ポリシーを無効にします。
 - サポートされているブラウザから、IBM Spectrum Protect Plus ユーザー・インターフェースにログインします。
 - デモ SLA に割り当てられているジョブを表示します。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。命名パターン `Job_Name_Demo` に従うジョブを見つけます。ここで、`Job_Name` はジョブの名前です。この命名パターンは、デモ SLA が使用されることを示します。
 - すべてのデモ・ジョブのスケジュールを一時停止します。「アクション」メニュー・アイコン  をクリックし、`_Demo` で終了するジョブごとに「スケジュールの一時停止」を選択します。
- 以下のステップを実行して、デモ SLA を削除します。

- a) 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。「SLA ポリシー」ペイン内の表までスクロールダウンして、デモ・ポリシーを見つけます。
 - b) デモ SLA の横にある「削除」アイコン  をクリックします。
 - c) 「確認」ダイアログ・ボックスにコードを入力し、「OK」をクリックします。
3. 以下のステップを実行して、ローカル・ホスト vSnap ディスク・ストレージを削除します。
- a) 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。デモ・サイトに割り当てられているローカル・ホスト vSnap ストレージを見つけます。
 - b) ローカル・ホスト vSnap ストレージの横にある「削除」アイコン  をクリックします。
 - c) 「確認」ダイアログ・ボックスにコードを入力し、「削除」をクリックします。
4. 以下のステップを実行して、デモ・サイトを削除します。
- a) 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。デモという名前のサイトを見つけます。
 - b) デモ・サイトの横にある「削除」アイコン  をクリックします。
 - c) 「確認」ダイアログ・ボックスで「はい」をクリックして、デモ・サイトの削除を完了します。
5. 以下のステップを実行して、LocalvSnapAdmin ID を削除します。
- a) ナビゲーション・パネルで、「アカウント」 > 「ID」をクリックします。
 - b) LocalvSnapAdmin ID の横にある「削除」アイコン  をクリックします。
 - c) 「確認」ダイアログ・ボックスで「はい」をクリックして ID を削除します。
6. 以下のステップを完了して、ファイル・システムと LVM 構成をクリーンアップします。
- a) Secure Shell (SSH) プロトコルを使用するか、serveradmin アカウントを使用してハイパーバイザー・コンソールから、IBM Spectrum Protect Plus にログインします。
 - b) ローカル・ホスト vSnap ストレージ・プールの ID を取得します。次のコマンドを発行します。

```
$ vsnap pool show
```



重要: データが失われないようにするために、取得した ID がローカル・ホスト vSnap ストレージ・プールの ID であることを確認してください。

- c) ローカル・ホスト vSnap ストレージ・プールを削除します。以下のコマンドを発行します。ここで、<ID> は前のステップで取得した ID です。

```
$ vsnap pool delete --id <ID>
```

- d) ローカル・ホスト vSnap ストレージのクラウド・キャッシュをアンマウントします。次のコマンドを発行します。

```
$ sudo umount -f /opt/vsnap-data
```

- e) fstab ファイルを編集して、クラウド・キャッシュが開始できないようにします。sudo およびテキスト・エディターを使用して、/dev/mapper/vsnapdata-vsnapdata1v で始まる行をコメント化します。
- f) クラウド・キャッシュに関連付けられている LVM ボリューム・グループを非アクティブにします。次のコマンドを発行します。

```
$ sudo vgchange -an vsnapdata
```

7. vSphere または Hyper-V マネージャーを使用することにより、IBM Spectrum Protect Plus アプライアンスから不要になった仮想ハード・ディスクを切り離します。正しいディスクが切り離されるように、慎重に進めます。ローカル・ホスト vSnap サーバーには、2 つの関連する仮想ハード・ディスクがあります。これらのサイズは 100 GB と 128 GB です。仮想ハード・ディスクの切り離しまたは除去に関する詳しい手順については、該当するハイパーバイザーの資料を参照してください。ハイパーバイザーごとの一般的な手順は次のとおりです。



重要: 仮想ハード・ディスクを切り離す前に、IBM Spectrum Protect Plus アプライアンスの電源をオフにしてください。アプライアンスの電源をオンにし、メンテナンス・ジョブを実行した後で、正しい機能が確認されるまでは、仮想ハード・ディスクを削除しないでください。

以下のステップを実行して、関連する仮想ハード・ディスクを仮想マシンから除去します。

a) VMware 環境の場合、vSphere を開き、以下のステップを実行します。

- 1) 「**VM とテンプレート**」をクリックします。
- 2) IBM Spectrum Protect Plus アプライアンスが含まれているホストを展開します。
- 3) IBM Spectrum Protect Plus 仮想マシンを選択します。
- 4) IBM Spectrum Protect Plus アプライアンスの電源をオフにします。
- 5) 「**アクション**」メニューから、「**設定の編集**」をクリックします。
- 6) 不要になった仮想ハード・ディスクを見つけます。除去できるディスクの横にあるサイズは、100 GB および 128 GB です。
- 7) 識別されたいずれかのディスクを選択し、除去ボタンをクリックします。

重要: どのディスクにも「**データ・ストアからファイルを削除する (Delete files from datastore)**」チェック・ボックスを選択しないでください。適切な機能が検証された後でのみディスクを削除します。

- 8) 識別された残りのディスクを選択し、除去ボタンをクリックします
- 9) 「**OK**」をクリックします。
- 10) IBM Spectrum Protect Plus の電源をオンにします。

b) Hyper-V 環境の場合は、Hyper-V マネージャーを開き、以下のステップを実行します。

- 1) IBM Spectrum Protect Plus 仮想マシンが属しているノードを選択します。
- 2) 「**仮想マシン**」ペインから IBM Spectrum Protect Plus 仮想マシンを選択します。
- 3) IBM Spectrum Protect Plus アプライアンスの電源をオフにします。
- 4) 仮想マシンの「**設定**」をクリックします。
- 5) 不要になった仮想ハード・ディスクを見つけます。接続されている仮想ハード・ディスクごとに「**検査 (Inspect)**」をクリックします。「**仮想ハード・ディスクのプロパティ (Virtual Hard Disk Properties)**」ウィンドウの「**最大ディスク・サイズ (Maximum Disk Size)**」の値は、100 GB および 128 GB でなければなりません。
- 6) 識別されたディスクの 1 つを選択して、「**除去**」をクリックします。
- 7) 識別された残りのディスクを選択して、「**除去**」をクリックします。
- 8) 「**OK**」をクリックします。
- 9) IBM Spectrum Protect Plus の電源をオンにします。

8. 以下のステップを実行して、SCSI バスを再スキャンし、vSnap サービスを無効にします。

- a) Secure Shell (SSH) プロトコルを使用するか、serveradmin アカウントを使用してハイパーバイザー・コンソールから、IBM Spectrum Protect Plus にログインします。
- b) 以下のコマンドを発行して、SCSI バスを再スキャンします。

```
$ sudo rescan-scsi-bus.sh
```

c) 次のコマンドを発行して、vSnap サービスを停止します。

```
$ sudo systemctl stop vsnap
```

d) 次のコマンドを実行して、vSnap サービスを無効にします。

```
$ sudo systemctl disable vsnap
```

第 9 章 バックアップ操作の SLA ポリシーの管理

サービス・レベル契約 (SLA) ポリシーは、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コピーするオプションがあります。事前定義された SLA ポリシーを使用できます。また、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。Amazon EC2 インスタンスおよびコンテナを除く、サポートされているすべてのリソースに対応しています。

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。Amazon EC2 インスタンスおよびコンテナのデータを除く、サポートされているすべてのリソースに対応しています。

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。Amazon EC2 インスタンスおよびコンテナのデータを除く、サポートされているすべてのリソースに対応しています。

EC2

Amazon EC2 インスタンスを保護するために、このポリシーは、31 日間の保存期間でスナップショット・バックアップを毎日実行します。

コンテナ

コンテナ・データを保護するために、このポリシーは以下の操作を実行します。

- 保存期間が 1 日の 6 時間ごとのスナップショット・バックアップ
- 保存期間が 31 日間の毎日のコピー・バックアップ

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。

標準オブジェクト・ストレージのコピー・ソース、宛先タイプ、またはターゲット・サーバーの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、差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 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。

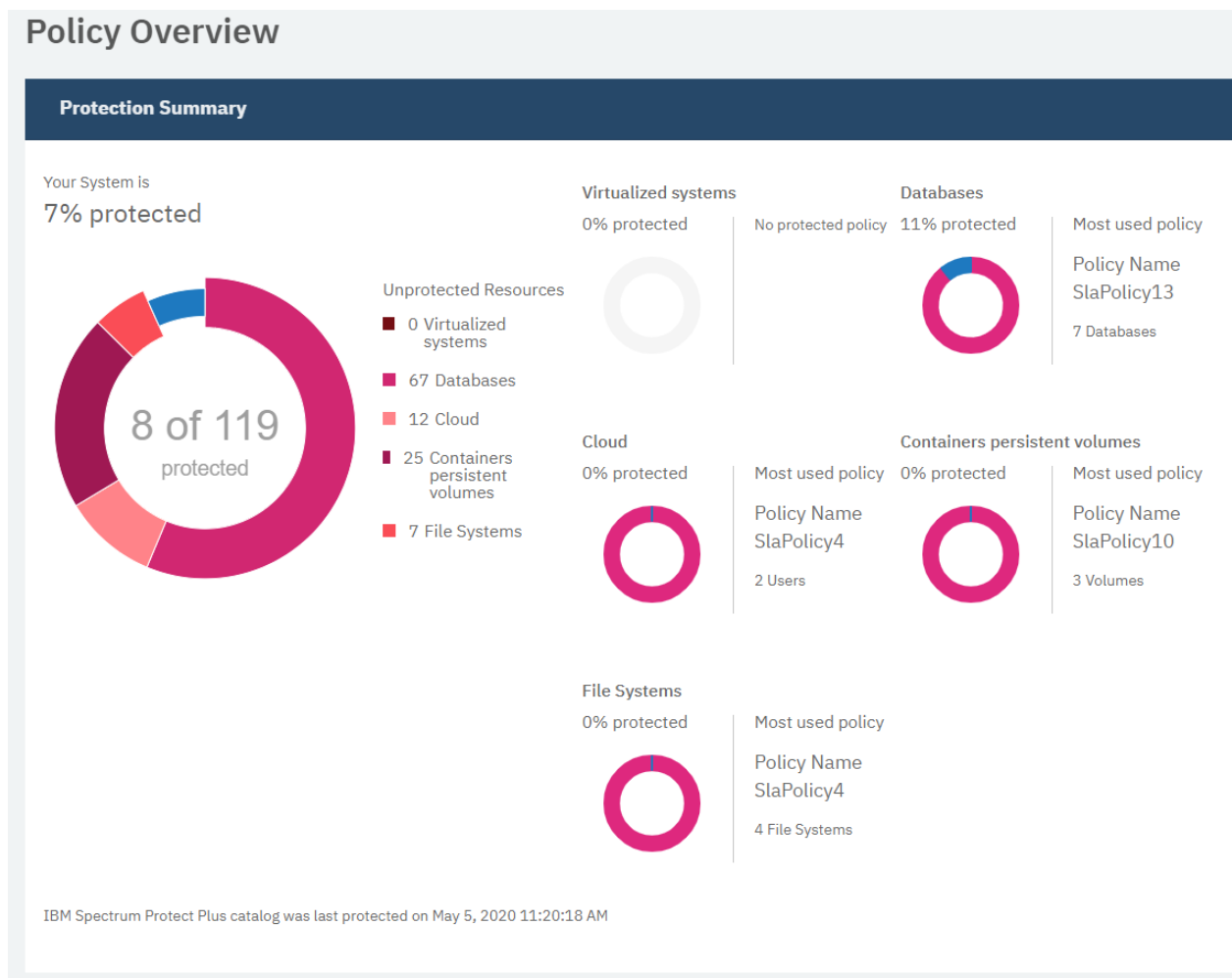
注：組み込み vSnap は、デモ・サイトによってのみ使用できるように設定されています。組み込み IBM Spectrum Protect Plus vSnap を他のサイトで使用しないでください。

保護の要約

「保護の要約」ペインで、システム内のリソースの保護状況を表示することができます。

「保護の要約」ペインは、保護されているリソースの数と保護されていないリソースの数を示すドーナツ・グラフで構成されています。リソースのタイプごとに、保護されているリソースのパーセンテージと、そのリソースで最も頻繁に使用されている SLA ポリシーを表示することができます。

「保護の要約」ペインを表示するには、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。



システム

「システム」グラフには、システムで IBM Spectrum Protect Plus によって保護されているリソースの合計パーセンテージが示されます。

% 保護

IBM Spectrum Protect Plus によって保護されているリソースのパーセンテージが示されます。ドーナツ・グラフで、保護されているリソースは青色の線で表されます。ドーナツのさまざまな部分にカーソルを移動すると、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を表示できます。

保護されていないリソース

保護されていないリソースの凡例が示されています。このリストには、IBM Spectrum Protect Plus のインスタンスによって管理されているリソースのタイプに関するデータのみが示されます。リソースのタイプが IBM Spectrum Protect Plus によって管理されていない場合、数は 0 です。

仮想化システム (Virtualized systems)

「仮想化システム (Virtualized systems)」グラフには、IBM Spectrum Protect Plus によって保護されている仮想化システムのパーセンテージが示されます。

% 保護

保護されている仮想化システムのパーセンテージが示されます。ドーナツのさまざまな部分にカーソルを移動すると、保護されている仮想化システムと保護されていない仮想化システムの数を表示できます。

IBM Spectrum Protect Plus によって管理されている仮想化システムがない場合、パーセンテージは 0 です。

最も使用されているポリシー (Most used policy)

最も頻繁に使用されている SLA ポリシーの名前と、そのポリシーを使用している仮想化システムの数が表示されます。IBM Spectrum Protect Plus によって管理されている仮想化システムがない場合、このフィールドは表示されません。

保護ポリシーなし (No protected policy)

このメッセージは、IBM Spectrum Protect Plus によって管理されている仮想化システムがない場合にのみ表示されます。

データベース

「データベース」グラフには、IBM Spectrum Protect Plus によって保護されているデータベースのパーセンテージが表示されます。

% 保護

保護されているデータベースのパーセンテージが表示されます。ドーナツのさまざまな部分にカーソルを移動すると、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の数を表示できます。

IBM Spectrum Protect Plus によって管理されているアプリケーション・データベースがない場合、パーセンテージは 0 です。

最も使用されているポリシー (Most used policy)

最も頻繁に使用されている SLA ポリシーの名前と、そのポリシーを使用しているデータベースの数が表示されます。IBM Spectrum Protect Plus によって管理されているデータベースがない場合、このフィールドは表示されません。

保護ポリシーなし (No protected policy)

このメッセージは、IBM Spectrum Protect Plus によって管理されているデータベースがない場合にのみ表示されます。

クラウド

「クラウド」グラフには、IBM Spectrum Protect Plus によって保護されているクラウド・ベースのアカウント (Microsoft Office 365 テナントなど) のパーセンテージが表示されます。

% 保護

保護されているクラウド・ベースのアカウントのパーセンテージが表示されます。ドーナツのさまざまな部分にカーソルを移動すると、保護されているアカウントと保護されていないアカウントの数を表示できます。

IBM Spectrum Protect Plus によって管理されているクラウド・ベースのアカウントがない場合、パーセンテージは 0 です。

最も使用されているポリシー (Most used policy)

最も頻繁に使用されている SLA ポリシーの名前と、そのポリシーを使用しているアカウントの数が表示されます。IBM Spectrum Protect Plus によって管理されているクラウド・ベースのアカウントがない場合、このフィールドは表示されません。

保護ポリシーなし (No protected policy)

このメッセージは、IBM Spectrum Protect Plus によって管理されているクラウド・ベースのアカウントがない場合にのみ表示されます。

コンテナ永続ボリューム (Containers persistent volumes)

IBM Spectrum Protect Plus によって保護されている永続ボリュームのパーセンテージが表示されます。

% 保護

保護されている永続ボリュームのパーセンテージが表示されます。ドーナツのさまざまな部分にカーソルを移動すると、保護されている永続ボリュームと保護されていない永続ボリュームの数を表示できます。

IBM Spectrum Protect Plus によって管理されている永続ボリュームがない場合、パーセンテージは 0 です。

最も使用されているポリシー (Most used policy)

最も頻繁に使用されている SLA ポリシーの名前と、そのポリシーを使用している永続ボリュームの数が表示されます。IBM Spectrum Protect Plus によって管理されている永続ボリュームがない場合、このフィールドは表示されません。

保護ポリシーなし (No protected policy)

このメッセージは、IBM Spectrum Protect Plus によって管理されている永続ボリュームがない場合にのみ表示されます。

ファイル・システム

IBM Spectrum Protect Plus によって保護されているファイル・システムのパーセンテージが示されます。

% 保護

保護されているファイル・システムのパーセンテージが示されます。ドーナツのさまざまな部分にカーソルを移動すると、保護されているファイル・システムと保護されていないファイル・システムの数を表示できます。

IBM Spectrum Protect Plus によって管理されているファイル・システムがない場合、パーセンテージは 0 です。

最も使用されているポリシー (Most used policy)

最も頻繁に使用されている SLA ポリシーの名前と、そのポリシーを使用しているファイル・システムの数が表示されます。IBM Spectrum Protect Plus によって管理されているファイル・システムがない場合、このフィールドは表示されません。

保護ポリシーなし (No protected policy)

このメッセージは、IBM Spectrum Protect Plus によって管理されているファイル・システムがない場合にのみ表示されます。

ハイパーバイザー、データベース、およびファイル・システムの SLA ポリシーの作成

カスタム・サービス・レベル・アグリーメント (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、およびコピーの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。

vSnap サーバーからクラウド・ストレージにデータをコピーする際、正常に完了した最新のスナップショットがコピーされます。

手順

ハイパーバイザー、データベース、およびファイル・システムの SLA ポリ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、「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. 「VMware、Hyper-V、Exchange、Office365、SQL、Oracle、Db2、MongoDB および Windows ファイル・システム (VMware, Hyper-V, Exchange, Office365, SQL, Oracle, Db2, MongoDB and Windows File Systems)」をクリックします。
5. 「バックアップ・ポリシー」セクションで、以下のバックアップ操作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

制約事項：「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

バックアップ操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

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。

タイム・ゾーンには、ブラウザの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「**ヨーロッパ/ダブリン**」)。フィールドをクリックして、「**検索**」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

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。

6. 「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、[114 ページの『バックアップ・ストレージ・パートナーの構成』](#)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

制約事項：「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

複製操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

複製操作を開始したい日時を入力します。

タイム・ゾーンには、ブラウザの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「ヨーロッパ/ダブリン」)。フィールドをクリックして、「検索」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

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。

7. 「追加コピー」セクションで、以下のオプションを設定して、データを標準オブジェクト・ストレージまたはアーカイブ・オブジェクト・ストレージにコピーします。

標準オブジェクト・ストレージ (差分コピー)

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・サーバーにデータをコピーする場合に選択します。

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・サーバーにコピーされます。バックアップ・ボリュームの最初のコピー時に、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コピーが終了した後、後続のコピーは段階的に増大し、最後のコピー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

頻度も開始時刻も定義せずにコピー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

制約事項: 「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

コピー操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

コピー操作を開始する日時を入力します。

タイム・ゾーンには、ブラウザの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「ヨーロッパ/ダブリン」)。フィールドをクリックして、「検索」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

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。

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」フィールドで選択されている場合、コピー保存オプションは無効です。

ソース

コピー操作のソースをクリックします。

メイン・ポリシーの宛先

コピー操作のソースは、「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

コピー操作のソースは、「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・サービス」または「リポジトリ・サーバー」をクリックします。

ターゲット

データの複製先にするクラウド・ストレージ・システムまたはリポジトリ・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・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、[177 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・オブジェクト・ストレージ (フルコピー)

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・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。

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コピーされます。

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

制約事項: 「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

アーカイブ操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

アーカイブ操作を開始する日時を入力します。

タイム・ゾーンには、ブラウザーの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「ヨーロッパ/ダブリン」)。フィールドをクリックして、「検索」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

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・サービス」または「リポジトリ・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・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、[177 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。

8. 「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。	509 ページの『役割の作成』 を参照してください。
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。	241 ページの『第 10 章 仮想化システムの保護』 、 353 ページの『第 14 章 データベースの保護』 、および 291 ページの『第 11 章 ファイル・システムの保護』 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

[10 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。

[11 ページの『2 次バックアップ・ストレージへのコピー・スナップショット』](#)

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・ストレージにコピーできます。

関連タスク

[232 ページの『Amazon EC2 インスタンスの SLA ポリシーの作成』](#)

カスタム・サービス・レベル・アグリーメント (SLA) ポリシーを作成して、Amazon EC2 インスタンスに固有のスナップショット保存ポリシーおよび頻度ポリシーを定義することができます。

[234 ページの『Kubernetes クラスター用の SLA ポリシーの作成』](#)

Kubernetes クラスターに接続されている永続ボリュームに対して、カスタム SLA ポリシーを作成することができます。スナップショット操作およびバックアップ操作の頻度を定義し、保存、複製、およびコピーの各ジョブにポリシーを指定することができます。

Amazon EC2 インスタンスの SLA ポリシーの作成

カスタム・サービス・レベル・アグリーメント (SLA) ポリシーを作成して、Amazon EC2 インスタンスに固有のスナップショット保存ポリシーおよび頻度ポリシーを定義することができます。

このタスクについて

スケジュールされたバックアップ・ジョブが実行されると、そのインスタンスのスナップショットは、スナップショット・ポリシーによって定義された頻度で作成されます。

インスタンスが複数の 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。

手順

インスタンスの SLA ポリ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、「**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. 「**Amazon EC2**」をクリックします。
EC2 インスタンスの SLA ポリシー・オプションが表示されます。
5. 「**スナップショット保護**」セクションで、スナップショット操作に対して以下のオプションを設定します。

保存

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スナップショット・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。このフィールドはオプションです。

頻度

制約事項：「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

スナップショット操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「**開始時刻**」は、選択した曜日に適用されます。

開始時刻

スナップショット操作を開始する日時を入力します。

タイム・ゾーンには、ブラウザーの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「**ヨーロッパ/ダブリン**」)。フィールドをクリックして、「**検索**」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

スナップショット接頭部 (Snapshot Prefix)

スナップショット名の先頭に追加する接頭部を入力します。接頭部は、スナップショットを編成したり、容易に識別したりするのに役立ちます。このフィールドはオプションです。

例えば、接頭部「daily_」を入力した場合、この SLA ポリシーで作成されたすべてのスナップショット名は「daily_」で始まります。

6. 「**保存**」をクリックします。

作成した SLA ポリシーが、「SLA ポリシー」ペインのテーブルに表示されます。

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。

- SLA ポリシーに対してユーザー許可を割り当てます。手順については、[509 ページの『役割の作成』](#)を参照してください。
- 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。手順については、[282 ページの『Amazon EC2 データのバックアップ』](#)を参照してください。

関連タスク

[239 ページの『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。

239 ページの『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。

Kubernetes クラスター用の SLA ポリシーの作成

Kubernetes クラスターに接続されている永続ボリュームに対して、カスタム SLA ポリシーを作成することができます。スナップショット操作およびバックアップ操作の頻度を定義し、保存、複製、およびコピーの各ジョブにポリシーを指定することができます。

始める前に

データを 2 次ストレージにコピーするか、データをクラウド・ストレージ・システムにアーカイブする予定の場合は、以下のアクションを実行します。

- データを 2 次ストレージ (クラウド・ストレージ・システムやリポジトリ・サーバーなど) にコピーする予定の場合は、2 次ストレージが構成されていることを確認してください。サポートされている 2 次ストレージ・システム、および構成手順については、[177 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。
- データをクラウド・ストレージ・システムにアーカイブする予定の場合は、クラウド・ターゲットにアーカイブ・バケットが定義されている必要があります。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、[177 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。

このタスクについて

定義済みの「**コンテナ**」ポリシーを使用しない場合は、カスタム SLA ポリシーを作成できます。「**コンテナ**」ポリシーによって以下の操作が実行されます。

- 保存期間が 1 日の 6 時間ごとのスナップショット・バックアップ
- 保存期間が 31 日間の毎日のコピー・バックアップ

Kubernetes バックアップ操作ではスナップショットが必要です。スケジュールされたバックアップ・ジョブが実行されると、Persistent Volume Claim (PVC) のスナップショットが、スナップショット・ポリシーによって定義された頻度で Ceph ストレージ・システムに作成されます。追加のポリシー設定を指定すると、スナップショットを IBM Spectrum Protect Plus vSnap サーバーにコピーしたり、vSnap サーバーを複製したり、クラウド内のオブジェクト・ストレージまたはリポジトリ・サーバーにデータをコピーしたりすることができます。

PVC 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。

手順

PVC の SLA ポリシーを作成する場合、以下の手順を実行します。

- 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。
- 「**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。
- 「**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。
- 「**Kubernetes**」をクリックします。
Kubernetes クラスターの SLA ポリシー・オプションが表示されます。
- 「**スナップショット保護**」セクションで、スナップショット操作に対して以下のオプションを設定します。

保存

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スナップショット・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。このフィールドはオプションです。

コピー・バックアップ、複製、または追加のコピー操作のためにポリシー・セクションを有効にする予定がある場合は、このチェック・ボックスを選択しないようにしてください。このチェック・ボックスを選択すると、vSnap サーバーにコピーできるスナップショットがなくなります。

頻度

制約事項：「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

スナップショット操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

スナップショット操作を開始する日時を入力します。

タイム・ゾーンには、ブラウザの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「ヨーロッパ/ダブリン」)。フィールドをクリックして、「検索」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

スナップショット 接頭部

スナップショット名の先頭に追加する接頭部を入力します。スナップショット名に接頭部を追加すると、スナップショットを編成し、容易に識別するのに役立ちます。このフィールドはオプションです。

接頭部には 32 文字まで入力できます。

例えば、接頭部「daily」を入力した場合、この SLA ポリシーを使用して作成されたすべてのスナップショット名は「daily」で始まります。

6. オプション: 「バックアップ・ポリシー」セクションで、vSnap サーバーへのコピー・バックアップ操作に対して以下のオプションを設定します。

バックアップ・ストレージ

vSnap サーバーへのコピー・バックアップ操作を有効にするには、このチェック・ボックスを選択します。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

vSnap サーバー上のコピー・バックアップに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バックアップ・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。このフィールドはオプションです。

頻度

制約事項：「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

コピー・バックアップ操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

コピー・バックアップ操作を開始する日時を入力します。

ヒント：コピー・バックアップ操作を開始するまでに、スナップショット・バックアップが完了する時間を割り当てます。例えば、スナップショット操作が午前 0 時 (0:00) に開始される場合、コピー・バックアップ操作は 15 分後 (00:15) に開始するように設定します。

タイム・ゾーンには、ブラウザの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「[ヨーロッパ/ダブリン](#)」)。フィールドをクリックして、「[検索](#)」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

ターゲット・サイト

バックアップ・コピーのターゲット・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

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含まれている場合、暗号化された vSnap サーバーにデータをバックアップするには、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。

7. オプション: 「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、[114 ページの『バックアップ・ストレージ・パートナーの構成』](#)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。

このオプションが有効であるのは、「バックアップ・ポリシー」が選択されている場合のみです。

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。このフィールドはオプションです。

頻度

制約事項: 「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

複製操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

複製操作を開始したい日時を入力します。

タイム・ゾーンには、ブラウザの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「[ヨーロッパ/ダブリン](#)」)。フィールドをクリックして、「[検索](#)」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

ターゲット・サイト

データの複製に使用するターゲット・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含まれている場合にデータを暗号化 vSnap サーバーに複製する場合に選択します。

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。

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。

8. オプション: 「追加コピー (Additional copies)」セクションで、標準オブジェクト・ストレージまたはアーカイブ・オブジェクト・ストレージにデータをコピーするためのオプションを設定します。

vSnap サーバーからクラウド・ストレージにデータをコピーする場合、正常に完了した最新のスナップショットがコピーされます。

標準オブジェクト・ストレージ (差分コピー)

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・サーバーにデータをコピーする場合に選択します。このオプションが有効であるのは、「バックアップ・ポリシー」が選択されている場合のみです。

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・サーバーにコピーされます。バックアップ・ボリュームの最初のコピー時に、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コピーが終了した後、後続のコピーは段階的に増大し、最後のコピー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のサーバー・リストア操作は、任意の vSnap サーバーから実行できます。

スケジュールの無効化

頻度も開始時刻も定義せずにコピー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。このフィールドはオプションです。

頻度

制約事項: 「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

コピー操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

コピー操作を開始する日時を入力します。

タイム・ゾーンには、ブラウザーの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「ヨーロッパ/ダブリン」)。フィールドをクリックして、「検索」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

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。

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」フィールドで選択されている場合、コピー保存オプションは無効です。

ソース

コピー操作のソースをクリックします。

バックアップ・ポリシーの宛先

コピー操作のソースは、「バックアップ・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

コピー操作のソースは、「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。

このオプションが有効であるのは、「バックアップ・ストレージの複製」が選択されている場合のみです。

宛先

「クラウド・サービス」または「リポジトリ・サーバー」をクリックします。

ターゲット

データのコピー先にするクラウド・ストレージ・システムまたはリポジトリ・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。

アーカイブ・オブジェクト・ストレージ (フルコピー)

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・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。このオプションが有効であるのは、「バックアップ・ポリシー」が選択されている場合のみです。

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コピーされます。

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。このフィールドはオプションです。

頻度

制約事項:「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

アーカイブ操作の頻度を入力します。「分」、「時間」、「日」、「週」、「月」、または「年」から選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。

開始時刻

アーカイブ操作を開始する日時を入力します。

タイム・ゾーンには、ブラウザの設定が自動的に取り込まれます。タイム・ゾーンを更新するには、フィールドをクリックして、リストから地域および市区町村を選択します (例えば、「ヨーロッパ/ダブリン」)。フィールドをクリックして、「検索」フィールドに地域または市区町村を入力し、一致する結果から項目を選択することもできます。

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。

バックアップ・ポリシーの宛先

アーカイブ操作のソースは、「バックアップ・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。

このオプションが有効であるのは、「バックアップ・ストレージの複製」が選択されている場合のみです。

宛先

「クラウド・サービス」または「リポジトリ・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・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。

9. 「保存」をクリックします。

作成した SLA ポリシーが、「SLA ポリシー」ペインのテーブルに表示されます。

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。

- SLA ポリシーに対してユーザー許可を割り当てます。手順については、[509 ページの『役割の作成』](#)を参照してください。
- 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。手順については、[317 ページの『永続ボリュームの SLA バックアップの定義』](#)を参照してください。

関連タスク

[239 ページの『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。

[239 ページの『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。

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。

第 10 章 仮想化システムの保護

IBM Spectrum Protect Plus で保護する仮想化システムを登録してから、システムに関連した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。

仮想化システムとは、VMware および Microsoft Hyper-V のハイパーバイザーと Amazon EC2 インスタンスを指します。

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。

ご使用の VMware 環境が [37 ページの『ハイパーバイザー \(Microsoft Hyper-V および VMware\) とクラウド・インスタンス \(Amazon EC2\) のバックアップとリストアの要件』](#) 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。

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・レベルでオリジナル・ロケーションにバックアップおよびリストアすることができます。代替の場所に仮想マシンをリストアする場合、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。リストア操作の完了後に 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

注：NFS ボリュームが、同じ vCenter に属する任意の数のデータ・センターにマウントされる場合があります。NFS ボリュームが複数のデータ・センターにマウントされる場合、vCenter は同じボリュームを 2 つの異なるデータ・ストアとして扱います。IBM Spectrum Protect Plus は、それを単一のデータ・ストアとして扱い、データ・ストアがマウントされているすべてのデータ・センターのデータ・ストアにあるすべての VM と VMDK を結合します。このデータ・ストアに対して SLA を選択すると、さまざまなデータ・センターにあるすべての VM が IBM Spectrum Protect Plus でバックアップまたはリストアされます。

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」>「仮想化システム (Virtualized Systems)」>「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**」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。

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。	509 ページの『役割の作成』 を参照してください。

関連概念

[514 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

[245 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。

[256 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	<ul style="list-style-type: none"> アラームの確認 アラーム・ステータスの設定
暗号操作 (6.5 および 6.7)	<ul style="list-style-type: none"> 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・ストア	<ul style="list-style-type: none"> スペースの割り振り データ・ストアの参照 低レベルのファイル操作 データ・ストアの削除 ファイルの削除 仮想マシン・ファイルの更新
分散スイッチ	<ul style="list-style-type: none"> ポート構成操作 ポート設定の操作
フォルダー	<ul style="list-style-type: none"> フォルダーの作成
グローバル	<ul style="list-style-type: none"> タスクのキャンセル
ホスト > 構成	<ul style="list-style-type: none"> 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 > タグ付け (6.0) vSphere タグ付け (6.5、6.7、および 7.0)	<ul style="list-style-type: none"> vSphere タグの割り当てまたは割り当て解除 オブジェクトの vSphere タグの割り当てまたは割り当て解除 (7.0) vSphere タグの作成 vSphere タグ・カテゴリの作成 カテゴリの 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	<ul style="list-style-type: none"> ネットワークの割り当て
リソース	<ul style="list-style-type: none"> 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 パワーオフ状態の仮想マシンの移行 パワーオン状態の仮想マシンの移行 vMotion のクエリー

vCenter Server オブジェクト	必要な特権
仮想マシン > 構成	<ul style="list-style-type: none"> • 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 • 拡張 (6.0 および 6.5) • 拡張構成 (6.7 および 7.0) • CPU カウントの変更 • メモリーの変更 (6.7 および 7.0) • 設定の変更 (7.0) • ロー・デバイスの構成 (6.7 および 7.0) • ディスク変更の追跡 (6.0 および 6.5) • メモリー (6.0 および 6.5) • デバイス設定の変更 • ロー・デバイス (6.0 および 6.5) • パスからの再ロード • ディスクの削除 • 名前変更 • 設定 (6.0、6.5、および 6.7) • ディスク変更の追跡の切り替え (6.7 および 7.0)
仮想マシン > ゲストの操作	<ul style="list-style-type: none"> • 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
仮想マシン > 相互作用	<ul style="list-style-type: none"> • 仮想マシン上でのバックアップ操作 • パワーオフ • パワーオン
仮想マシン > インベントリー	<ul style="list-style-type: none"> • 登録 • 削除 • 登録抹消
仮想マシン > プロビジョニング	<ul style="list-style-type: none"> • 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
仮想マシン > スナップショット管理	<ul style="list-style-type: none"> • スナップショットの作成 • スナップショットの削除 • スナップショットの復帰

vCenter Server オブジェクト	必要な特権
vApp	<ul style="list-style-type: none"> 仮想マシンの追加 リソース・プールの割り当て vApp の割り当て 作成 削除 パワーオフ パワーオン 名前変更 登録抹消 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」 > 「仮想化システム (Virtualized Systems)」 > 「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 Plus 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」 > 「仮想化システム (Virtualized Systems)」 > 「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・ジョブを定義する前に、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、[241 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、[157 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、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)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。
- 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ていることを確認してください。

このタスクについて

- 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 サーバーに転送します。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。アプライアンスが 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。
- vMotion 操作によって既存の VM がマイグレーションされる場合、IBM Spectrum Protect Plus は必要に応じてリベース操作を実行します。

制約事項: 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atalog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atalog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atalog・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。

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**」 > 「**仮想化システム (Virtualized Systems)**」 > 「**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**」をクリックして、バックアップ基準に合った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・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。ジョブをすぐに実行するには、「**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：選択されたSLAポリシーのジョブが実行されると、そのSLAポリシーに関連付けられているすべてのリソースがバックアップ操作に含まれます。選択されたリソースのみをバックアップする場合、オンデマンド・ジョブを実行します。オンデマンド・ジョブはバックアップ操作を即時に実行します。

- 単一リソースのオンデマンド・バックアップ・ジョブを実行するには、リソースを選択し、「**実行**」をクリックします。リソースがSLAポリシーに関連付けられていない場合、「**実行**」ボタンは使用できません。
- 1つ以上のリソースに対してオンデマンド・バックアップ・ジョブを実行するには、「**ジョブの作成**」をクリックし、「**アドホック・バックアップ**」を選択して、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の指示に従います。

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、[250 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

負荷のバランスを取るためのVADPプロキシを選択します。

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が設定されます。

「**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・サーバーにコピーされたリストア・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。

除外するファイル

ファイルの索引付け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 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選択して、「**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**」セクションのジョブに関連付けられ

ている「**ポリシー・オプション**」クリップボード・アイコン  アイコ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、バックアップや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。

バックアップ前にインベントリを実行

バックアップ・ジョブを開始する前に、インベントリ・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 プロキシを作成して負荷の共有を有効にすることを検討する。	252 ページの『VADP プロキシの作成』 を参照してください。
VMware リストア・ジョブ定義を作成する。	256 ページの『VMware データのリストア』 を参照してください。

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 に増やします。[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。

関連概念

487 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

481 ページの『オンデマンドでのジョブの開始』

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。

始める前に

バックアップ操作から 1 つ以上の VMDK を除外すると、リカバリーの正常な完了に影響を与える可能性があります。VM バックアップ操作からディスクを除外する前に、以下のシナリオについて考慮してください。

- インスタント・ディスク・リストアでは、リストア操作で VMDK が選択される場合は宛先として既存の VM が選択されます。IBM Spectrum Protect Plus では、リストアされたディスクを、選択された宛先 VM にマウントします。
- インスタント VM リストアでは、バックアップ中に除外された VMDK に仮想マシンのブートに必要なデータが含まれている場合、リストアされた VM はブートできない可能性があります。
- Windows ベースのゲストを使用する VM では、メイン・オペレーティング・システムがインストールされているディスク (通常は C: ドライブ) がバックアップ操作中に除外された場合、リストアされた VM がブートできない可能性があります。
- Linux ベースのゲストを使用する VM では、リストアされた VM が以下の場合に失敗することがあります。
 - ブートまたはルートの区画を含むディスクがバックアップから除外された場合。
 - バックアップ中にデータ (非ルート) 区画を含むディスクが除外され、データ・ボリュームで /etc/fstab に nofail オプションが指定されていない場合は、リストアされた VM に障害が起きる可能性があります。

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」 > 「仮想化システム (Virtualized Systems)」 > 「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を作成できます。これらのプロキシは、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。

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。差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にシフトされます。プロキシが存在しない場合、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 プロキシが一番すいていて、使用可能なメモリとフリー・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。

ジョブの開始前に、プロキシ・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、他のプロキシが引き継ぎ、ジョブが完了します。他のプロキシが存在しない場合、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・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・ジョブは、1 つ以上のプロキシ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・モードは一般的に高速で信頼性が高いため、直接ストレージ環境では推奨されません。
- HotAdd トランスポート・モードは、VADP プロキシが仮想化される場合に推奨されます。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。

注: 代替トランスポート・モードにフォールバックせずに HotAdd トランスポート・モードのみを使用するには、「[グローバル設定](#)」で「**VADP プロキシは HotAdd トランスポート・モードのみを使用する (VADP proxy uses only HotAdd transport mode)**」を選択します。詳しくは、[216 ページの『グローバル設定の構成』](#)を参照してください。

- 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 プロキシを作成できます。

始める前に

[31 ページの『VADP プロキシ要件』](#)に記載されている IBM Spectrum Protect Plus システム要件を確認します。

VADP プロキシ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 プロキシ許可の管理についての説明は、[509 ページの『許可タイプ』](#)を参照してください。

制約事項: VADP プロキシを作成するステップを実行するには、SYSADMIN 役割が割り当てられているユーザー ID があることを確認してください。役割について詳しくは、[507 ページの『役割の管理』](#)を参照してください。

ヒント: IBM Spectrum Protect Plus バージョンの VADP プロキシ・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・インストーラーにより、外部 VADP プロキシ・サポートに vSphere 6.5 が提供されます。

手順

VMware VADP プロキシを作成するには、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**」をクリックします。
2. 「**プロキシの登録**」をクリックします。
3. 「**VADP プロキシのインストール**」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・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・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。
5. 確認画面の「**はい**」をクリックします。
6. 作成するプロキシごとに、上記のステップを繰り返します。

タスクの結果

プロキシが「**VADP プロキシ**」テーブルに追加されます。省略符号アイコン *** をクリックしてアクション・メニューを開くことによって、プロキシ・サーバーの一時停止、アンインストール、登録抹消、または編集を行うことができます。プロキシを一時停止すると、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または登録解除されたプロキシ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。プロキシが一時停止されている間に、保守作業を実行できます。プロキシの使用を再開するには、省略符号アイコン *** をクリックしてアクション・メニューを開き、「再開」をクリックします。正常に作成された後、プロキシ・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。

IBM Spectrum Protect Plus 仮想アプライアンスと登録済み VADP プロキシ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 プロキシへの接続が、VADP プロキシには 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 プロキシへの適切な接続を確実にするには、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. コマンド ping <vadp_ip> を実行します。ここで、<vadp_ip> は、VADP プロキシの解決可能な 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 プロキシのコマンド・ラインに接続します。
2. コマンド 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 プロキシを作成後、以下のアクションを実行できます。

アクション	方法
VMware バックアップ・ジョブを実行する。	<p>245 ページの『VMware データのバックアップ』を参照してください。</p> <p>プロキシは、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。</p> <pre>Run remote vmdkbackup of MicroService: http://<proxy> nodename, IP:proxy_IP_address</pre>

関連タスク

[254 ページの『VADP プロキシのオプションの設定』](#)

IBM Spectrum Protect Plus で VADP プロキシを作成する場合、VADP プロキシごとにさまざまなオプションを構成できます。

vSnap サーバーでの VADP プロキシの登録

物理または仮想 vSnap サーバーで VADP プロキシのインストールと登録を行うことができます。vSnap サーバーで VADP プロキシをインストールして登録する場合、2つのシステムが同じマシン上にあるため、NFS マウントを除去することによってデータ移動を最適化するのに役立ちます。

始める前に

1 つ以上のスタンドアロン vSnap サーバーが環境内に正しくデプロイされ、構成され、IBM Spectrum Protect Plus バックアップ・ストレージ・プロバイダーに追加されなければなりません。手順については、109 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 vSnap サーバーの登録』を参照してください。


vSnap サーバーと VADP プロキシのシステム要件の組み合わせについては、[vSnap サーバー上の VADP プロキシの要件](#)を参照してください。

VADP プロキシ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 プロキシ許可の管理についての説明は、509 ページの『許可タイプ』を参照してください。

vSnap サーバーに関連付けられている ID は、vSnap サーバー上の VADP プロキシの登録に使用されるアカウントです。vSnap サーバーで VADP プロキシを登録すると、インストーラーがプッシュされ、VADP プロキシ・ソフトウェアを正常にインストールするための sudo 特権が必要です。vSnap サーバーに関連付けられた ID には、sudo 特権が必要です。

ヒント : vSnap サーバーを IBM Spectrum Protect Plus に追加する場合は、serveradmin ユーザー ID を使用してください。VADP プロキシを vSnap サーバーにデプロイする場合、必要なすべての特権が既にこのアカウントが使用されます。

手順

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。使用可能な vSnap サーバーが「ディスク・ストレージ」ペインのテーブルに表示されます。
2. VADP プロキシがインストールされ、登録される vSnap サーバーを選択します。
3. 「アクション」メニュー・アイコン  をクリックします。「VADP プロキシとして登録 (Register as VADP Proxy)」を選択します。
4. 「確認」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

プロセスが完了したら、「ディスク・ストレージ」ペインの表の「VADP プロキシ」列に緑色のチェック・マークが表示されます。

VADP プロキシのオプションの設定

IBM Spectrum Protect Plus で VADP プロキシを作成する場合、VADP プロキシごとにさまざまなオプションを構成できます。

始める前に

VADP プロキシ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 プロキシ許可の管理についての説明は、509 ページの『許可タイプ』を参照してください。

手順

VMware VADP プロキシ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」をクリックします。
2. 構成する VADP プロキシをクリックすると、隣接する詳細ペインにその情報が表示されます。

3. 「VADP プロキシ」の詳細ペインで、省略符号アイコン *** をクリックし、「プロキシ・オプション」を選択します。
4. 「VADP プロキシ・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。

「トランスポート・モード (番号付きリスト)」

プロキシが使用するトランスポート・モードを設定します。各モードを選択する順序によって、トランスポート・モードが使用される順序が決まります。トランスポート・モードを削除するには、トランスポート・モードの横にある削除アイコンをクリックします。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。使用可能な圧縮タイプには、**libz**、**fastlz**、および **skipz** があります。

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・サイズ

データ転送のバッファ・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・オプションを設定後、以下のアクションを実行できます。

アクション	方法
VMware バックアップ・ジョブを実行する	245 ページの『VMware データのバックアップ』 を参照してください。
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をアンインストールする	256 ページの『VADP プロキシのアンインストール』 を参照してください。

関連タスク

[252 ページの『VADP プロキシの作成』](#)

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 プロキシを作成できます。

VADP プロキシ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。

注：この手順は、環境内にインストールされている VADP プロキシにのみ適用されます。この手順は IBM Spectrum Protect Plus アプライアンスとともにデプロイされている VADP プロキシには適用されません。

1. ナビゲーション・ペインで、「システム構成」 > 「VADP プロキシ」をクリックします。
2. アンインストールしたい VADP プロキシをクリックすると、隣接する詳細ペインにその情報が表示されます。
3. 詳細ペインで省略符号アイコン *** をクリックし、「アンインストール」を選択します。

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、245 ページの『[VMware データのバックアップ](#)』を参照してください。
- バックアップ操作とリストア操作を実行できるように、IBM Spectrum Protect Plus ユーザーに適切な役割が割り当てられていることを確認してください。「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。詳しくは、503 ページの『[第 18 章 ユーザー・アクセスの管理](#)』および 512 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。
- 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。
- クローン・モードを利用し、元の IP 構成を使用して仮想マシンをリストアする場合は、バックアップ・ジョブ定義内の「ゲスト OS のユーザー名」および「ゲスト OS パスワード」オプションを使用して資格情報が設定されていることを確認してください。

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、その後クリーンアップされます。隔離ネットワークングにより安全な環境を確立し、実際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、263 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。

vSnap コピーから 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、コピー操作時に 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。

IBM Spectrum Protect アーカイブから VMware データをリストアする場合、ファイルはまず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。リストア操作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。

制約事項: 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。

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」>「仮想化システム (Virtualized Systems)」>「VMware」>「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。


ヒント:


- ウィザードは、「ジョブと操作」>「ジョブの作成」>「リストア」>「VMware」をクリックして開くこともできます。
- 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。
- ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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、作成する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。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。

4. 「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンドの単一リソースのリストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none">リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプが、デフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショット、複数リソースのリストア、または反復リストアの場合に表示されるフィールド

オプション	説明
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。

オプション	説明
	<p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

5. 「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。

オリジナルの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

このオプションは、vCenter Server をバイパスし、データを直接 ESXi ホストにリストアする場合に選択します。その他のリストア・シナリオでは、アクションは vCenter Server を介して実行します。vCenter Server が利用不可の場合、このオプションは、vCenter Server が依存するコンポーネントが含まれる仮想マシン (複数可) をリストアします。

ESXi ホストを選択する場合は、ホスト・ユーザーを指定する必要があります。ホストに対して既存のユーザーを選択するか、新規ユーザーを作成することができます。

ユーザーを作成するには、ユーザー名、ユーザー ID、およびユーザー・パスワードを入力します。

ESXi ホスト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。

ESXi ホストにデータをリストアするには、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分散スイッチが必要です。265 ページの『vCenter Server 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』の情報を参照して、このオプションを使用するために正しい環境が構成されていることを確認してください。

6. 「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 ESXi 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。
- オリジナルの ESXi ホストまたはクラスターにデータをリストアする場合、このページは表示されません。

7. 「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 ESXi 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。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 ESXi 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。

注: マッピングを追加するときには、+ ボタンで、フィールドにソース IP アドレスを入力する必要があります。宛先 IP アドレス情報は、「**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**」の各フィールドに入力する必要があります。再アドレス指定は、リストア対象のバックアップ・ジョブを実行する前に、VMware Tools がインストールされているマシンでのみ実行できます。

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。

8. 「**リストア方式**」ページで、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。
9. リストア・ジョブを拡張モードで実行している場合は、次のように追加のオプションを設定できます。

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、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。

ストリーミング (VADP) リストアの有効化

仮想マシンのリストア操作の並列ストリーミングは、デフォルトで設定されています。仮想マシンのリストア操作ではこのオプションを選択解除することができます。

ヒント : AWS Software-Defined Data Center (SDDC) で VMware Cloud (VMC) によって管理されている仮想マシンをリストアする場合は、データのストリーミングを許可するために常にこのオプションを有効にする必要があります。

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。

10. 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。
11. 「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。
12. 「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

241 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、[256 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」 > 「仮想化システム (Virtualized Systems)」 > 「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**」セッションの「**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

[241 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 Server 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 Server、または vCenter Server が使用するコンポーネントの 1 つがアクセス不能である場合に、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 Server が使用するコンポーネントを含む仮想マシンをリストアします。

始める前に

この手順を実行するには、ESXi および vCenter Server のユーザー・インターフェースについての知識が必要です。

このタスクについて

vCenter Server は以下のコンポーネントを使用します。

- 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 がダウンしている場合は ESX ホスト (ESX host if vCenter is down)**」オプションを使用するには、ESXi ホストに標準スイッチまたは分散スイッチが必要です。分散スイッチには一時バインディングが設定されている必要があります。これらのスイッチの一方または両方が使用可能な場合は、[256 ページの『VMware データのリストア』](#)で説明されている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できます。これ以上の手動構成は必要ありません。

どちらのスイッチも使用できない場合は、「**vCenter がダウンしている場合は ESX ホスト (ESX host if vCenter is down)**」オプションを使用できるようにするため、以下のステップを実行する必要があります。

手順

1. 宛先 ESXi ホストのユーザー・インターフェースに接続し、標準仮想スイッチを作成します。
新規スイッチにはポート・グループもアップリンクもありません。
2. セキュア・シェル (SSH) プロトコルを使用して ESXi ホストに接続します。
3. 次のコマンドを発行して ESXi ホストで構成されている分散スイッチをリストします。

```
#esxcli network vswitch dvs vmware list
```

4. リストア操作で使用したい分散スイッチの物理ネットワーク・インターフェース・カード (NIC) およびポート・グループを特定します。
5. 以下のコマンドを発行して、分散スイッチから物理 NIC およびポート・グループを削除します。

```
#esxconfig-vswitch -Q physical_unic -V port_group switch_name
```

6. 以下のコマンドを発行して、新規標準スイッチに物理 NIC およびポート・グループを追加します。

```
#esxcli network vswitch standard uplink add --uplink-name=physical_unic --vswitch-name=new_standard_vswitch
```

7. ESXi ホスト・ユーザー・インターフェースで、一時ポート・グループを追加し、ステップ [265 ページの『1』](#)で作成した標準スイッチを選択します。
標準スイッチには、1つのポート・グループと 1つのアップリンクが含まれます。
8. 「**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。
リストア操作を実行する手順については、[256 ページの『VMware データのリストア』](#)を参照してください。

9. ESXi ホストの ESXi ホスト・ユーザー・インターフェースで、リストアされた VM の電源をオンにします。
10. vCenter ユーザー・インターフェースにログインし、ステップ 265 ページの『7』で作成した一時ポート・グループから、使用可能な分散ポート・グループへの管理 VM のマイグレーションを開始します。
11. 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スイッチに再取り込みします。例えば、以下のコマンドは、ポート・グループ 64 に含まれる「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) を例として使用しています。
 - a. 次のコマンドを発行して、標準スイッチをネットワーク・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・カードを分散スイッチに追加します。

```
#esxcli network vswitch standard uplink add --uplink-name=vmnic0 --vswitch-name=vSwitch
```

例えば、次のようにします。

```
#esxcli network vswitch standard uplink add --uplink-name=vmnic0 --vswitch-name=vSwitch
```

12. 一時ポート・グループと標準スイッチを ESXi ホスト・ユーザー・インターフェースから 除去します。
13. VM がマイグレーションされてアクセス可能になった後、元のホストに到達可能な場合は、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。このオプションにより、VM は vCenter Server 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。データ・ストアではファイルはストレージ・スペースを消費します。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 37 ページの『[ハイパーバイザー \(Microsoft Hyper-V および VMware\) とクラウド・インスタンス \(Amazon EC2\) のバックアップとリストアの要件](#)』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。

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」 > 「仮想化システム (Virtualized Systems)」 > 「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」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。

「**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。268 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。	509 ページの『役割の作成』を参照してください。

関連タスク

269 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。

273 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・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**」 > 「**仮想化システム (Virtualized Systems)**」 > 「**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 Plus 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**」 > 「**仮想化システム (Virtualized Systems)**」 > 「**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・ジョブを定義する前に、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。詳しくは、[266 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、[157 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、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)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くてください。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。

このタスクについて

制約事項：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atalog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atalog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atalog・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・キーを追加してください。

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」 > 「仮想化システム (Virtualized Systems)」 > 「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: 選択された SLA ポリシーのジョブが実行されると、その SLA ポリシーに関連付けられているすべてのリソースがバックアップ操作に含まれます。選択されたリソースのみをバックアップする場合、オンデマンド・ジョブを実行します。オンデマンド・ジョブはバックアップ操作を即時に実行します。

- 単一リソースのオンデマンド・バックアップ・ジョブを実行するには、リソースを選択し、「実行」をクリックします。リソースが SLA ポリシーに関連付けられていない場合、「実行」ボタンは使用できません。
 - 1つ以上のリソースに対してオンデマンド・バックアップ・ジョブを実行するには、「ジョブの作成」をクリックし、「アドホック・バックアップ」を選択して、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の指示に従います。
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。「Hyper-V 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が設定されます。

「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 サーバーにコピーされたリストア・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・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、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て、「**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、バックアップや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。	273 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

[487 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

481 ページの『オンデマンドでのジョブの開始』

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、269 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。詳しくは、503 ページの『第 18 章 ユーザー・アクセスの管理』および 512 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。
- クローン・モードを利用し、元の IP 構成を使用して仮想マシンをリストアする場合は、バックアップ・ジョブ定義内の「**ゲスト OS のユーザー名**」および「**ゲスト OS パスワード**」オプションを使用して資格情報が設定されていることを確認してください。

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」 > 「仮想化システム (Virtualized Systems)」 > 「Hyper-V」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。


ヒント:


- ウィザードは、「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Hyper-V」をクリックして開くこともできます。
- 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。
- ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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、作成する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。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。

4. 「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンドの単一リソースのリストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リスト元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプが、デフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショット、複数リソースのリストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」 > 「サイト」 ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」 > 「バックアップ・ストレージ」 > 「オブジェクト・ストレージ」 ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」 ペインで定義されます。</p>

オプション	説明
	<p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1 次 スナップショットのリストア元の 1 次サイト。</p> <p>2 次 スナップショットのリストア元の 2 次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

5. 「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。

オリジナルの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。

6. 「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、このページは表示されません。

7.「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。

注: マッピングを追加するときには、+ ボタンで、フィールドにソース IP アドレスを入力する必要があります。宛先 IP アドレス情報は、「**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**」の各フィールドに入力する必要があります。再アドレス指定は、リストア対象のバックアップ・ジョブを実行する前に、VMware Tools がインストールされているマシンでのみ実行できます。

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。

8. 「**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。
9. 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。

10. 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。

11. 「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。

12. 「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

269 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。

266 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がキャプチャされるため、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。

Amazon EC2 データのバックアップとリストア

Amazon EC2 データを保護するには、最初に EC2 インスタンスのアカウントを IBM Spectrum Protect Plus に追加してから、それらのインスタンス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。

EC2 アカウントを IBM Spectrum Protect Plus に追加するには、アクセス・キーが必要です。アクセス・キーは、Identity and Access Management (IAM) ユーザーまたは Amazon Web Services (AWS) アカウントのルート・ユーザーの長期の資格情報です。

IBM Spectrum Protect Plus に必要なアクセス・キーと権限を使用して IAM ユーザーを作成する方法については、[280 ページの『AWS IAM ユーザーの作成』](#)を参照してください。

セキュリティを強化するために、AWS アカウントのルート・ユーザーを IBM Spectrum Protect Plus に使用しないことをお勧めします。ルート・ユーザーについては、[AWS Identity and Access Management User Guide](#) を参照してください。

EC2 データは、vSnap サーバーではなく、Amazon Web Services (AWS) Elastic Block Store (EBS) スナップショットに保管されます。IBM Spectrum Protect Plus は、これらのスナップショットをバックアップ操作およびリストア操作に管理します。

ご使用の EC2 環境が [37 ページの『ハイパーバイザー \(Microsoft Hyper-V および VMware\) とクラウド・インスタンス \(Amazon EC2\) のバックアップとリストアの要件』](#) 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。

AWS IAM ユーザーの作成

IBM Spectrum Protect Plus ユーザー・インターフェースでタスクを実行するには、IAM ユーザーがアクセス・キー、および必須許可を持っている必要があります。

このタスクについて

AWS マネジメントコンソールを使用して IAM ユーザーを作成するには、以下のステップを利用します。これらのステップは、IBM Spectrum Protect Plus に必要な設定を表示するために、[AWS Identity and Access Management User Guide](#) に記載されているステップを要約したものです。IAM ユーザーを作成するための詳しい完全なステップについては、このガイドを参照してください。

ユーザーを作成するには、IAM 管理権限が必要です。

手順

1. [AWS Management Console](#) にサインインし、「サービス」 > 「IAM」をクリックして IAM 管理コンソールを開きます。
2. コンソール・ナビゲーション・ペインで、「ユーザー」 > 「ユーザーの追加」をクリックします。
3. 新しいユーザーのユーザー名を入力します。
4. AWS アクセス・タイプに「プログラムによるアクセス」を選択します。
このアクセス・タイプは、IBM Spectrum Protect Plus によって必要とされるアクセス・キーを作成するために必要です。IBM Spectrum Protect Plus では、アクセス・タイプ「**AWS マネジメントコンソールのアクセス (AWS Management Console access)**」は必要ありません。
5. 「次のステップ: アクセス権限」をクリックします。
6. 「既存のポリシーを直接アタッチ」をクリックしてから、「ポリシーの作成」をクリックします。
「ポリシーの作成」ページは新しいブラウザ・ウィンドウで開きます。
7. 「JSON」タブをクリックして、以下のアクションを入力します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DetachVolume",
        "ec2:AttachVolume",
        "ec2:DeregisterImage",
        "ec2:DeleteSnapshot",
        "ec2:DescribeInstances",
        "ec2:CreateVolume",
        "ec2:DescribeTags",
        "ec2:CreateTags",
        "ec2:RegisterImage",
        "ec2:DescribeRegions",
        "ec2:RunInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateSnapshots",
        "ec2:DescribeVolumes",
        "ec2:CreateSnapshot",
        "ec2:DescribeSubnets",
        "iam:PassRole"
      ],
      "Resource": "*"
    }
  ]
}
```

8. 「ポリシーの確認」をクリックします。
9. 作成するポリシーの名前と説明 (オプション) を入力します。
10. 「要約 (Summary)」セクションを参照して、ポリシーによって付与されたアクセス権限を確認します。
11. 「ポリシーの作成」をクリックします。

12. ブラウザー・ウィンドウを閉じて、「**ユーザーを追加**」ページが表示されているウィンドウに戻ります。
13. ポリシー・リストから、作成したポリシーを選択します。
14. オプション: アクセス権限の境界を設定します。
15. 「**次のステップ: タグ**」をクリックします。
16. オプション: タグをキー/値のペアとして添付し、メタデータをユーザーに追加します。
タグを使用して、EC2 データのバックアップまたはリストア時にリソースをフィルターに掛けることができます。
17. 「**次のステップ: 確認**」をクリックします。
18. 選択項目を確認してから、「**ユーザーの作成**」をクリックします。
新規ウィンドウが開き、ユーザー名、アクセス・キー、およびシークレット・キーが表示されます。
19. シークレット・キーを表示するには、シークレット・キーの横にある「**表示**」をクリックします。
20. アクセス・キー ID とシークレット・アクセス・キーをコンピューター上の CSV ファイルに保存するには「**.csv のダウンロード**」をクリックします。
このファイルは安全な場所に保管してください。このダイアログ・ボックスがクローズすると、シークレット・アクセス・キーに再びアクセスすることはできません。
21. 「**クローズ**」をクリックして、ウィンドウをクローズします。

次のタスク

EC2 のアカウントを追加します。アカウントを作成するには、[281 ページの『Amazon EC2 アカウントの追加』](#)の手順に従います。

Amazon EC2 アカウントの追加

Amazon EC2 アカウントが IBM Spectrum Protect Plus に追加されると、そのアカウントに関連付けられているインスタンスのインベントリーがキャプチャーされます。その後、バックアップ・ジョブとリストア・ジョブを実行し、インスタンスのレポートを生成することができます。

始める前に

EC2 アカウントの追加には、アクセス・キーが必要です。アクセス・キーは、IBM Spectrum Protect Plus が、データ保護のために EC2 インスタンスに接続し、インベントリーを作成できるようにします。既に IBM Spectrum Protect Plus に入力されているアクセス・キーは、選択リストに表示されます。使用したいアクセス・キーがリスト内にない場合、そのアクセス・キーとセキュリティー・キーを追加する必要があります。追加したいアクセス・キーと秘密鍵があることを確認してください。

手順

EC2 アカウントを追加するには、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**」 > 「**仮想化システム (Virtualized Systems)**」 > 「**Amazon EC2**」をクリックします。
2. 「**アカウントの管理**」をクリックします。
3. 「**アカウントの追加**」をクリックします。
4. 「**アカウント・プロパティー (Account Properties)**」セクションのフィールドにデータを設定します。

アカウント名

アカウント用に選択したアクセス・キーを識別するために、分かりやすい名前を入力します。

既存のアクセス・キーを使用する

アカウントについて以前に入力されたアクセス・キーを指定するには、このオプションを選択してから、「**キーの選択**」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。

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。

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、EC2 アカウントがデータベースに追加され、アカウント・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、入力内容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。

次のタスク

EC2 アカウントを IBM Spectrum Protect Plus に追加すると、そのアカウントに関連付けられている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。インスタンスを確実にバックアップできるようにするには、インスタンスが検出されなければなりません。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、[282 ページの『Amazon EC2 インスタンスの検出』](#)を参照してください。

関連タスク

[282 ページの『Amazon EC2 データのバックアップ』](#)

バックアップ・ジョブを使用して Amazon EC2 データをバックアップします。

[284 ページの『Amazon EC2 データのリストア』](#)

リストア・ジョブを使用して、EC2 データをバックアップ・コピーからリストアします。例えば、インスタンスのデータが失われたり、破壊されたりした場合などにリストアを行います。ジョブを定義して、元のアベイラビリティ・ゾーンまたは同じリージョンの異なるアベイラビリティ・ゾーンにデータをリストアすることができます。その際に、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。

Amazon EC2 インスタンスの検出

Amazon EC2 インスタンスは、EC2 アカウントが 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、アカウント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」 > 「仮想化システム (Virtualized Systems)」 > 「Amazon EC2」をクリックします。
2. EC2 アカウントのリストで、アカウント (複数可) を選択するか、アカウントのリンクをクリックして、インベントリーを作成するリージョンまたはインスタンスにナビゲートします。
ナビゲーションは、「注文アカウント (order account)」 > 「リージョン (region)」 > 「instance (インスタンス)」内にあります。
3. 「インベントリーの実行」をクリックします。

Amazon EC2 データのバックアップ

バックアップ・ジョブを使用して Amazon EC2 データをバックアップします。

始める前に

以下のステップを実行してください。

1. バックアップするアカウントが IBM Spectrum Protect Plus に追加されていることを確認してください。詳しい手順については、[281 ページの『Amazon EC2 アカウントの追加』](#)を参照してください。
2. EC2 インスタンスに対して 1 つ以上の SLA ポリシーが構成されていることを確認してください。詳しい手順については、[232 ページの『Amazon EC2 インスタンスの SLA ポリシーの作成』](#)を参照してください。
3. リストア・ジョブをセットアップするユーザーに 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ことを確認してください。役割の割り当てについて詳しくは、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)を参照してください。


4. アカウントが複数の 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。

手順

EC2 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」 > 「仮想化システム (Virtualized Systems)」 > 「Amazon EC2」をクリックします。
2. 以下のいずれかのアクションを実行して「Amazon EC2 バックアップ」ペインでバックアップするインスタンスを選択します。
 - EC2 アカウントに関連付けられているすべてのインスタンスを選択するには、そのアカウントのチェック・ボックスを選択します。このアカウントに追加されたインスタンスは、選択した SLA ポリシーに自動的に割り当てられます。
 - リージョンまたは特定インスタンスによってインスタンスを選択するには、アカウント名をクリックし、リージョンまたはインスタンスに移動します。ナビゲーションは、「注文アカウント (order account)」 > 「リージョン (region)」 > 「instance (インスタンス)」内にあります。インスタンスに割り当て名がない場合、インスタンス ID がインスタンス名として表示されます。

使用可能なインスタンスを検索するには、検索機能を使用し、「表示」フィルターで使用して表示されたインスタンスを切り替えます。選択可能なオプションは、「インスタンス」および「タグ」です。

3. 「SLA ポリシーの選択」をクリックして、バックアップ基準に合う 1 つ以上の SLA ポリシーを、「SLA ポリシーのステータス」テーブルのジョブ定義に追加します。
4. オプション: 定義に追加した SLA ポリシーの追加オプションを構成するには、「SLA ポリシーのステータス」表の「ポリシー・オプション」列で、SLA ポリシーのクリップボード・アイコン  をクリックして、以下のオプションを設定します。

ジョブがすで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。

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。

このオプションが無効になっている場合は、バックアップや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・ジョブを実行し、選択されたインスタン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・ジョブから特定のインスタンスを除外します。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。

5. 「保存」をクリックして、ジョブ定義を作成します。

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。ジョブをすぐに実行するには、「**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: 選択された SLA ポリシーのジョブが実行されると、その SLA ポリシーに関連付けられているすべてのインスタンスがバックアップ操作に含まれます。選択されたインスタンスのみをバックアップする場合、オンデマンド・ジョブを実行します。オンデマンド・ジョブはバックアップ操作を即時に実行します。

- 単一インスタンスのオンデマンド・バックアップ・ジョブを実行するには、インスタンスを選択し、「**実行**」をクリックします。リソースが SLA ポリシーに関連付けられていない場合、「**実行**」ボタンは使用できません。
- 1 つ以上のインスタンスに対してオンデマンド・バックアップ・ジョブを実行するには、「**ジョブの作成**」をクリックし、「**アドホック・バックアップ**」を選択して、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の指示に従います。

次のタスク

EC2 バックアップ・ジョブの定義後、EC2 リストア・ジョブ定義を作成します。

関連概念

[487 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

[284 ページの『Amazon EC2 データのリストア』](#)

リストア・ジョブを使用して、EC2 データをバックアップ・コピーからリストアします。例えば、インスタンスのデータが失われたり、破壊されたりした場合などにリストアを行います。ジョブを定義して、元のアベイラビリティ・ゾーンまたは同じリージョンの異なるアベイラビリティ・ゾーンにデータをリストアすることができます。その際に、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。

[481 ページの『オンデマンドでのジョブの開始』](#)

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。

Amazon EC2 データのリストア

リストア・ジョブを使用して、EC2 データをバックアップ・コピーからリストアします。例えば、インスタンスのデータが失われたり、破壊されたりした場合などにリストアを行います。ジョブを定義して、元のアベイラビリティ・ゾーンまたは同じリージョンの異なるアベイラビリティ・ゾーンにデータをリストアすることができます。その際に、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

以下のタスクを実行してください。

- EC2 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、[282 ページの『Amazon EC2 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するユーザーに 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ことを確認してください。役割の割り当てについては詳しくは、[503 ページの『第 18 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

IBM Spectrum Protect Plus では、インスタンスの長期コピーを作成する際にクローン・モードを使用します。

手順

EC2 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」 > 「仮想化システム (Virtualized Systems)」 > 「Amazon EC2」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。


ヒント:

- ウィザードは、「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Amazon EC2」をクリックして開くこともできます。
- 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。
- ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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) リスト内のアカウントをクリックして、リストア操作に使用できるインスタンスを表示します。検索機能を使用して使用可能なインスタンスを検索することができます。検索基準に一致するインスタンスを見つけるには、名前の全体または一部を入力します。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。

表示されたインスタンスを切り替えるには、「表示」 フィルターを使用します。

- b) リストア操作のソースとして使用するインスタンスの横にあるプラス・アイコン  をクリックします。

複数のインスタンスをリストから選択できます。ただし、選択されたインスタンスはすべて同じリージョン内になければなりません。

インスタンスに接続済みのボリュームがある場合は、そのボリュームにナビゲートし、リストア操作用に選択することができます。インスタンスと接続済みのボリュームの両方を選択することはできません。

選択したインスタンスまたは接続済みのボリュームが、アカウント・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」 ページのフィールドに入力して、リストアするインスタンス・スナップショットを選択し、「次へ」 をクリックして続行します。

表示されるフィールドは、「ソースの選択」 ページで選択されたインスタンスの数によって異なります。

- 単一インスタンスを選択した場合、リストアするスナップショットの日付範囲を選択してください。その日付範囲で使用可能なスナップショットがリストされます。リストアしたいスナップショットを選択します。
- 複数のインスタンスを選択した場合、リストアするスナップショットの日付範囲を選択してください。その日付範囲内にスナップショットがあるインスタンスがリストされます。インスタンスごとに、リストアしたいリストア・ポイントを選択します。

4. 「宛先の設定」 ページで、インスタンスをリストアする先のアベイラビリティ・ゾーンを指定して、「次へ」 をクリックします。

オリジナル・アベイラビリティ・ゾーン (Original Availability Zone)

オリジナル・アベイラビリティ・ゾーンにインスタンスをリストアするには、このオプションを選択します。

代替アベイラビリティ・ゾーン (Alternate Availability Zone)

オリジナル・アベイラビリティ・ゾーンとは異なるアベイラビリティ・ゾーンにインスタンスをリストアするには、このオプションを選択します。そして、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。

接続済みのボリュームをリストアする場合は、代替アベイラビリティ・ゾーンで宛先インスタンスを選択し、「宛先の添付 (Destination Attachment)」セクションにオプションでデバイス名を入力します。

5. 「宛先の設定」 ページで「代替アベイラビリティ・ゾーン」を選択した場合は、「ネットワークの設定」 ページの各アベイラビリティ・ゾーンのサブネットを変更します。「オリジナル・アベイラビリティ・ゾーン」を選択した場合は、このページには設定がありません。「次へ」をクリックして先に進みます。
アベイラビリティ・ゾーンのサブネットは、ステップ 285 ページの『2』で選択されているインスタンスと同じリージョンになければなりません。
6. 「リストア方式」 ページで、「インスタンスの名前変更 (オプション) (Rename Instance (optional))」に新規インスタンス名を入力して、リストアされたインスタンスの名前を変更できます。「次へ」をクリックして先に進みます。
7. リストア・ジョブを拡張モードで実行している場合は、次のように追加のオプションを設定できます。

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インスタンスの電源状態を切り替えます。インスタンスは、リカバリーされた順序で電源オン状態になります。

失敗した場合でもリストアを続行します

直前のインスタンス・リカバリーが失敗した場合、シリーズ内でインスタン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、インスタン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

インスタンス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。

インスタンス・タグのリストア

vSphere を使用してインスタンス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。

インスタンス名の前に接頭部を付加します

リストアされたインスタンスの名前に付加する接頭部を入力します。

インスタンス名に接尾部を付加します

リストアされたインスタンスの名前に付加する接尾部を入力します。


8. 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。

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ジョブが始まると、すぐに「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。

関連タスク

281 ページの『Amazon EC2 アカウントの追加』

Amazon EC2 アカウントが IBM Spectrum Protect Plus に追加されると、そのアカウントに関連付けられているインスタンスのインベントリがキャプチャーされます。その後、バックアップ・ジョブとリストア・ジョブを実行し、インスタンスのレポートを生成することができます。

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。

- 40 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・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・サーバーにコピーされたリストア・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atalog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ATALOG・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atalog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atalog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、*xfspgros* 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、*xfspgros* 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、*xfspgros* をバージョン 4.2.0 以降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. ファイルを名前を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、537 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。

注：指定された日付範囲内にスナップショットが取られたファイル・オブジェクトのみが表示されます。そのオブジェクトの場合、ファイル・オブジェクトの横に矢印がクリックされると、そのファイル・オブジェクトの以前のすべてのスナップショットが表示されます。

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

[245 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。

[256 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 11 章 ファイル・システムの保護

保護するディレクトリーとファイルを格納しているファイル・システムを IBM Spectrum Protect Plus に登録できます。保護するデータを格納しているファイル・システム・サーバーおよびドライブを選択してください。Microsoft Windows の ReFS ファイル・システムおよび NTFS ファイル・システムを IBM Spectrum Protect Plus に登録して、バックアップ・ジョブや定期的にスケジュールされる SLA ポリシーをセットアップすることができます。

ドライブ名に割り当てられているローカル・ファイル・システムを保護できます。クラスター化ボリュームおよびドライブ共有は、IBM Spectrum Protect Plus によって保護されません。

Windows ファイル・システム

Microsoft Windows NTFS または ReFS ファイル・システム をホストするマシンを IBM Spectrum Protect Plus に正常に登録した後、リストされているボリュームおよびドライブでデータの保護を開始できます。ファイル・システム・データのオンデマンド・バックアップを作成したり、定期的なスケジュール済みバックアップ・ジョブを実行するための SLA ポリシーをセットアップしたりすることができます。

ファイル・システムが配置されている環境が最小システム要件を満たしていることを確認してください。システムの要件について詳しくは、[47 ページの『ファイル・システムの要件』](#)を参照してください。

登録するマシンの IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。両方のサーバーで、Windows Remote Management サービスがポート 5985 で listen している必要があります。

完全修飾ドメイン名は、解決可能で、IBM Spectrum Protect Plus アプライアンス・サーバーおよび vSnap サーバーから経路指定できる必要があります。

ファイル・システムの前提条件

リソースの保護を開始する前に、ファイル・システムで IBM Spectrum Protect Plus を使用するためのすべての前提条件が満たされている必要があります。

IBM Spectrum Protect Plus を使用してファイル・システムを操作するための要件は、[47 ページの『ファイル・システムの要件』](#)で確認できます。

注：Windows ファイル・サーバーを登録するためのユーザー ID は、以下のいずれかの Windows 構成でセットアップできます。

- ユーザー・アカウント制御 (UAC) セキュリティー・コンポーネントが無効に設定されたローカル・システム管理者 ユーザー・アカウント。このユーザーとして、Windows システムの「**コントロール パネル**」 > 「**ユーザー アカウント制御の設定**」を開き、スライダーを「**通知しない**」に移動する必要があります。
- 管理者承認モードのセキュリティ・ポリシー設定が無効になっているローカル管理者グループのメンバーであるユーザー。このユーザーとして、Windows システムの「**ローカル セキュリティ ポリシー**」を開く必要があります。「**セキュリティの設定**」メニューから、「**ローカル ポリシー**」 > 「**セキュリティ オプション**」 > 「**ユーザー アカウント制御：管理者承認モードですべての管理者を実行する**」ポリシーを選択し、このオプションを「**無効**」に設定します。ローカル管理者グループに「**サービスとしてログオン**」ポリシー・オプションが含まれていることを確認します。

スペースの前提条件

保護するファイル・システムをホストしているマシンに十分なスペースがあることを確認してください。スペース所要量について詳しくは、[292 ページの『ファイル・システムを保護するためのスペース所要量』](#)を参照してください。データを代替ロケーションにリストアする場合は、追加のスペースを使用できるようにしてください。リストア・プロセス中、どのファイルも上書きされません。同じ名前のファイルが検出された場合は、両方のコピーが保持されます。

Windows 用のセキュリティ証明書の取り扱い

IBM Spectrum Protect Plus でファイル・システム・ファイルを保護するためのアクセスを確保するには、証明書を作成し、その配置を管理する必要があります。

このタスクについて

注: リストア・サービスが証明書をロードできない場合は、ファイルが削除され、新しい自己署名証明書および鍵が作成されます。

ヒント: IBM Spectrum Protect Plus ファイル・システム・エージェントが実行されている場合は、自己署名証明書と鍵が %LOCALAPPDATA%\FSPA\ で見つかります。エージェントがまだ実行されていない場合、自己署名証明書と鍵を作成して移動する手順を実行してください。

管理者は、次のパスでこのディレクトリーにアクセスできます。C:\Users\Administrator\AppData\Local\

手順

1. クライアント・マシンの鍵および署名付き証明書を作成します。
ファイルのロードに影響するため、鍵も証明書も、パラフレーズの保護を使用できません。
2. FSPA というディレクトリー・フォルダーを、%LOCALAPPDATA%\FSPA のような場所に作成します。
3. 鍵と証明書をコピーして、FSPA フォルダーに置きます。
4. このフォルダー内の鍵と証明書をコピーします。
5. 鍵の名前を localfspagent.key に変更します。
6. 証明書の名前を localfspagent.crt に変更します。

ファイル・システムを保護するためのスペース所要量

登録されているファイル・システムに保管されている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、ソース・ホスト、および vSnap リポジトリ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。

ファイル・システムの追加

ReFS または NTFS ファイル・システム上のデータの保護を開始するには、ファイル・システムが置かれているホスト・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。

始める前に

注: Windows ファイル・サーバーを登録するためのユーザー ID は、以下のいずれかの Windows 構成でセットアップすることができます。

- ユーザー・アカウント制御 (UAC) セキュリティー・コンポーネントが「無効」に設定されているローカル・システム管理者ユーザー・アカウント。このユーザーとして、Windows システムの「コントロールパネル」>「ユーザー アカウント制御の設定」を開き、スライダーを「通知しない」に移動する必要があります。
- 管理者承認モードのセキュリティ・ポリシー設定が無効になっているローカル管理者グループのメンバーであるユーザー。このユーザーとして、Windows システムの「ローカル セキュリティ ポリシー」を開く必要があります。「セキュリティの設定」メニューから、「ローカル ポリシー」>「セキュリティ オプション」>「ユーザー アカウント制御: 管理者承認モードですべての管理者を実行する」ポリシーを選択し、このオプションを「無効」に設定します。ローカル管理者グループに「サービスとしてログオン」ポリシー・オプションが含まれていることを確認してください。

このタスクについて

ファイル・システムを IBM Spectrum Protect Plus に追加するには、マシンの DNS 名または IP アドレス、ユーザー ID、およびパスワードが必要です。

手順

1. ナビゲーションで、「保護の管理」 > 「ファイル・システム」 > 「Microsoft Windows」を展開します。
2. 「Microsoft Windows」 ページで、「ファイル・サーバーの管理 (Manage file servers)」をクリックし、「ファイル・サーバーの追加 (Add file server)」をクリックしてホスト・サーバーを追加します。

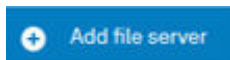


図 22. ファイル・システム・サーバーの追加

3. 「ファイル・サーバー・プロパティ (File server properties)」セクションで、マシンの DNS 名または IP アドレスを入力します。
4. 追加しようとしている Windows サーバーのユーザーのタイプを指定します。
 - ・ 既存のユーザー ID とパスワードを使用します。
 - ・ 新しいユーザー ID とパスワードを入力します。

注: Windows ファイル・システムを登録するためのユーザー ID は、以下のいずれかの Windows 構成でセットアップする必要があります。

- ・ ユーザー・アカウント制御 (UAC) セキュリティー・コンポーネントが「無効」に設定されているローカル・システム管理者ユーザー・アカウント。このユーザーとして、Windows システムの「コントロールパネル」で「ユーザー アカウント制御の設定」ダイアログにアクセスし、スライダーを「通知しない」に移動する必要があります。
- ・ 管理者承認モードのセキュリティー・ポリシー設定が無効になっているローカル管理者グループのメンバーであるユーザー。このユーザーとして、Windows システムの「ローカル セキュリティ 設定」ダイアログにアクセスし、「ユーザー アカウント制御: 管理者承認モードですべての管理者を実行す」ポリシー設定を無効にする必要があります。ローカル管理者グループに「サービスとしてログオン」ポリシー・オプションが含まれていることを確認してください。

The screenshot shows the 'Manage file servers' dialog box. It has a title bar 'Microsoft Windows' and a subtitle 'Manage file servers'. Below the subtitle is a section 'File server properties' with fields for 'Host Address', 'Use existing user' (checkbox), 'User ID' (containing 'domain/user'), and 'Password' (containing 'Password'). Below this is an 'Options' section with a field for 'Maximum parallel file systems' (containing '10'). At the bottom are 'Cancel' and 'Save' buttons. A 'Create job' button is visible in the top right corner of the window.

図 23. エージェント・ユーザーの管理

重要: ユーザー ID を入力するときに、ドメインを入力する必要はありません。

5. 保護されるファイル・システムからデータをバックアップするために使用される並列ファイル・システムの最大数を設定します。

この設定は、このホスト上の各ファイル・システムに適用されます。オプションの値が2以上に設定される場合、複数のリソースを並列にバックアップすることができます。複数の並列ファイル・システムによりリストア操作の速度が向上する可能性があります。

6. フォームを保存します。

次のタスク

ファイル・システム・ホストを IBM Spectrum Protect Plus に追加すると、関連するボリュームおよびドライブを検出するために、インベントリーが自動的に実行されます。

ドライブとボリューム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、開始されたインベントリーに対応するアプリケーション・サーバー・インベントリー・ログ・エントリーを探します。

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。

ファイル・システム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、[ファイル・システムの検出](#)を参照してください。

ファイル・システムを検出するためのインベントリーの実行

ファイル・システムを IBM Spectrum Protect Plus に追加した後、ボリューム、ドライブ、およびマウント・ポイントを検出するための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、選択されたホストで検出されるファイル・システム・リソースの検出、リスト、保管が行われ、データを IBM Spectrum Protect Plus で保護できるようになります。

始める前に

ファイル・システムを 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、[ファイル・システムの追加](#)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**」 > 「**ファイル・システム**」 > 「**Microsoft Windows**」を展開します。

ヒント: ファイル・システムを「**サーバー**」ペインに追加するには、[ファイル・システムの追加](#)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。

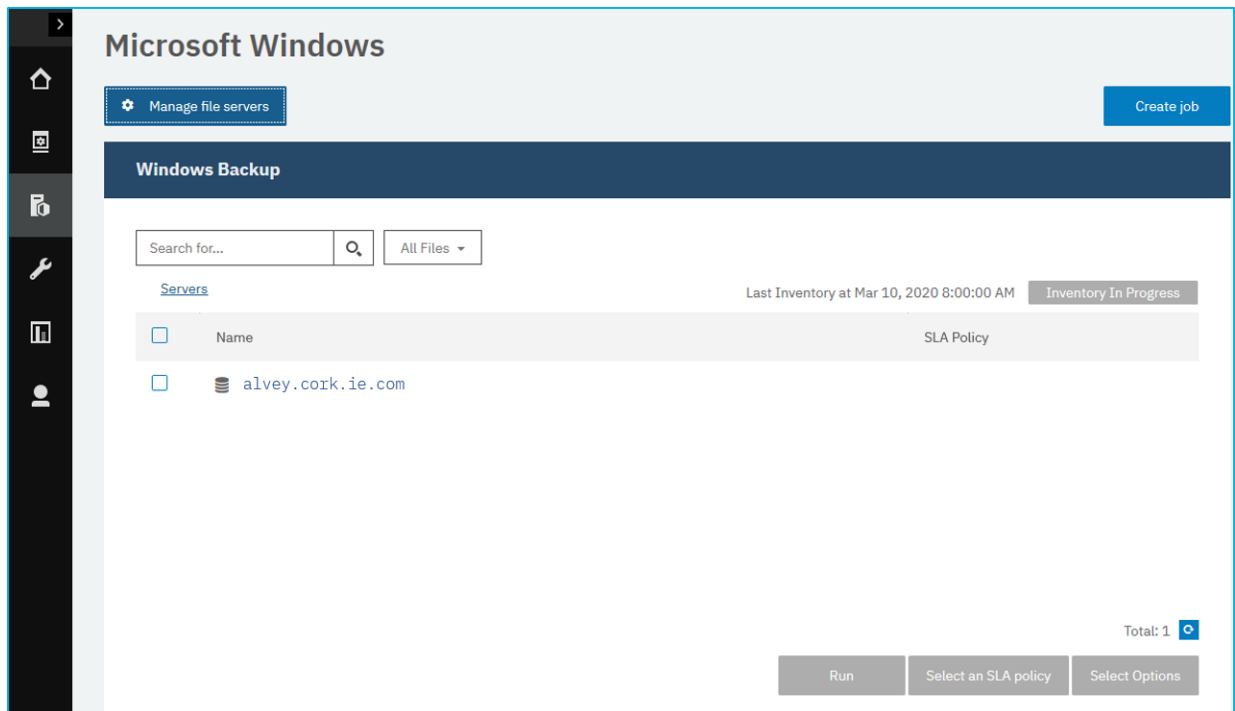


図 24. ファイル・システムの検出

インベントリの実行中、テキストが変わって「インベントリが進行中」を表示します。任意の使用可能なファイル・システムサーバーでインベントリを実行できますが、インベントリ・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・ログ・エントリを見つけます。

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。ジョブが表示されない場合は、「ジョブ・ヒストリー期間」を調整して時間間隔を長くします。

3. サーバーをクリックして、そのサーバーで検出されたボリューム、ドライブ、およびマウント・ポイントを示すビューを開きます。「サーバー」リストでエントリが欠落している場合は、ファイル・システムを確認して、インベントリを再実行します。場合によっては、特定のエントリにバックアップに不適格というマークが付けられていることがあります。そのエントリ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: サーバーのリストに戻るには、「サーバー」ハイパーテキストをクリックしてください。

ファイル・システム 接続のテスト

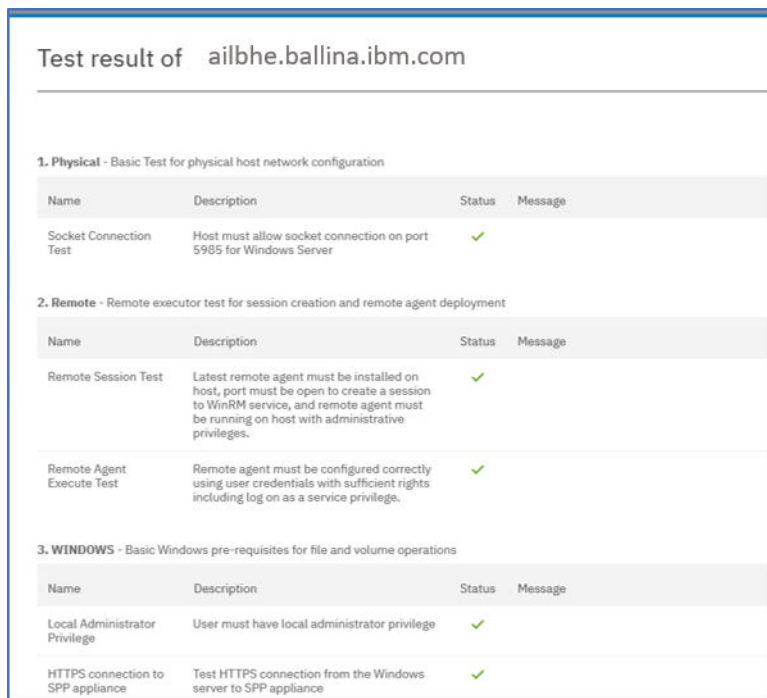
ファイル・システムを追加した後、接続をテストできます。テストでは、サーバーとの通信と、IBM Spectrum Protect Plus と ファイル・システムサーバーの間の DNS 設定が検証されます。

手順

1. ナビゲーション・ペインで、「保護の管理」 > 「ファイル・システム」 > 「Microsoft Windows」をクリックします。
2. 「Microsoft Windows」ウィンドウで、「ファイル・サーバーの管理 (Manage file servers)」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。

使用可能なマシン・ホストのリストが表示されます。

3. 「アクション」をクリックし、「テスト」を選択して、物理ネットワーク接続、リモート・アクセス、および Windows の特権接続と設定の検証テストを開始します。



Test result of aibhe.ballina.ibm.com

1. Physical - Basic Test for physical host network configuration			
Name	Description	Status	Message
Socket Connection Test	Host must allow socket connection on port 5985 for Windows Server	✓	

2. Remote - Remote executor test for session creation and remote agent deployment			
Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, port must be open to create a session to WinRM service, and remote agent must be running on host with administrative privileges.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient rights including log on as a service privilege.	✓	

3. WINDOWS - Basic Windows pre-requisites for file and volume operations			
Name	Description	Status	Message
Local Administrator Privilege	User must have local administrator privilege	✓	
HTTPS connection to SPP appliance	Test HTTPS connection from the Windows server to SPP appliance	✓	

図 25. 接続のテスト

テスト・レポートに、実行された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、ホスト上のリモート・サーバー・インストールのテスト、および Windows の接続と特権のテストで構成されています。

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。

ファイル・システム・データのバックアップ

通常のバックアップ・ジョブを定義し、ファイル・システム・データを保護するためのバックアップ・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。差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 ファイル・システム・エージェントは、バックアップが実行される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 ファイル・システム サーバーを追加します。手順については、[ファイル・システム サーバーの追加](#)を参照してください。
- このタスクで説明されているとおり、SLA ポリシーを構成します。
- 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、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)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。

パスが 255 文字を超えている場合、バックアップ操作は失敗します。パスが 255 文字より長い場合は、Windows ポリシー・エディターで「Win32 の長いパスを有効にする」オプションを使用して、長いパスを使用可能にする必要があります。

注: ファイル・システム共有も、Microsoft クラスター・ボリュームも、IBM Spectrum Protect Plus で保護できません。

このタスクについて

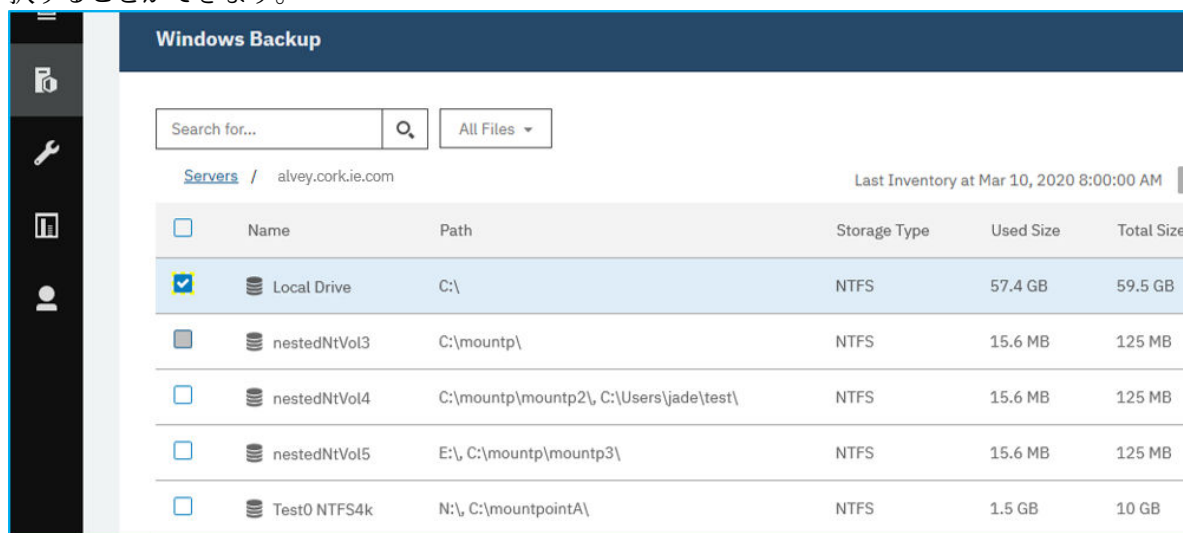
以下のステップでは、SLA ポリシーに割り当てられたリソースをバックアップする方法について説明します。リソースが既に SLA ポリシーに関連付けられているかどうかに関係なく、1 つ以上のリソースに対してオンデマンド・バックアップ・ジョブを実行するには、「**ジョブの作成**」をクリックし、「**アドホック・バックアップ (Ad hoc backup)**」を選択し、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の手順を実行します。

手順

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**ファイル・システム**」 > 「**Microsoft Windows**」を展開します。
2. 「**Windows バックアップ**」ペインで、バックアップするファイル・システム・サーバーを選択します。
 - サーバー名のチェック・ボックスをクリックして、ファイル・システム・サーバー全体を選択することができます。このサーバーに追加されるデータはすべて、選択する SLA ポリシーに割り当てられ

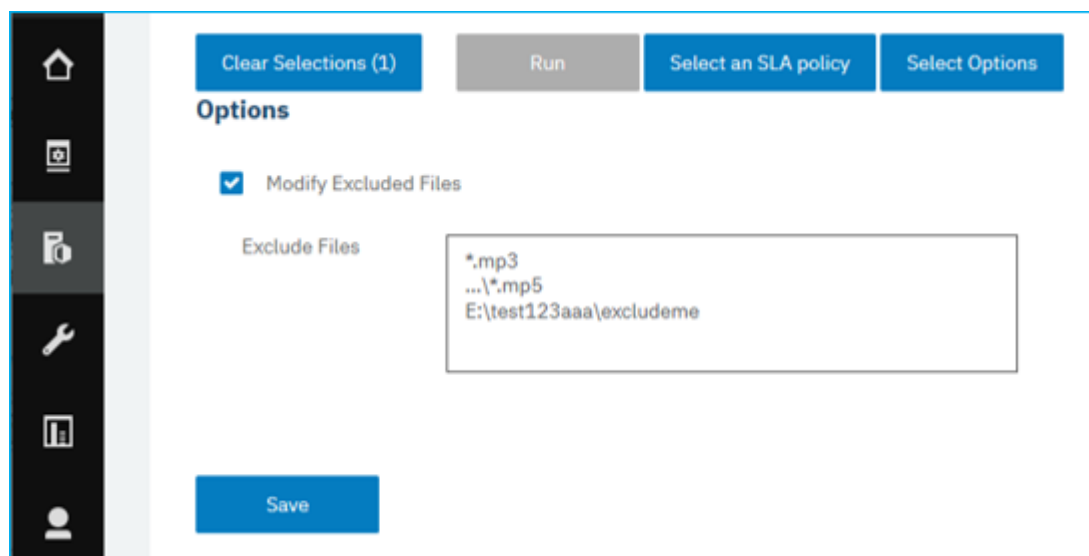
ます。

- あるいは、サーバー名をクリックし、リストからドライブまたはマウント・ポイントを選択することによって、特定のファイル・システム・サーバーから特定のドライブまたはマウント・ポイントを選択することができます。



3. 「**オプションの選択**」をクリックして、セットアップするバックアップ・ジョブから除外されるファイルを指定します。あるいは、「**除外されるファイルの変更 (Modify Excluded Files)**」をクリックして、除外ルールを既に定義されているままにすることができます。「**保存**」をクリックして変更内容をコミットします。

ドライブからすべてのファイルを除外する場合は、ドライブまたはドライブ内のフォルダー (例: Z:\test) を指定することができます。特定のタイプのすべてのファイルをバックアップ・ジョブから除外したい場合は、ストリング (例: *.png) を使用して、その除外を指定できます。




- ヒント: 変更を保存せずに「オプション」ペインを閉じるには、「オプションの選択」をクリックします
4. バックアップ用のファイル・システム・サーバー、ドライブ、またはマウント・ポイントを選択し、「SLA

ポリシーの選択」 **Select an SLA policy** をクリックして、その項目の SLA ポリシーを選択します。オプション「ゴールド」、「シルバー」、または「ブロンズ」の中から選択できます。以下の図に示されているように、各ポリシー・タイプには異なる頻度と保存率があります。

SLA Policy	Frequency	Retention
<input type="checkbox"/> Gold	Every 4 Hours	1 Weeks
<input type="checkbox"/> Silver	Every 1 Days at 3:47:23 AM	1 Months
<input type="checkbox"/> Bronze	Every 1 Days at 3:47:23 AM	1 Weeks
<input type="checkbox"/> Demo	Every 1 Days at 3:47:31 AM	1 Months

新規 SLA ポリシーを定義する場合は、「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。カスタムの保存

率および頻度で既存のポリシーを編集するには、編集アイコン  をクリックして、設定を定義します。「保存」をクリックして変更内容をコミットします。

5. 「保存」をクリックして、SLA ポリシーを保存します。

バックアップ・ジョブを即時に実行する場合は、「アクション」 > 「開始」をクリックします。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。

既存のファイル・システム SLA ポリシーの状況を表示するには、「保護の管理」 > 「ポリシーの概要」を選択して、以下の図に示されているように、保護の要約を表示します。



除外規則は、Windows ファイル・システム・アプリケーション全体に対して定義できます。除外されるリソースを定義する規則は、保護されている各ファイル・システムに継承されます。特定のファイル・システムに新しい規則を定義する場合、「保護の管理」>「ファイル・システム」>「**Microsoft Windows**」「**Windows バックアップ (Windows Backup)**」ウィンドウで既存の規則に追加できます。そのファイル・システムのバックアップ・ジョブに定義する新しい規則により、Windows ファイル・システムに設定されている除外規則が指定変更されます。バックアップ・ジョブの定義について詳しくは、[296 ページの『ファイル・システム・データのバックアップ』](#)を参照してください。

ファイルを除外する場合は、`Z:\%test%\excludedFile.txt` のようにファイルの名前を指定できます。フォルダー内のすべてのファイルを除外する場合は、`Z:\%test%*` のように規則を指定できます。フォルダーを除外する場合は、`DIR Z:\%excludedFolder` のように規則を指定できます。

表 56. Windows の除外規則の構文

第 11 章 ファイル・システムの保護 299

表 56. Windows の除外規則の構文 (続き)

構文	構文の動作
\	<ul style="list-style-type: none"> 次のディレクトリー・レベルを示します。 規則の末尾を円記号 ¥ 文字にすることはできません。
\...\	<ul style="list-style-type: none"> 規則が、このレベルの下にあるすべてのディレクトリーに適用されることを示します。 規則の先頭と末尾を文字列 ¥...¥ にすることはできません。 この文字列は、ドライブ指定の文字列より後でなければなりません。
*	<ul style="list-style-type: none"> この構文は、任意の文字または任意の数の文字を表すワイルドカードです。どの文字も定義されていない場合にも使用されます。 規則の先頭または末尾をこの構文にすることができます。 ドライブ名を表すために使用される場合、この構文は英字 1 文字でなければなりません。 このワイルドカードを円記号 ¥ 文字にすることはできません。
?	<ul style="list-style-type: none"> この構文は、任意の文字を 1 回のみ表すワイルドカードとして使用されます。 規則の先頭と末尾をこの構文にすることができます。 この構文がドライブ名を表すために使用される場合は、A から Z の英字 1 文字でなければなりません。
DIR	<ul style="list-style-type: none"> この構文はディレクトリー規則を示しますが、影響を受けるディレクトリー内のどのファイルも除外しません。 この構文は、見出しの規則で、その後にブランクが続く必要があります。
FS	<ul style="list-style-type: none"> ファイル・システム・ドライブ全体がジョブから除外されることを示します。 この構文の後に、1 文字またはワイルドカードのドライブ名が続く必要があります。
スペース	<ul style="list-style-type: none"> ファイル名またはディレクトリー名にスペースを入れることができます。 ブランクは、円記号 ¥ の前、規則の行の見出しまたは末尾では使用できません。 スペースは、1 文字として検証されます。
大文字と小文字のテキスト	Microsoft Windows では、大文字小文字が区別されます。除外規則では、大文字小文字は無視されます。

表 57. 有効な除外ステートメント	
規則の例	
:	この規則は、すべてのドライブのファイル・システム・ルートにあるすべてのファイルを除外しますが、ディレクトリーは除外しません。
DIR *:¥*	この規則は、すべてのドライブにあるすべてのディレクトリーを除外しますが、ルート・ディレクトリー内のファイルは除外しません。
DIR E:¥...¥*temp*	この規則は、E: ドライブのすべてのディレクトリーにある、ディレクトリー名が temp で始まるすべてのディレクトリーを除外します。
DIR F:¥Users¥Bobby¥*	このルールは、Bobby ディレクトリー内のすべての内容を除外しますが、そのディレクトリー自体は除外しません。Bobby ディレクトリー内のファイルは除外されません。
DIR F:¥Users	この規則は、Users ディレクトリーにリストされているすべてのユーザーを除外して、Users ディレクトリーも除外します。
DIR F:¥Users¥Bobby M?gee	この規則は、名前が 1 文字のワイルドカードと一致するすべてのディレクトリーを除外します。この規則は、Magee、Megee、Migee といった名前を持つユーザーを除外します。
DIR F:¥Users¥Bobby Magee	この規則は、定義されているユーザー (この例では Bobby Magee) のディレクトリーを除外します。この規則では、そのユーザーのディレクトリーと、ファイルやサブフォルダーを含むすべての内容が除外されます。
F:\...*	この規則は、F:¥ ドライブにあるすべてのファイルを除外しますが、ディレクトリーは除外しません。
F:¥Bobby.mp?	この規則は、ファイル・システム・ルート内の Bobby.mp? と一致するすべてのファイル (Bobby.MP3、Bobby.MP4 など) を除外します。
F:¥Bobby.txt	この規則は、ファイル・システム・ルートにあるファイル Bobby.txt を除外します。
F:¥Users¥...¥*.mp3	この規則は、F ドライブでリストされているすべてのユーザーの MP3 ファイルをすべて除外します。
F:¥Users¥Bobby¥...¥*.mp3	この規則は、ユーザー・ディレクトリー Bobby にあるすべての MP3 ファイルを除外します。
F:¥Users¥Bobby¥...¥*music*¥...¥*.mp?	この規則は、ユーザー Bobby のディレクトリー名に music という単語が含まれるすべてのディレクトリー内のすべての MP ファイルを除外します。除外されるファイルは、MP2、MP3、MP4 などです。
F:¥Users¥John¥* DIR F:¥Users¥John¥*	この規則の組み合わせは、ユーザー John のすべてのファイルとすべてのサブディレクトリーを除外しますが、John ディレクトリー自体は除外しません。

表 57. 有効な除外ステートメント (続き)	
規則の例	
F:¥Users¥John¥tax¥Tax_20??.pdf	この規則は、John¥tax ディレクトリーにある、パターン Tax_20 と一致するすべての文書を除外します。TAX_2000.pdf、TAX_2019.pdf などのファイルが除外されます。
FS F	この規則は、ファイル・システムの F ドライブを除外します。
FS *	この規則は、ファイル・システム内のすべてのドライブを除外します。
FS ?	この規則は、すべてのドライブを除外します。

無効な除外構文

以下の無効な構文は、除外規則定義では機能しません。

- ¥no
- *
- *
- F:¥no¥
- DIR ¥no
- DIR F:¥no¥
- DIR *
- DIR F:¥*¥

ジョブ・ログ・ファイルを表示するには、「**ジョブと操作**」に移動して、「**実行中のジョブ**」タブを開きます。最新の「**Application Server Backup**」ログ項目を見つけてください。

ファイル・システム データのリストア

ファイル・システム データを vSnap リポジトリ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。ファイル・システムのファイル・レベル・リストアのブラウザーを使用して、ジョブに追加するファイル・システム・リソースを選択し、元のインスタンスにデータをリストアするか、別のマシン上の代替インスタンスにデータをリストアするかを指定することができます。

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 ファイル・システム のバージョン・レベルが同じでなければなりません。さらに、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。


以下の追加要件が満たされていることを確認してください。

- 少なくとも 1 つのファイル・システム・バックアップ・ジョブが正常に実行されたことを確認します。バックアップ・ジョブのセットアップについての説明は、[296 ページの『ファイル・システム・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するユーザーに 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ことを確認します。役割の割り当てについて詳しくは、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)を参照してください。
- リストア・ジョブの IBM Spectrum Protect Plus 宛先ターゲットが登録され、正しくセットアップされていることを確認します。

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。スペース所要量について詳しくは、[ファイル・システム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、[ファイル・システム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」 > 「ファイル・システム」 > 「Microsoft Windows」を展開し、「ジョブの作成」  をクリックします。

2. 「リストア」を選択します。

「リストア」ウィザードが開きます。

3. 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 **ファイル・システム** をクリックし、「次へ」をクリックします。

ヒント:

- ・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・ペインで「**リストアのプレビュー (Preview Restore)**」をクリックします。
 - ・ウィザードはデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「**拡張セットアップ (Advanced Setup)**」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
4. 「ソースの選択」 ページで、ファイル・システム・サーバーをクリックして、そのサーバー上で使用可能なボリュームを表示します。ボリューム名の横にあるプラス・アイコン  をクリックして、ボリュームを選択します。「次へ」をクリックして先に進みます。
 5. 「ソース・スナップショット」 ページで、ターゲットにリストアするスナップショットを選択します。「次へ」をクリックして先に進みます。

選択されたボリュームに使用可能なスナップショットが、タイム・スタンプ、そのスナップショットに関連付けられている SLA ポリシー、およびバックアップ・コピーであるか、アーカイブ・コピーであるか、複製コピーであるかにかかわらず使用可能なソース・タイプと一緒にリストされます。

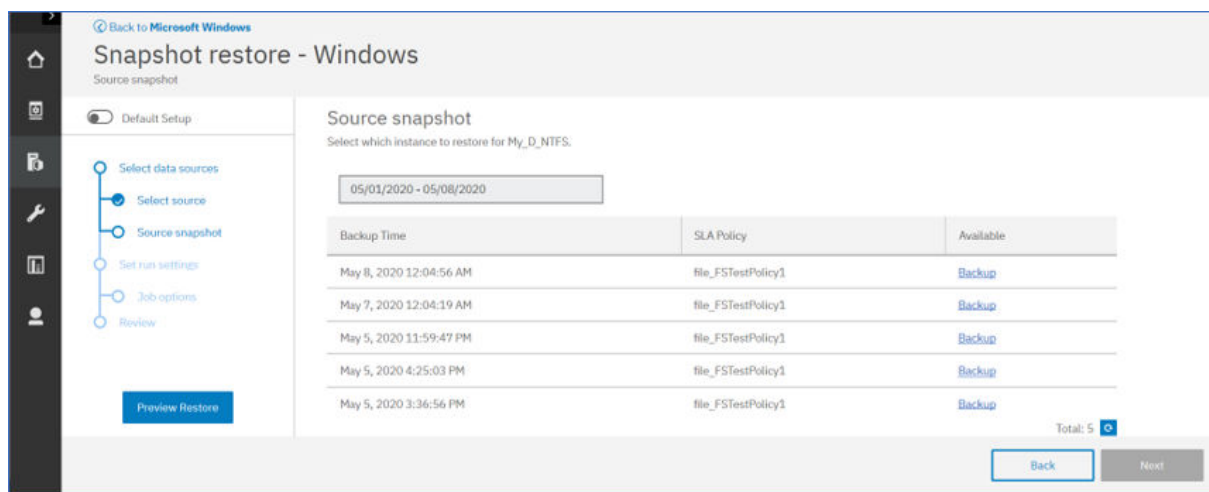


図 26. ソース・スナップショットの選択

6. 「ジョブ・オプション」 ページで実行内容を設定することができます。リストア・ジョブが失敗した場合にクリーンアップ操作が行われるかどうかを示します。「次へ」をクリックして先に進みます。
7. 「確認」 ページで、リストア・ジョブ用の選択を確認します。すべての選択が正しい場合は「実行」をクリックするか、「戻る」をクリックして選択内容を編集します。

「ジョブと操作」の「アクティブ・リソース」タブが開き、リストア・ウィザードを終了したときに準備されるアクティブ・リソースが表示されます。

注: 実行依頼されたリストア・ジョブのアクティブ・リソースは即時ではなく、表示にしばらく時間がかかります。

8. 「アクティブ・リソース」 タブの「ブラウザーを開く (Open Browser)」をクリックして、ファイル・システムのファイル・レベル・リストアのブラウザーを開きます。

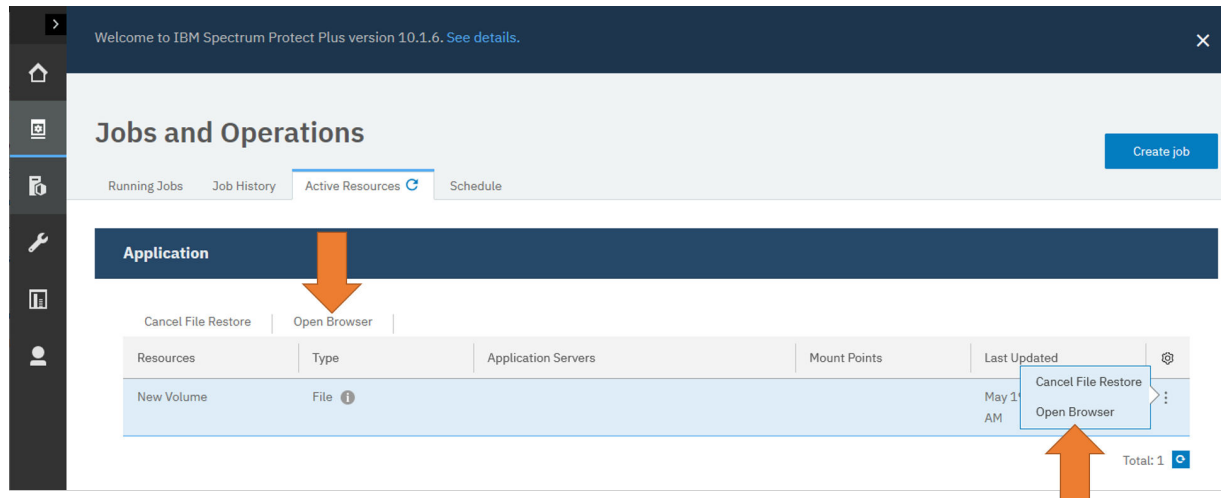


図 27. 「アクティブ・リソース」 タブからファイル・システムのファイル・レベル・リストアのブラウザーを開く

9. ファイル・システムのファイル・レベル・リストア・ブラウザーで、リストア・ジョブに追加するフ



ァイル・システム・リソースを選択します。該当する項目の横にある追加アイコンをクリックして、項目を追加します。

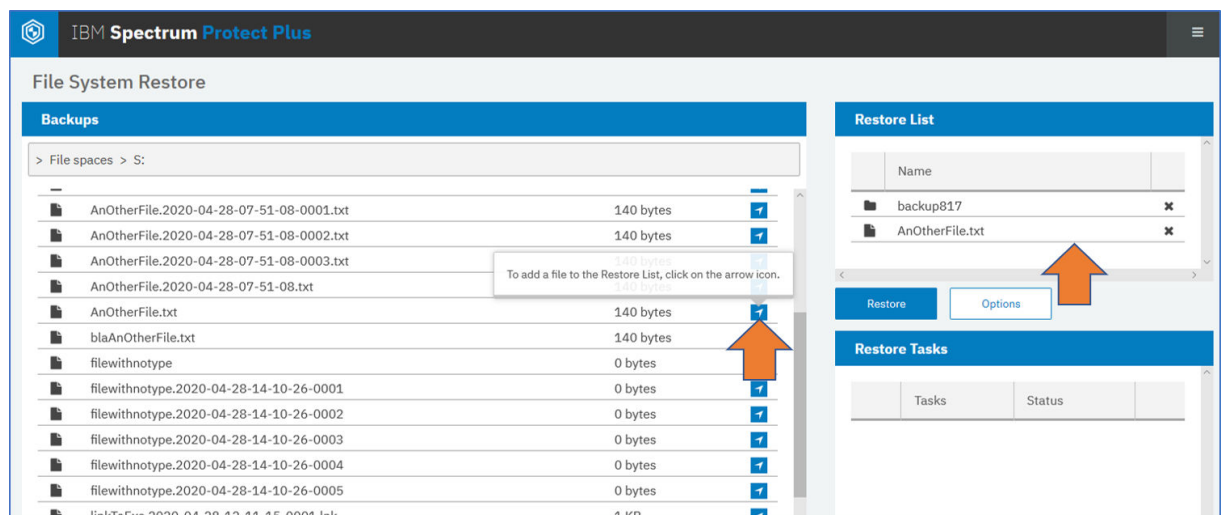


図 28. ファイル・システムのファイル・レベル・リストアのブラウザー: 「リストア・リスト」 セクションへのリソースの追加

10. リストア・ジョブの代替ロケーションを指定するには、「オプション」をクリックし、有効な Windows ローカル・ボリューム・パスをターゲットとして入力します。

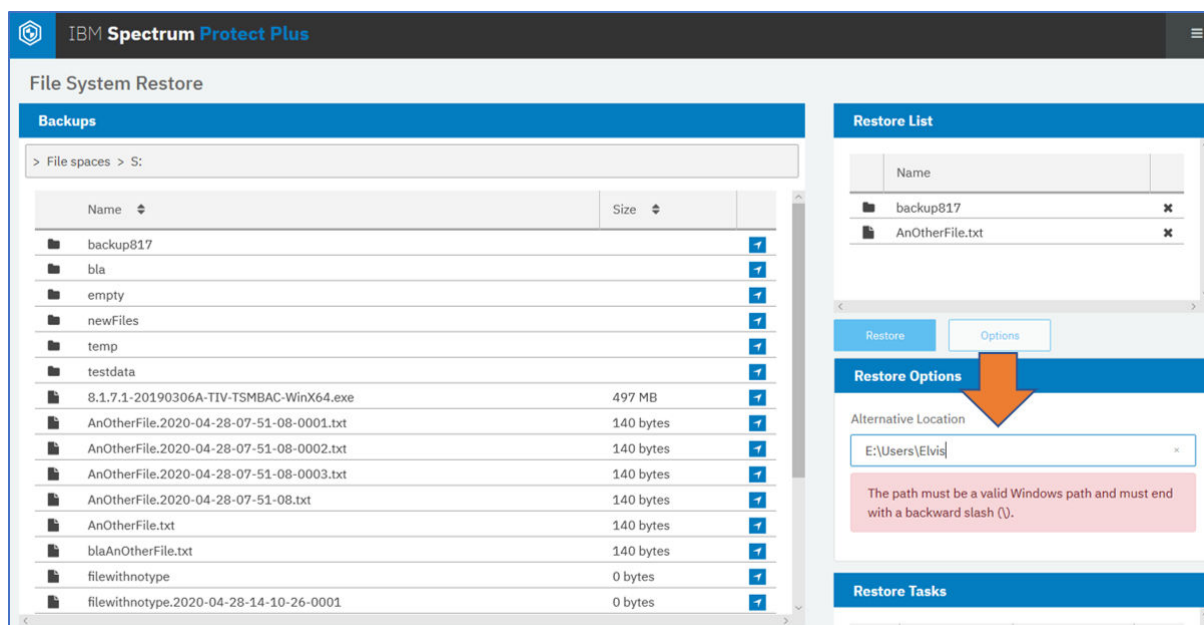


図 29. ファイル・システムのファイル・レベル・リストアのブラウザーでリストア・ジョブの代替ロケーションを指定

制約事項: ネットワーク共有は、リストア・ジョブの有効な代替ロケーションではありません。

11. 「リストア」をクリックして、リストア・プロセスを開始します。

リストア操作中に既存のファイルは上書きされません。同じ名前のファイルがターゲットで検出された場合、タイム・スタンプが新規ファイルに追加され、両方のファイルがターゲットに保管されます。

12. オプション: 「リストア・タスク (Restore Tasks)」 ペインでリストア操作の進行状況をモニターします。

ヒント: IBM Spectrum Protect Plus の「ジョブと操作」 ページでは、リストア・プロセスは追跡されません。リストア・ジョブの進行状況は、ファイル・システムのファイル・レベル・リストアのブラウザーで追跡されます。

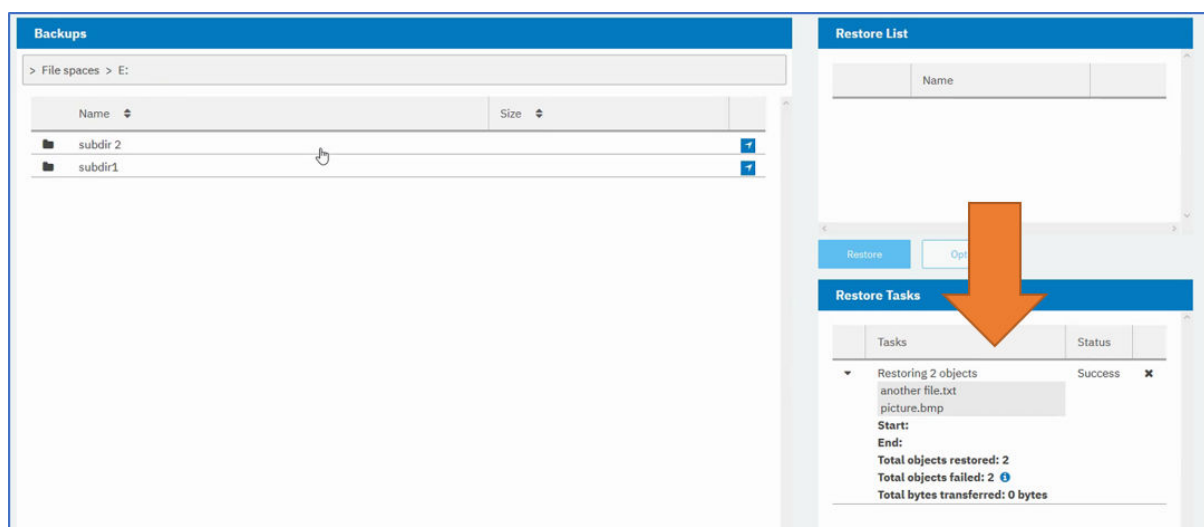


図 30. ファイル・システムのファイル・レベル・リストアのブラウザーでのリストア・ジョブのモニター

次のタスク

リストア・ジョブが完了したら、以下のアクションを実行して、アクティブ・リソースを除去します。

1. 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」をクリックします


2. 終了したアクティブ・リソースを選択し、「ファイル・システム・リストアのキャンセル (Cancel File System Restore)」をクリックします。

ファイル・システムのファイル・レベル・リストア・ブラウザー

特定のファイル・システムのリストア・ジョブを準備する際、作成されたアクティブなリソースをファイル・システムのファイル・レベル・リストア・ブラウザーで表示できるため、リストアする項目を定義することができます。このブラウザーを使用して、そのファイル・システムからリストアするディレクトリまたはファイルを見つけて指定します。その後、リストアされたリソースをソースとは別のロケーションに送信するために代替ロケーションを指定できます。

ファイル・システムのファイル・レベル・リストア・ブラウザーを開く

「リストア」ウィザードで「実行」をクリックした後、リストア・ジョブが準備され、「ジョブと操作」ページの「アクティブ・リソース」タブが開きます。ファイル・システムのファイル・レベル・リストア・

ブラウザーを開くには、「リソース」テーブルのアクション・アイコン  をクリックするか、図示されているように「ブラウザーを開く (Open Browser)」をクリックします。

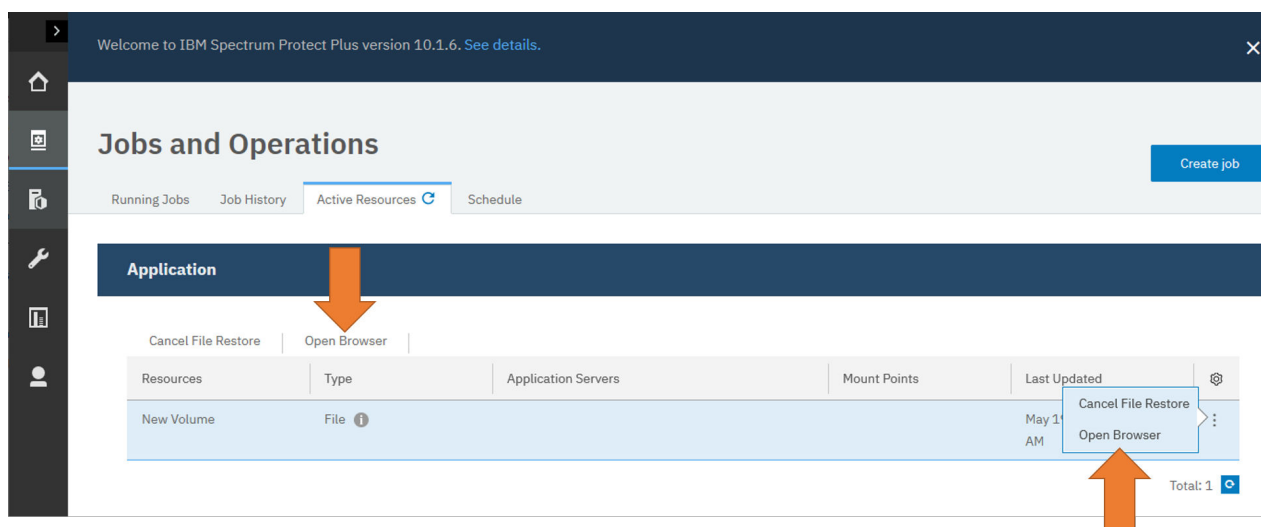


図 31. 「アクティブ・リソース」タブからファイル・システムのファイル・レベル・リストアを開く

ファイル・システムのファイル・レベル・リストア・ブラウザーを使用したリストア操作へのリソースの追加

特定のファイル・システムのリソースをリストア・ジョブに追加するには、必要なファイル・システム、ディレクトリ、またはファイルにナビゲートします。ファイル・システムの項目の横にあるアイコン



をクリックして、「リストア・リスト」セクションに項目を追加します。

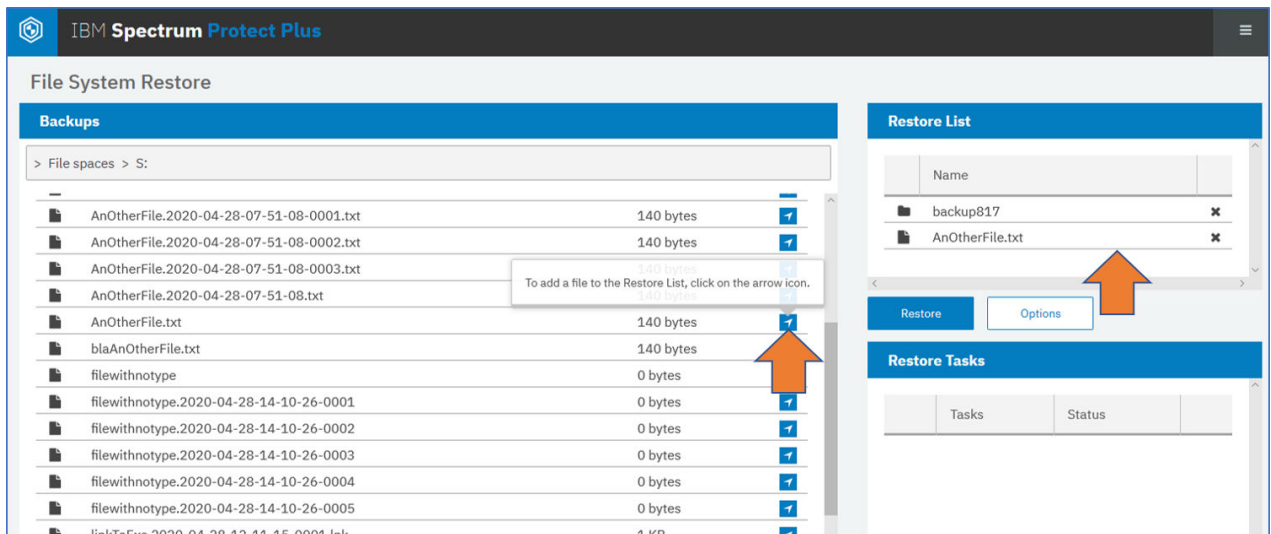


図 32. ファイル・システムのファイル・レベル・リストア・ブラウザーでのリストア・ジョブへのファイル・システム・オブジェクトの追加

代替ロケーションへのファイル・システムのリソースのリストア

リソースを複製またはコピーして、それらのリソースをソース・ロケーションとは別のロケーションにリストアするために、「オプション」ペインの「代替の場所」でターゲットとして有効な Windows パスを指定できます。

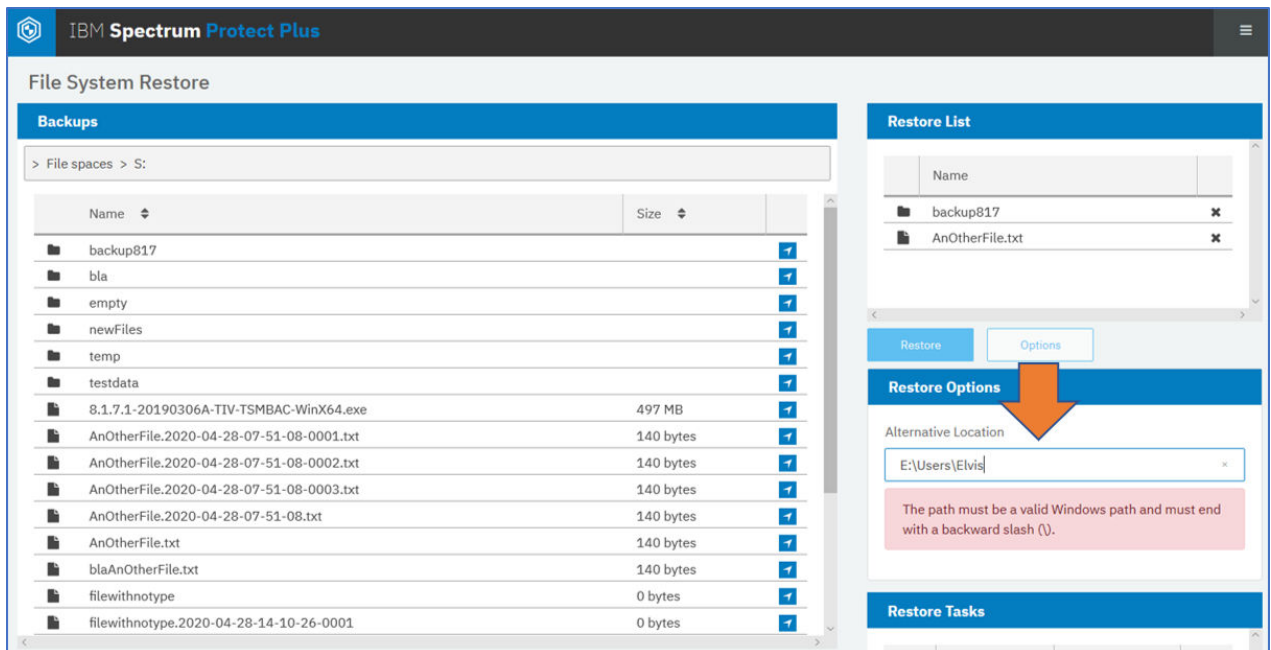


図 33. ファイル・システムのファイル・レベル・リストア・ブラウザーでのリストア・ジョブの代替の場所の指定

リストア・ジョブのモニター

ファイル・システムのファイル・レベル・リストア・ブラウザーの「リストア」をクリックすると、「リストア・タスク (Restore Tasks)」ペインでリストア・ジョブの進行状況をモニターすることができます。

図 34. ファイル・システムのファイル・レベル・リストア・ブラウザーでのリストア・ジョブのモニター

Backups

> File spaces > E:

Name	Size
subdir 2	
subdir1	

Restore List

Name

Restore Options

Restore Tasks

Tasks	Status
Restoring 2 objects another file.txt picture.bmp Start: End: Total objects restored: 2 Total objects failed: 2 Total bytes transferred: 0 bytes	Success

第 12 章 コンテナの保護

Kubernetes Backup Support は、データ保護を Kubernetes クラスター内のコンテナに拡張する IBM Spectrum Protect Plus のフィーチャーです。Kubernetes は、ホストのクラスター全体でコンテナのオーケストレーションを行うためのシステムです。

Kubernetes 環境の永続ボリュームを保護するには、最初にバックアップの頻度と保存期間を指定する SLA ポリシーを作成します。次に、バックアップ操作およびリストア操作のジョブを作成します。

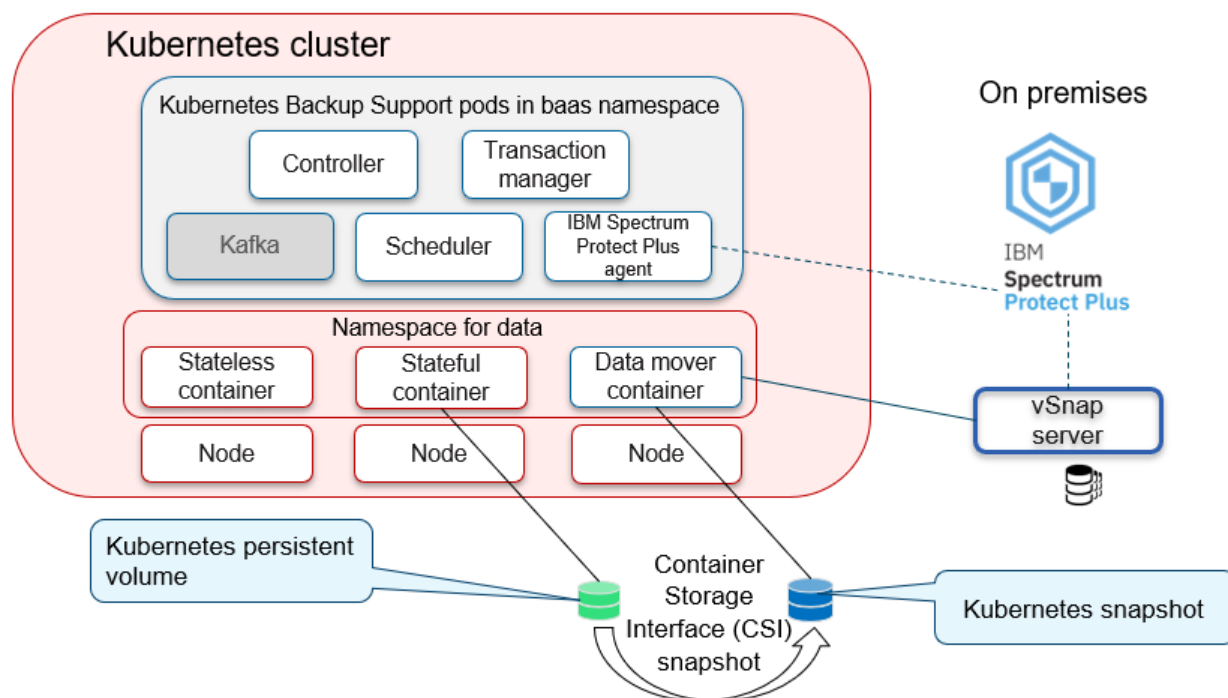
Kubernetes Backup Support の概要

IBM Spectrum Protect Plus Kubernetes Backup Support は、Kubernetes クラスター内のコンテナに接続されている永続ボリュームを保護します。永続ボリュームのスナップショット・バックアップが作成され、IBM Spectrum Protect Plus vSnap サーバーにコピーされます。

アプリケーション・データが格納されている永続ボリュームは、スナップショット・バックアップおよびコピー・バックアップが作成される頻度と保存期間を指定する、事前定義された SLA ポリシーによって保護されます。元のボリューム上のデータが損傷したか、失われた場合、vSnap サーバー上のスナップショット・バックアップまたはコピー・バックアップのいずれかからボリュームをリストアできます。

Kubernetes Backup Support は、Kubernetes 向けに提供されている Container Storage Interface (CSI) をサポートするストレージ・プラグインによって割り振られた永続ストレージのみを保護します。Kubernetes Backup Support は、CSI をサポートする Red Hat Ceph ブロック・ストレージで十分にテストされています。CSI プラグインは、バックアップ操作に使用されるスナップショット機能を提供します。

次の図に、Kubernetes Backup Support がどのように Kubernetes 環境にデプロイされ、IBM Spectrum Protect Plus と対話するかを示します。



データ・ムーバー・コンテナ

データ・ムーバーは、Persistent Volume Claims (PVC) が存在する名前空間のコンテナとしてデプロイされます。データ・ムーバー・コンテナは、コピー・バックアップ・サポートのために、Kubernetes 環境の外部にある IBM Spectrum Protect Plus インスタンスと通信します。

Kubernetes Backup Support は、PVC を使用してバックアップする永続ボリュームを識別します。コピー・バックアップ操作の場合、スケジュールが実行されると、SLA によって指定されている時間間隔で PVC のスナップショット・バックアップおよびコピー・バックアップが作成されます。データ・ムーバーは、データをコピーして、IBM Spectrum Protect Plus の「**ジョブと操作**」ウィンドウにスナップショット・バックアップを記録します。オンデマンド・バックアップによって作成されるスナップショットも IBM Spectrum Protect Plus で記録されます。

マルチテナンシーのサポート

Kubernetes Backup Support は、Kubernetes のカスタム・リソースを使用して、バックアップ操作とリストア操作を管理します。バックアップおよびリストアのオブジェクトはすべて Kubernetes 名前空間に属します。Kubernetes 管理者は、これらのオブジェクトへのアクセスを制限できます。制御されたアクセスにより、複数のユーザーが同じ Kubernetes クラスターでバックアップ要求とリストア要求を実行できます。バックアップおよびリストアのオブジェクトは、バックアップ操作とリストア操作の対象の永続ボリュームを識別する PVC から名前空間を継承します。マルチテナンシーについて詳しくは、[313 ページの『Kubernetes Backup Support のセキュリティ機能』](#)を参照してください。

バックアップおよびリストアのタイプ

Kubernetes Backup Support は、複数のタイプのバックアップ機能とリストア機能を提供します。IBM Spectrum Protect Plus ユーザー・インターフェースまたは Kubernetes コマンド・ラインを使用して、バックアップ操作とリストア操作を開始できます。

バックアップ・タイプ

以下のタイプのバックアップ操作を使用できます。

スナップショット・バックアップ

Container Storage Interface (CSI) ストレージ・プラグインのスナップショット機能を使用して、永続ボリュームのバックアップを作成します。スナップショットは、バックアップ管理者によって定義されるように Kubernetes スナップショット・クラスによって割り当てられたロケーションに保管されます。通常、このロケーションは、バックアップされている永続ボリュームと同じ保管場所です。スナップショット・クラスは、永続ボリュームのストレージ・クラスと互換性がなければなりません。つまり、スナップショット・クラスとストレージ・クラスは、同じ CSI ストレージ・プラグインによって定義され、指定されます。

スナップショット・バックアップは、スケジュール済みバックアップ要求とオンデマンド・バックアップ要求によって作成されます。

スケジュール済みバックアップ時には、SLA ポリシーによって定義されている間隔でスナップショット・バックアップが作成されます。

オンデマンド・バックアップ要求では、スナップショットは即時に作成されますが、コピー・バックアップは作成されません。最初のスナップショット・バックアップの後、指定された SLA ポリシーによってボリュームが保護されます。

コピー・バックアップ

永続ボリューム全体を IBM Spectrum Protect Plus vSnap サーバーにコピーします。事前定義された SLA ポリシーに基づき、IBM Spectrum Protect Plus は、スナップショット・バックアップと比較して長期にわたってコピー・バックアップを保存します。

スケジュール済みバックアップ時には、SLA ポリシーによって定義されている間隔でスナップショット・バックアップおよびコピー・バックアップが作成されます。

リストア・タイプ

以下のタイプのリストア操作を使用できます。

スナップショット・リストア

スナップショットを新規の永続ボリュームにリストアします。このタイプの操作は、最近のスナップショット・バックアップを迅速にリストアするのに適しています。

コピー・バックアップ・リストア

コピー・バックアップを元の永続ボリュームまたは新規の永続ボリュームにリストアします。コピー・バックアップを元の永続ボリュームにリストアする場合、その永続ボリュームが接続されているコンテナーが稼働してはなりません。

このタイプの操作は、IBM Spectrum Protect Plus で長期にわたって保存されているコピー・バックアップから永続ボリュームをリストアするのに適しています。

SLA ポリシー

SLA ポリシーは、スナップショット・バックアップとコピー・バックアップの操作が実行される頻度、およびスナップショットとコピー・バックアップが保存される期間を定義します。運用上の要件を満たすカスタムの SLA をセットアップできます。

ストレージ管理者は、IBM Spectrum Protect Plus ユーザー・インターフェースを使用して SLA ポリシーを作成することができます。手順については、[234 ページの『Kubernetes クラスター用の SLA ポリシーの作成』](#)を参照してください。

コンテナー用に作成された SLA ポリシーのリストを表示するには、以下のいずれかの方法を使用します。

- IBM Spectrum Protect Plus ユーザー・インターフェースで、「保護の管理」 > 「ポリシーの概要」をクリックします。「**SLA ポリシー**」セクションには、使用できるすべてのポリシーがリストされます。事前定義された SLA ポリシーの「**コンテナー**」は、永続ボリュームを保護するために使用できます。「**コンテナー**」ポリシーによって以下の操作が実行されます。
 - 保存期間が 1 日の 6 時間ごとのスナップショット・バックアップ
 - 保存期間が 31 日間の毎日のコピー・バックアップ
- Kubernetes 環境で、次のコマンドを実行して、baas 名前空間の ConfigMap オブジェクト baas-sla の SLA ポリシーを表示します。

```
kubect1 describe configmap baas-sla -n baas
```

このコマンドにより、コンテナーに使用できる SLA ポリシーが表示されます。コンテナー用に作成された SLA ポリシーがない場合、出力は空です。

出力は、以下の例のようになります。

```
Name:          baas-sla
Namesapce:     baas
Labels:        app=baas
                component=scheduler
                release=10.1.6
Annotations:   <none>

Data
====
SLAs:
----
daily_midnight:
Snapshots are performed every 1 days and retained for 7 days.
No copy backups are performed.
----
every_4hours:
Snapshots are performed every 4 hours and retained for 1 days.
No copy backups are performed.
----
hourly:
Snapshots are performed every 1 hours and retained for 1 days.
No copy backups are performed.
```

SLA は、バックアップ・スケジュール定義でボリュームに割り当てられます。複数の SLA を 1 つのボリュームに割り当てることができます。

スナップショットおよびコピー・バックアップは、有効期限が切れると、IBM Spectrum Protect Plus で期限切れのマークが付けられ、IBM Spectrum Protect Plus のメンテナンス・ジョブによって削除されます。

関連タスク

[317 ページの『永続ボリュームの SLA バックアップの定義』](#)

IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、SLA ポリシーに従って実行されるバックアップ・ジョブを定義することができます。SLA ポリシーは、バックアップ操作が実行される頻度、およびスナップショット・バックアップまたはコピー・バックアップが保持される期間を指定します。

329 ページの『[コマンド・ラインを使用した永続ボリュームのバックアップのスケジュール](#)』

Kubernetes コマンド・ラインを使用すると、SLA ポリシーに基づいてバックアップ要求をスケジュールすることができます。SLA ポリシーは、バックアップ操作が実行される頻度、およびスナップショット・バックアップとコピー・バックアップが保持される期間を指定します。

ユーザー役割

エンタープライズ・アプリケーション開発者とバックアップ管理者は、それぞれの役割に応じて、コンテナ内の永続データを保護するためにさまざまなユーザー・インターフェースと対話します。

アプリケーション開発者

エンタープライズ・アプリケーション開発者は、Kubernetes コマンド・ライン・ツール (**kubect1**) を使用して、以下のタスクをバックアップ管理者から独立して実行します。

- セルフサービスのバックアップ要求とリストア要求を開始します
- ボリュームを保護するためのバックアップ要求で使用する SLA ポリシーを選択します
- ボリュームをリストアします
- バックアップ要求とリストア要求の状況を表示します
- スナップショット・バックアップおよびコピー・バックアップに関する情報を照会します
- SLA ポリシーの割り当てを PVC から削除します
- 使用されていないスケジュール済みバックアップ要求およびオンデマンド・スナップショット要求を削除します

バックアップ管理者

バックアップ管理者は以下のタスクを実行します。

- Kubernetes 環境で Kubernetes Backup Support ソフトウェアをデプロイしてセットアップします
- 永続ボリューム用の Kubernetes ストレージ・クラスと、スナップショットを保管するためのスナップショット・クラスを作成します
- IBM Spectrum Protect Plus をインストールして構成します
- IBM Spectrum Protect Plus ユーザー・インターフェースで以下のタスクを実行します
 - Kubernetes クラスターを手動で登録したり、クラスターのプロパティを更新したりします
 - クラスター・リソースを検出するためにインベントリーを手動で実行します
 - SLA ポリシーを作成します
 - ボリュームを保護するための SLA バックアップ・ジョブを定義します
 - SLA ポリシーの割り当てを PVC から削除します
 - ボリュームをリストアします
 - IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、インベントリー、バックアップ、およびリストアのジョブをモニターします
 - IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、コンテナのバックアップ・ジョブの履歴を示すレポートを生成します
- Kubernetes 環境でデバッグするためのログ・ファイルの収集や、Kubernetes Backup Support のトレース・ログ・ファイルの表示など、トラブルシューティング・タスクを実行します

Kubernetes Backup Support のセキュリティ機能

Kubernetes Backup Support に統合されている基本的なセキュリティ機能に加えて、コンテナとネットワーク接続の保護、データの暗号化、インストール・パッケージの検証のための高度なセキュリティ機能が提供されています。

コンテナのセキュリティ・スキャン

Kubernetes Backup Support コンポーネントは、Red Hat Universal Based Image (UBI) から派生したコンテナを土台に構築されています。各コンテナ上の Kubernetes Backup Support ソフトウェアは、脆弱なコンポーネントやライブラリがないか静的にスキャンされています。さらに、コード注入などの実行時の脆弱性を防止できるように、コンテナは動的にスキャンされます。スキャンの後、自動テスト・スイートを使用してソフトウェアがテストされ、Kubernetes Backup Support が期待どおりに動作でき、誤った入力を正しく処理できることが検証されます。

データ・ムーバー・コンテナを除くすべてのコンテナが、さらなるセキュリティ分離を提供する専用の名前空間で稼働します。データ・ムーバーは、バックアップ操作またはリストア操作の Persistent Volume Claim (PVC) と同じ名前空間で稼働する必要があります。ボリュームのマウントが単一の名前空間のコンテナに制限されているためです。

最小特権コンテナ

Kubernetes Backup Support の各コンポーネントは、最小特権の原則で稼働します。コンテナのアクションは、それぞれ別個の名前空間のサービス・アカウントに関連付けられている役割ベースの認証制御規則によって制約されます。さらに、各コンテナのソフトウェアは、非 root ユーザーとして実行されます。データ・ムーバーは、バックアップまたはリストアされるボリュームのホスト・システム上のマウント・ポイントにアクセスするため、データ・ムーバーだけは特権コンテナとして稼働します。その他すべてのコンテナに特権はありません。

ネットワーク接続の認証

Kubernetes Backup Support コンポーネント間のネットワーク接続は、正しい操作のために必要なものに接続を制限するネットワーク・ポリシーによって制御されます。IBM Spectrum Protect Plus への接続は、IBM Spectrum Protect Plus によって提供されるセキュリティ・プロトコルに依存します。

マルチテナンシー

マルチテナンシーが Kubernetes Backup Support でサポートされており、Kubernetes クラスターによって名前空間に提供されている認証と許可に大きく依存します。許可は名前空間に関連しているため、その名前空間で BaaSReq オブジェクトを作成することを許可されているユーザーは、その名前空間に関連付けられている任意の PVC に対するバックアップまたはリストアを要求できます。BaaSReq オブジェクトは、Kubernetes Backup Support 要求で使用されるカスタムの Kubernetes リソースです。

スナップショットは、元の PVC の名前空間へのアクセスを制限するために Container Storage Interface (CSI) によって保護されます。Kubernetes Backup Support は、IBM Spectrum Protect Plus に保管されているバックアップ・コピーに名前空間を関連付けます。バックアップ・コピーは、同じ名前空間のボリュームにリストアされる必要があります。

保存データの暗号化

クラスターとストレージの管理者は、暗号化を使用して保存データを保護するためのメカニズムを有効にする責任を負います。機密データには、コピー・バックアップ・データと、インストール・プロセスで指定されたユーザー ID とパスワードで構成される Kubernetes Backup Support のシークレットが含まれます。クラスター管理者は、シークレットがクラスターの etcd データベースに保管されるときに暗号化されることを指定できます。詳しくは、[Encrypting Secret Data at Rest](#) を参照してください。

Kubernetes Backup Support は、クラスターで提供されている暗号化を超える暗号化を実装しません。ただし、ストレージ管理者は、暗号化が有効になっている IBM Spectrum Protect Plus vSnap サーバーをデプロイできます。

ストレージ管理者は、IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、暗号化されたディスクにバックアップ・データを保管する SLA を定義できます。暗号化が有効になっている SLA を指定するバックアップ要求が作成されると、vSnap サーバーで保存データの暗号化が有効になっている場合は、データは暗号化のために vSnap サーバーに送信されます。

コード署名

クラスター管理者は、Kubernetes Backup Support インストール・パッケージが IBM によって生成された後で変更されていないことを確認できます。このプロセスは、インストール・パッケージに含まれている署名ファイルを適切な署名および証明書に対して検証することで行われます。検証プロセスについては、インストールの資料で説明されています。

詳しくは、[146 ページの『Kubernetes 環境での Kubernetes Backup Support イメージのインストールとデプロイメント』](#)を参照してください。

IBM Spectrum Protect Plus ユーザー・インターフェースを使用した Kubernetes クラスターのバックアップおよびリストア

Kubernetes クラスターに接続されている永続ボリュームを保護するには、IBM Spectrum Protect Plus ユーザー・インターフェースで SLA ポリシーを作成して、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 Kubernetes 環境が [51 ページの『Kubernetes Backup Support 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。

関連概念

[309 ページの『Kubernetes Backup Support の概要』](#)

IBM Spectrum Protect Plus Kubernetes Backup Support は、Kubernetes クラスター内のコンテナに接続されている永続ボリュームを保護します。永続ボリュームのスナップショット・バックアップが作成され、IBM Spectrum Protect Plus vSnap サーバーにコピーされます。

[327 ページの『コマンド・ラインを使用したコンテナの保護』](#)

Kubernetes 環境のアプリケーション開発者は、コマンド・ライン・インターフェースを使用して、コンテナ・データのバックアップとリストアを行い、Kubernetes Backup Support 要求の状況を照会することができます。

Kubernetes クラスターの登録

必要に応じて、IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、手動で Kubernetes クラスターを登録したり、登録された Kubernetes クラスターのプロパティを変更したりすることができます。

このタスクについて

Kubernetes Backup Support がインストールされた後、Kubernetes Backup Support コンテナ用のアプリケーション・ホストは、Kubernetes のクラスター・ホストの始動時に自動的に登録されます。クラスターが IBM Spectrum Protect Plus に登録されると、クラスター内のリソースのインベントリーが自動的に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。


ただし、自動登録が失敗した場合、または登録済みクラスターの登録が誤って抹消された場合は、IBM Spectrum Protect Plus ユーザー・インターフェースを使用して手動でクラスターを登録することができます。

また、Kubernetes Backup Support コンテナ・エージェント・サービスへの接続に使用される SSH ポートの変更など、登録済みクラスターのプロパティを変更することもできます。

例えば、ロード・バランサーを使用してクラスター内のワークロードを分散する場合、ロード・バランサーを編集して、Kubernetes Backup Support エージェント・コンテナ・サービスのポート番号を使用することができます。その後、ロード・バランサーとポート番号を IBM Spectrum Protect Plus に登録すると、ポート番号を再構成する必要がありません。

手順

クラスターを手動で登録するか、クラスターのプロパティを変更するには、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」 > 「コンテナー」 > 「Kubernetes」をクリックします。
2. 「Kubernetes」 ページで「クラスターの管理 (Manage clusters)」をクリックします。
3. 次のアクションのいずれか 1 つを実行してください。
 - ・ クラスターを手動で登録するには、「クラスターの追加 (Add cluster)」をクリックします。
 - ・ 既存のクラスターのプロパティを更新するには、ホスト・アドレスのリストで、更新するクラスター・ホストの編集アイコン  をクリックします。
4. 「アプリケーション・プロパティ」 セクションのフィールドを更新します。

クラスター名

Kubernetes Backup Support コンテナのクラスター・ホストまたはロード・バランサーの名前。ホスト名または IP アドレスを入力できます。

クラスター名は、baas_config.cfg 構成ファイル内の **CLUSTER_NAME** パラメーターに使用されている値と一致しなければなりません。

ホスト・アドレス

クラスター・ホストまたはロード・バランサーのホスト・アドレス。IP アドレスまたは完全修飾ドメイン名を入力できます。

ポート番号

Kubernetes Backup Support エージェント・コンテナ・サービスへの接続のための SSH ポート。

デフォルトでは、Kubernetes Backup Support のインストール時に、ポートは自動的に Kubernetes によって割り当てられます。このポート番号を取得するには、**kubect1** コマンド・ラインで次のコマンドを発行します。

```
kubect1 get service -n baas | grep baas-spp-agent
```

出力は、以下の例のようになります。

baas-spp-agent	NodePort	10.110.235.90	<none>	22:31299/TCP	111m
----------------	----------	---------------	--------	--------------	------

ポート番号は、22: の後に続く数値ストリングです。この例では、ポート番号は 31299 です。

既存のユーザーの使用

クラスター・ホスト用に以前に入力された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**」 リストでユーザー名を選択します。

ユーザー ID

アプリケーション・ホストのユーザー名を入力します。このフィールドは、既存のユーザーを使用している場合は使用できません。

baas-secret オブジェクトからアプリケーション・ホスト・ユーザー名を取得するには、以下のコマンドを発行して、データ・ムーバーのユーザー名を取得してデコードします。

```
echo "`kubect1 get secret baas-secret -n baas -o yaml | /bin/grep datamoveruser | cut -d: -f2 | tr -d ' ' | base64 -d`"
```

「**ユーザー ID**」 フィールドに結果を入力します。例えば、W36KdGtLWXtuN6L と入力します。

アプリケーション・ホストの資格情報が、既存のユーザーのリストに追加されます。

パスワード

アプリケーション・ホストのパスワードを入力します。このフィールドは、既存のユーザーを使用している場合は使用できません。

baas-secret オブジェクトからアプリケーション・ホスト・パスワードを取得するには、以下のコマンドを発行して、データ・ムーバーのパスワードを取得してデコードします。

```
echo "`kubectl get secret baas-secret -n baas -o yaml | /bin/grep datamoverpassword |  
cut -d: -f2 | tr -d ' ' | base64 -d`"
```

「パスワード」フィールドに結果を入力します。例えば、w6EFx36vrdPzm0BC5Rth0S66f23PCznL と入力します。

5. オプション: 「オプション」セクションのフィールドにデータを設定します。

最大同時 PVC 数

同時に作成する PVC スナップショットまたはコピー・バックアップの最大数を設定します。多数の PVC を同時にバックアップすると、データのコピー時に各 PVC で複数のスレッドが使用され、帯域幅が消費されるため、クラスターのパフォーマンスに影響が及びます。クラスター・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。

デフォルト値は 10 です。

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、クラスターが IBM Spectrum Protect Plus データベースに追加され、名前空間や PVC などのクラスター・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。入力正しいのに、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。

次のタスク

クラスターが更新されたことを確認するには、ジョブ・ログを調べます。ナビゲーション・ペインで、「ジョブと操作」をクリックします。「実行中のジョブ」タブをクリックし、最近の Application Server Inventory ログ・エントリーを探します。フィルターを指定してインベントリー・ジョブのみを表示するには、フィルター・アイコンをクリックし、「インベントリー」を選択し、「適用」をクリックします。

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。ジョブを名前での検索するには、「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。インベントリー・ジョブの状況が Partial である場合は、「ジョブ・ログ」をクリックし、ログ・エントリーを確認してエラーを検出します。

クラスターのリソースを確実にバックアップできるようにするには、クラスターが検出されなければなりません。いつでも手動でインベントリーを実行して、クラスター・リソースの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、[316 ページの『Kubernetes クラスター・リソースの検出』](#)を参照してください。Kubernetes バックアップ・ジョブのスケジュールの手順については、[317 ページの『永続ボリュームの SLA バックアップの定義』](#)を参照してください。

Kubernetes クラスター・リソースの検出

Kubernetes クラスター・リソースは、クラスターが 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、クラスタ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。

このタスクについて

すべてのクラスター・リソースが検出され、バックアップできることを確認するために、インベントリー・ジョブを定期的に行います。

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」 > 「コンテナー」 > 「Kubernetes」をクリックします。
2. クラスターのリストで、クラスターを選択するか、必要なリソースにナビゲートできるクラスターのリンクをクリックします。

3. 「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、「インベントリーの実行」ボタンが「インベントリーが進行中」に変わります。任意の使用可能なクラスタ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。

クラスターのリストでクラスターを選択しないで、「インベントリーの実行」をクリックすると、インベントリー・ジョブがすべてのクラスターに対して開始されます。

次のタスク

インベントリー・ジョブをモニターするには、ナビゲーション・ペインで「**ジョブと操作**」をクリックします。「**実行中のジョブ**」タブをクリックし、最近の Application Server Inventory ログ・エントリーを探します。フィルターを指定してインベントリー・ジョブのみを表示するには、フィルター・アイコンをクリックし、「インベントリー」を選択し、「適用」をクリックします。

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。インベントリー・ジョブの状況が Partial である場合は、「**ジョブ・ログ**」をクリックし、ログ・エントリーを確認してエラーを検出します。

Kubernetes クラスターへの接続のテスト

IBM Spectrum Protect Plus に追加した Kubernetes クラスターへの接続をテストすることができます。テスト機能は、クラスターとの通信を検証し、IBM Spectrum Protect Plus サーバーとクラスターとの間のドメイン・ネーム・サーバー (DNS) 設定をテストします。

手順

クラスターへの接続をテストするには、以下の手順を実行します。

1. ナビゲーション・ペインで、「**保護の管理**」 > 「**コンテナ**」 > 「**Kubernetes**」をクリックします。
2. 「**クラスターの管理 (Manage clusters)**」をクリックします。
使用可能なクラスターのリストが表示されます。
3. リストをスクロールし、テストしたいクラスターを見つけます。
4. クラスター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、「**テスト**」を選択します。

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。

永続ボリュームの SLA バックアップの定義

IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、SLA ポリシーに従って実行されるバックアップ・ジョブを定義することができます。SLA ポリシーは、バックアップ操作が実行される頻度、およびスナップショット・バックアップまたはコピー・バックアップが保持される期間を指定します。

始める前に

次のアクションを実行してください。

- 保護したいボリュームの Persistent Volume Claim (PVC) がフォーマット設定されていることを確認します。バックアップ要求は PVC に送信されます。ロー・ブロック・ボリュームのバックアップ操作はサポートされていません。
- コンテナにデフォルトの SLA ポリシーを使用する計画がない場合は、必ず SLA ポリシーを構成してください。手順については、[234 ページの『Kubernetes クラスター用の SLA ポリシーの作成』](#)を参照してください。
- バックアップ・ジョブを実行するユーザーに、適切な役割およびリソース・グループが割り当てられていることを確認します。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。手順については、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)を参照してください。

- PVC 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。





このタスクについて

通常のスケジュールで PVC の保護を開始するには、ご使用の PVC に SLA ポリシーを適用する必要があります。SLA ポリシーは、PVC のバックアップ・ターゲット・ロケーションも定義します。

手順

1 つ以上の PVC に対して SLA バックアップ・ジョブを定義するには、以下の手順を実行します。

1. ナビゲーション・ペインで、「保護の管理」 > 「コンテナー」 > 「Kubernetes」をクリックします。
2. 「Kubernetes バックアップ (Kubernetes Backup)」ペインで、バックアップする PVC を選択します。以下のいずれかの方法を使用することができます。

方式	ステップ
クラスター内のすべての PVC をバックアップする	クラスター名のチェック・ボックスを選択します。クラスターは、クラスター・アイコン  によって識別されます。
名前空間に関連付けられている PVC をバックアップする	<ol style="list-style-type: none"> a. 「表示」 > 「名前空間」をクリックします。 b. バックアップしたい PVC が含まれているクラスターの名前をクリックします。クラスター内の名前空間のリストが表示されます。名前空間は、名前空間アイコン  によって識別されます。 c. 名前空間内のすべての PVC をバックアップするには、名前空間のチェック・ボックスを選択します。個々の PVC をバックアップするには、名前空間リンクをクリックし、バックアップする PVC ごとにチェック・ボックスを選択します。PVC は、PVC アイコン  によって識別されます。
ラベルに関連付けられている PVC をバックアップする	<ol style="list-style-type: none"> a. 「表示」 > 「ラベル」をクリックします。 b. バックアップしたい PVC が含まれているクラスターの名前をクリックします。クラスター内のラベルのリストが表示されます。ラベルはキーと値のペアとして表示され、ラベル・アイコン  によって識別されます。 c. ラベルに割り当てられているすべての PVC をバックアップするには、ラベルのチェック・ボックスを選択します。個々の PVC をバックアップするには、ラベル名をクリックし、バックアップする PVC ごとにチェック・ボックスを選択します。
検索機能を使用して、PVC のリストを SLA でフィルタリングする	<ol style="list-style-type: none"> a. 「検索対象」フィールドに検索基準を入力します。PVC 名の全部または一部を入力することができます。または、「検索対象」フィールドを空のままにして、SLA のすべての PVC を表示できます。 b. 「すべての PVC (All PVCs)」メニューから項目を選択して、検索基準に一致する結果をフィルターに掛けます。結果をフィルターに掛けて、すべての PVC、SLA に含まれない PVC、および特定の SLA に含まれる PVC を表示することができます。 c. バックアップする PVC ごとにチェック・ボックスを選択します。

3. 「SLA ポリシーの選択」をクリックし、「SLA ポリシー」表から 1 つ以上のポリシーを選択します。デフォルトの「コンテナー」ポリシーを選択するか、定義したカスタム SLA ポリシーを選択することができます。

このアクションは、選択された SLA ポリシーを選択された PVC に割り当てます。ラベルまたは名前空間レベルで SLA ポリシーを割り当てると、そのラベルまたは名前空間で作成した新規 PVC はすべて、自動的に SLA に割り当てられます。

4. 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。ジョブを即時に実行するには、「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。

オンデマンド・バックアップ・ジョブの実行: 選択した SLA ポリシーのジョブが実行されると、その SLA ポリシーに関連付けられているすべての PVC がバックアップ操作に組み込まれます。選択した PVC のみをバックアップするには、オンデマンド・ジョブを実行できます。オンデマンド・ジョブは、スナップショット・バックアップ操作を即時に実行します。

- 単一の PVC に対してオンデマンド・バックアップ・ジョブを実行するには、その PVC を選択して「実行」をクリックします。リソースが SLA ポリシーに関連付けられていない場合、「実行」ボタンは使用不可になります。
- 1 つ以上の PVC に対してオンデマンド・バックアップ・ジョブを実行するには、「ジョブの作成」をクリックし、「アドホック・バックアップ (Ad hoc backup)」を選択し、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の手順を実行します。

次のタスク

必要に応じて、SLA に追加のオプションを構成することができます。手順については、[319 ページの『Kubernetes バックアップ・ジョブの SLA オプションの指定』](#)を参照してください。

オプション: PVC の SLA バックアップの中止: PVC が SLA バックアップ・ジョブに参加する必要がなくなった場合は、以下のアクションを実行して、PVC から SLA ポリシー割り当てを除去します。

1. 「**Kubernetes バックアップ (Kubernetes Backup)**」ペインで、クラスター表を参照し、バックアップ操作を中止したい PVC を選択して、「**SLA ポリシーの選択**」をクリックします。
2. 「**SLA ポリシー**」表で、PVC に割り当てられている SLA ポリシーを識別します。割り当てられた SLA のチェック・ボックスが選択されています。
3. 除去する SLA ポリシーのチェック・ボックスをクリアします。
4. 「保存」をクリックします。この SLA ポリシーは PVC に割り当てられなくなりました。

関連概念

[310 ページの『バックアップおよびリストアのタイプ』](#)

Kubernetes Backup Support は、複数のタイプのバックアップ機能とリストア機能を提供します。IBM Spectrum Protect Plus ユーザー・インターフェースまたは Kubernetes コマンド・ラインを使用して、バックアップ操作とリストア操作を開始できます。


[311 ページの『SLA ポリシー』](#)

SLA ポリシーは、スナップショット・バックアップとコピー・バックアップの操作が実行される頻度、およびスナップショットとコピー・バックアップが保存される期間を定義します。運用上の要件を満たすカスタムの SLA をセットアップできます。

Kubernetes バックアップ・ジョブの SLA オプションの指定

バックアップ・ジョブ用の SLA を選択した後、その SLA 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. ナビゲーション・ペインで、「保護の管理」 > 「コンテナ」 > 「**Kubernetes**」をクリックします。
2. 「**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、SLA ポリシーのクリップボード・アイコン  をクリックして、以下のオプションを設定します。

事前スクリプト

ジョブの実行前にスクリプトを実行する場合は、このチェック・ボックスを選択します。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。次のアクションのいずれか 1 つを実行してください。

- 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」ページを使用して構成します。

事後スクリプト

ジョブの実行後にスクリプトを実行する場合は、このチェック・ボックスを選択します。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。次のアクションのいずれか 1 つを実行してください。

- 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」ページを使用して構成します。

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・タスクまたは事後スクリプト・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のジョブは試行されず、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

1 つ以上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 - _ * 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。

3. 「保存」をクリックします。

コンテナー・データのリストア

IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、スナップショットまたはコピー・バックアップから永続ボリュームをリストアすることができます。通常、スナップショット・リストア操作が、永続ボリュームを最も速くリストアする方法です。

始める前に

以下の制約事項を確認してください。

- スナップショットまたはコピー・バックアップを別の名前空間またはクラスターにリストアすることはできません。
- スナップショットまたはコピー・バックアップを元の永続ボリュームにリストアすることはできません。スナップショットまたはコピー・バックアップは、新しい永続ボリュームにのみリストアすることができます。新しいボリュームの Persistent Volume Claim (PVC) は、リストア操作中に自動的に作成されます。
- リストア要求が確実に正しく機能するように、Kubernetes Backup Support によって保護されているボリュームのスナップショットを手動で削除しないでください。

このタスクについて




リストア・ジョブを作成するには、「リストア」ウィザードを使用します。ウィザードの完了後に1回実行されるオンデマンド・ジョブを作成できます。

手順

スナップショットまたはコピー・バックアップから永続ボリュームをリストアするには、以下のステップを実行してリストア・ジョブを定義します。

1. ナビゲーション・ペインで、「保護の管理」 > 「コンテナ」 > 「Kubernetes」をクリックします。
2. 「ジョブの作成」をクリックして、「ジョブの作成」ページに進みます
3. 「リストア」ペインで、「選択」をクリックして「リストア」ウィザードを開きます。

ヒント:

- 「リストア」ウィザードは、「ジョブと操作」 > 「ジョブの作成」をクリックして開くこともできます。次に、「リストア」ペインで「選択」をクリックし、「Kubernetes」をクリックします。
 - 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。
 - ウィザードはデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、モードを「拡張セットアップ (Advanced Setup)」に設定します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
4. 「ソースの選択」ページで、表を参照し、リストアしたい PVC のプラス・アイコン  をクリックしてその PVC を選択します。
- 選択された PVC が「項目」リストに表示されます。リストから項目を削除する必要がある場合は、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。
- あるいは、「検索対象」フィールドに PVC 名の全部または一部を指定し、検索アイコン  をクリックして、PVC を検索することもできます。
5. 「ソース・スナップショット」ページで、以下のいずれかの方法を使用して、リストア元のソースを選択します。
- スナップショットから PVC をリストアするには、以下のようになります。

- a. 「起点 (Origin)」 > 「スナップショットから (From Snapshot)」をクリックします。
 - b. 「リストアのタイプ」 > 「オンデマンド」をクリックして、一回限りのリストア操作を実行します。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。「反復」オプションは、Kubernetes リストア操作には適用されません。
 - c. 日付範囲フィールドをクリックし、日付の範囲を指定して、その日付範囲内で使用可能なスナップショット・バックアップを表示します。
 - d. 1つの PVC をリストアする場合は、使用可能な項目のリストの中からスナップショットを選択します。複数の PVC をリストアする場合は、リストされている PVC ごとにリストア・ポイントを選択します。
 - e. 「次へ」をクリックして先に進みます。
- コピー・バックアップから PVC をリストアするには、以下のようになります。
- a. 「起点 (Origin)」 > 「コピーから (From Copy)」をクリックします。
 - b. 「リストアのタイプ」 > 「オンデマンド」をクリックして、一回限りのリストア操作を実行します。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。「反復」オプションは、Kubernetes リストア操作には適用されません。
 - c. 「リストア・ロケーションのタイプ」メニューで、データをリストアする元のロケーションのタイプを選択します。

サイト

データがバックアップされた先のサイト。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・サービス

データがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」で定義されます。

リポジトリ・サーバー

データがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」で定義されます。

クラウド・サービス・アーカイブ

データがコピーされた先のクラウド・アーカイブ・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。

リポジトリ・サーバー・アーカイブ

データがテープにコピーされたリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。

d. 「**ロケーションの選択**」メニューで、以下のいずれかのアクションを実行します。

- 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

コピー・バックアップのリストア元のデモンストレーション・サイト。

1次

コピー・バックアップのリストア元の1次サイト。

2次

コピー・バックアップのリストア元の2次サイト。

- クラウドまたはリポジトリ・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。

e. 日付範囲フィールドをクリックし、日付の範囲を指定して、その日付範囲内で使用可能なコピー・バックアップを表示します。

f. 1つのPVCをリストアする場合は、使用可能な項目のリストの中からバックアップを選択します。複数のPVCをリストアする場合は、リストされているPVCごとにリストア・ポイントを選択します。

g. 「**次へ**」をクリックして先に進みます。

6. 「**リストア方式**」ページで、リストアされたPVCの新しい名前を入力します。

新しいPVCを指定するには、PVC名に最大221文字と32文字の接頭部を入力できます。英数字、ピリオド(.)、およびハイフン(-)を含めることができます。新しいPVC名には大文字を含めることはできません。また、末尾にハイフンまたはピリオドを使用することはできません。例えば、restored-pvc1は有効なPVC名です。

PVCは、実動モードでのみ元の名前空間にリストアできます。

「**次へ**」をクリックして先に進みます。

7. 「**ジョブ・オプション**」ページで、リストア・ジョブの追加オプションを構成します。

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

PVCリカバリーが失敗した場合、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します。

セッションの上書きを許可する

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。

いずれかが失敗しても、他の選択されたPVCのリストアを続行する

1つのPVC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PVCに対するリストア・ジョブは続行されます。このオプションが有効になっていない場合、PVC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。

「次へ」をクリックして先に進みます。

8. オプション: 拡張セットアップ・モードでウィザードを実行している場合は、「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・レベルで実行す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・タスク状況または事後スクリプト・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、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。

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

オンデマンド・ジョブの場合、「実行」をクリックした後でジョブが始まり、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。「.zip のダウンロード」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。

次のタスク

PVC がリストアされているかどうかを確認するには、次の **kubectl** コマンドを発行します。

```
kubectl get pvc restored_pvc -n namespace
```

ここで、*restored_pvc* は、リストアされた PVC の名前を指定し、*namespace* は、リストアされた PVC の名前空間を指定します。

Kubernetes ジョブ・セッションの有効期限切れ

Kubernetes バックアップ・ジョブ・セッションを期限切れにして、スナップショット・バックアップまたはコピー・バックアップが作成されたときに割り当てられた保存設定をオーバーライドすることができません。ジョブ・セッションの有効期限が切れると、リストア・ポイント (スナップショット・バックアップまたはコピー・バックアップ) は、次のメンテナンス・ジョブ中に除去されます。



このタスクについて

割り当てられた SLA ポリシーの保存設定に従ってジョブ・セッションが自動的に期限切れになるのを待ちたくない場合、このタスクを実行します。

手順

Kubernetes ジョブ・セッションを期限切れにするには、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」 > 「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、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。
あるいは、「仮想マシン / データベース」タブで、「アプリケーション」を選択し、名前を入力してカタログ・エントリーを検索します。

名前を検索するには、一部のテキストを入力するか、アスタリスク (*) をワイルドカード文字として入力するか、または疑問符 (?) をパターン・マッチングに使用します。検索機能の使用法について詳しくは、[537 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: 「バックアップ・セッション」タブから検索を行う場合は、フィルターを使用して、スナップショットまたはコピー・バックアップの検索を絞り込みます。関連したバックアップ・ジョブが開始されたときの日付範囲を指定することもできます。
 - a) 「タイプ」フィールドで、「アプリケーション」を選択します。
 - b) 「サブポリシー・タイプ」フィールドで、スナップショット・バックアップを検索するには「スナップショット」を選択し、コピー・バックアップを検索するには「バックアップ」を選択します。
 - c) 必要な場合は、「バックアップ時刻範囲」フィールドをクリックし、検索する日付範囲を選択します。
4. 検索アイコン  をクリックします。
5. 検索結果で、期限切れにしたいジョブ・セッションを選択します。
6. 「バックアップ・セッション」タブが表示されている場合は、「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。
 - 単一のジョブ・セッションを期限切れにするには、「満了」をクリックします。
 - 選択したジョブの期限切れ前のすべてのジョブ・セッションを期限切れにするには、「すべてのジョブ・セッションの満了」をクリックします。
「仮想マシン / データベース」タブが表示されている場合は、期限切れにしたいリソースの「削除」アイコン  をクリックします。
7. 確認ウィンドウの手順に従い、「OK」をクリックします。

関連タスク

[476 ページの『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。

Kubernetes Backup Support のジョブのモニターおよびレポートの実行

バックアップ管理者は、IBM Spectrum Protect Plus ユーザー・インターフェースを使用して、Kubernetes Backup Support ジョブをモニターし、コンテナのバックアップ・ヒストリーを示すレポートを作成することができます。

ジョブ・ログの表示

「ジョブと操作」ウィンドウを使用して、Kubernetes Backup Support ジョブのモニター、ジョブ・ヒストリーの確認、スケジュールされたジョブの表示を行うことができます。

このタスクについて

「実行中のジョブ」タブと「ジョブ・ヒストリー」タブで、以下のようにジョブを識別できます。

- インベントリ・ジョブは、Application Server Inventory ラベルで識別されます。
- メンテナンス・ジョブは、Maintenance ラベルで識別されます。
- バックアップ・ジョブ名は、k8s_sla_name ラベルで識別されます。

ジョブ・タイプは Type フィールドに表示されます。例えば、スナップショット・バックアップ・ジョブは、タイプ Type: Backup - Snapshot で識別されます。コピー・バックアップは、タイプ Type: Backup で識別されます。

- リストア・ジョブ名は、onDemandRestore_timestamp ラベルで識別されます。ジョブ・タイプは Type: Restore です。

手順

1. IBM Spectrum Protect Plus ナビゲーション・ペインで、「**ジョブと操作**」をクリックします。
2. 該当するタブをクリックします。
 - 実行中のインベントリ・ジョブ、バックアップ・ジョブ、およびリストア・ジョブを表示するには、「**実行中のジョブ**」をクリックします。
 - 正常に実行されたジョブ、警告を出して処理が完了したジョブ、または失敗したジョブを表示するには、「**ジョブ・ヒストリー**」をクリックします。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。

ダウンロードされたファイルには、次の命名規則があります。
JobLog_job_name_timestamp.zip

- スケジュールされたジョブの状況を表示するには、「**スケジュール**」をクリックします。
- 「**保護の管理**」セクションの「**Kubernetes**」ページにアクセスせずに、アドホック・バックアップ・ジョブまたはリストア・ジョブを作成するためのショートカットを取るには、「**ジョブの作成**」をクリックします。

関連概念

[480 ページの『ジョブおよびジョブ・スケジュールの作成』](#)

ジョブおよびジョブ・スケジュールを作成する方法は、ジョブ・タイプに応じて異なります。

関連タスク

[482 ページの『ジョブの表示』](#)

実行中のジョブの状況、そして正常に完了したジョブまたは失敗や警告で完了したジョブの全体的な状況に関する情報を表示します。

永続ボリュームのバックアップ・ヒストリー・レポートの作成

レポートを実行して、保護された永続ボリュームのバックアップ・ヒストリーを表示することができます。バックアップ・ヒストリーを表示すると、バックアップ・ジョブが計画通りに実行されているかどうかを判別できます。

始める前に





特定の時刻に実行するようにレポートをスケジュールする予定の場合は、メール通知用に SMTP サーバーを構成してください。手順については、[202 ページの『SMTP 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

Persistent Volume Claim (PVC) ごとに、バックアップ・ヒストリーには、Kubernetes 環境で作成された Container Storage Interface (CSI) スナップショット、および IBM Spectrum Protect Plus vSnap サーバーにコピーされたバックアップに関する情報が表示されます。バックアップ操作の日時、バックアップのサイズ、およびコピー操作の所要時間などの情報を表示できます。このデータから、PVC に設定した SLA ポリシーに従って、スケジュールされたバックアップが実行されているかどうかを検証できます。

手順

1. IBM Spectrum Protect Plus 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. 「**名前 (役職) (Name (job title))**」列で、「**コンテナー永続ボリューム・バックアップ・ヒストリー (Container Persistent Volume Backup History)**」行を見つけ、以下のいずれかのアクションを実行します。

アクション	ステップ
レポートを即時に実行する	a. 「レポートの実行」アイコン  をクリックします。 b. 「レポートの実行」ウィンドウで、必要に応じてパラメーターを変更し、「実行」をクリックします。
デフォルト・パラメーターを指定してレポートをスケジュールする	a. 「デフォルト・パラメーターを指定してレポートをスケジュールする」アイコン  をクリックします。 b. 「デフォルト・パラメーターを指定してレポートをスケジュールする (Schedule Report with default parameters)」ウィンドウで、頻度、開始時刻、および受信者のメール・アドレスを指定します。 c. 「スケジュール」をクリックします。
カスタム・レポートを作成する	a. 「カスタム・レポートの作成」アイコン  をクリックします。「カスタム・レポートの作成 (Create Custom Report)」ウィンドウが表示されます。 b. 「パラメーター」タブで、カスタム・レポートの名前と説明を入力し、必要に応じてレポート・パラメーターを変更します。レポートの名前にスペースを含めることはできません。 c. 特定の時刻に実行するようにレポートをスケジュールするには、「スケジュール」タブをクリックし、「スケジュールの定義」を選択します。 d. 頻度、開始時刻、および受信者のメール・アドレスを指定します。 e. 「レポートの保存」をクリックします。 カスタム・レポートは、「レポート」ウィンドウの「カスタム・レポート」タブに保存されます。
カスタム・レポートを実行する	a. 「カスタム・レポート」タブをクリックします。 b. 実行するレポートを識別し、「カスタム・レポートの実行」アイコン  をクリックします。 c. 「カスタム・レポートの実行 (Run Custom Report)」ウィンドウで、「実行」をクリックします。

タスクの結果

レポートを即時に実行した場合、バックアップ・ヒストリー・レポートは「**コンテナ永続ボリューム・バックアップ・ヒストリー (Container Persistent Volume Backup History)**」ウィンドウに表示されます。レポートをダウンロードするには、「**ダウンロード**」をクリックし、レポート形式を選択します。「レポート」ウィンドウに戻るには、「**レポートに戻る (Back to Reports)**」をクリックします。

レポートのスケジュールを定義した場合、バックアップ・ヒストリー・レポートは、スケジュールされた時刻に実行され、指定した受信者に送信されます。

報告されたデータの説明は、以下の表に示されています。

表 58. バックアップ・ヒストリー・レポートの詳細	
列	説明
SLA ポリシー	PVC の保護に使用される SLA ポリシー。
保護時刻	各バックアップ・ジョブが完了した日時。
状況	各バックアップ・ジョブの状況。バックアップ・ジョブが失敗した場合は、考えられる理由が示されます。

表 58. バックアップ・履歴・レポートの詳細 (続き)	
列	説明
スナップショット・バックアップ?	バックアップ・インスタンスがスナップショット・バックアップであるかどうかを示します。インスタンスがスナップショット・バックアップであることを示すチェック・マークが列に表示されます。チェック・マークが表示される場合、「バックアップ・サイズ」列と「バックアップ速度」列にデータが表示されません。
バックアップ・サイズ	コピー・バックアップの場合、vSnap サーバーにバックアップされたデータの量。Kubernetes 環境で作成されたスナップショット・バックアップ、または失敗したバックアップの場合、サイズは表示されません。
バックアップ速度	コピー・バックアップが完了した速度。スナップショット・バックアップまたは失敗したバックアップの場合、データは表示されません。

関連概念

491 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。

コマンド・ラインを使用したコンテナの保護

Kubernetes 環境のアプリケーション開発者は、コマンド・ライン・インターフェースを使用して、コンテナ・データのバックアップとリストアを行い、Kubernetes Backup Support 要求の状況を照会することができます。

ご使用の Kubernetes 環境が [51 ページの『Kubernetes Backup Support 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。

Kubernetes Backup Support 要求

コンテナ・データを保護するために、Kubernetes コマンド・ライン・インターフェースを使用して Kubernetes Backup Support 要求を実行依頼することができます。

Kubernetes Backup Support 要求は、BaaSReq という種類の Kubernetes のカスタム・リソースです。要求は、YAML Ain't Markup Language (YAML) 構成ファイルで指定されます。その後、**kubect1** コマンド・ライン・インターフェースを使用して要求が実行依頼されます。

Kubernetes Backup Support における要求のタイプ

次の表に、使用可能なタイプの Kubernetes Backup Support 要求を示します。要求タイプは、YAML ファイルで **requesttype** キーの値として指定されます。要求の作成と実行依頼に関する説明へのリンクも示されています。

表 59. Kubernetes Backup Support 要求のタイプ		
要求タイプ	説明	説明
Backup	Persistent Volume Claim (PVC) のバックアップ操作 (スナップショットとコピーのバックアップを含む) をスケジュールします	329 ページの『コマンド・ラインを使用した永続ボリュームのバックアップのスケジュール』
BackupLabel	特定のラベルを持つすべての PVC をバックアップします	333 ページの『コマンド・ラインを使用した、ラベルによる永続ボリュームのバックアップ』
BackupNamespace	特定の名前空間にあるすべての PVC をバックアップします	336 ページの『コマンド・ラインを使用した、名前空間による永続ボリュームのバックアップ』

表 59. Kubernetes Backup Support 要求のタイプ (続き)

要求タイプ	説明	説明
OnDemandBackup	PVC の即時スナップショット・バックアップを要求します	332 ページの『コマンド・ラインを使用した、オンデマンドでの永続ボリュームのバックアップ』
Restore	スナップショット・バックアップまたはコピー・バックアップから PVC をリストアします	339 ページの『コマンド・ラインを使用したコンテナ・データのリストア』
Destroy	すべてのスナップショットおよびコピー・バックアップを削除して、スケジュールされたジョブに destroyed のマークを付けます	345 ページの『コンテナ・バックアップの削除』

要求の実行

要求を開始するには、要求タイプと必須パラメーターを指定した YAML ファイルを作成します。次に、**kubectl create** コマンドを実行して、要求を実行依頼します。

次のサンプル・ファイル (baas-req.yaml) は、YAML ファイルの一般的な形式を示しています。

```
#-----
# Filename: baas-req.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: request_name
  namespace: namespace
spec:
  requesttype: request_type
  sla: [sla_policy]
  volumesnapshotclass: snapshot_class_name
```

ここで、

request_name

要求の名前を指定します。スケジュール済みバックアップ要求の場合、要求の名前は PVC の名前と一致している必要があります。

namespace

永続ボリュームが存在する名前空間を指定します。名前空間を指定しない場合は、デフォルトの名前空間が使用されます。

request_type

要求のタイプを指定します。使用可能な要求タイプのリストについては、[327 ページの『Kubernetes Backup Support における要求のタイプ』](#)を参照してください。

[sla_policy]

要求に割り当てる 1 つ以上の SLA ポリシーを指定します。SLA ポリシーの指定については、[329 ページの『コマンド・ラインを使用した永続ボリュームのバックアップのスケジュール』](#)を参照してください。

snapshot_class_name

ボリュームのスナップショット・クラスを指定します。スナップショット・クラスを指定しないと、デフォルトのスナップショット・クラス内のサイドカー・コンテナ csi-snapshotter がボリュームのプロビジョナーと一致する場合、デフォルトのスナップショット・クラスが使用されます。そうでない場合、バックアップ要求は無効です。

baas-req.yaml サンプル・ファイルで指定されている要求を開始するには、次のコマンドを実行します。

```
kubectl create -f baas-req.yaml
```

要求の状況を確認するには、以下のいずれかの方法を使用します。

- アクセスできるすべての名前空間のすべての Kubernetes Backup Support 要求をリストするには、次のコマンドを実行します。

```
kubect1 get baasreq --all-namespaces
```

- 指定した名前空間のすべての Kubernetes Backup Support 要求の状況を表示するには、次のコマンドを実行します。

```
kubect1 describe baasreq -n namespace
```

ここで、*namespace* は、永続ボリュームの名前空間です。

- 特定の Kubernetes Backup Support 要求の状況を表示するには、次のコマンドを実行します。

```
kubect1 describe baasreq request_name -n namespace
```

ここで、*request_name* は要求の名前、*namespace* は永続ボリュームの名前空間です。

コンテナ・データのバックアップ

コンテナに接続されている永続ボリュームを保護するために、事前定義された SLA ポリシーに指定されているように実行されるバックアップ操作をスケジュールすることができます。オンデマンド・バックアップ要求を実行して、永続ボリュームのスナップショットを即時に作成することもできます。

コマンド・ラインを使用した永続ボリュームのバックアップのスケジュール

Kubernetes コマンド・ラインを使用すると、SLA ポリシーに基づいてバックアップ要求をスケジュールすることができます。SLA ポリシーは、バックアップ操作が実行される頻度、およびスナップショット・バックアップとコピー・バックアップが保持される期間を指定します。

始める前に

バックアップ要求は、保護する Persistent Volume Claim (PVC) に送信されます。バックアップ・ジョブをスケジュールする前に、以下のアクションを実行してください。

- 指定された名前空間に PVC が存在していることを確認してください。
- PVC がフォーマット設定されていることを確認してください。PVC は、バックアップされる前にフォーマット設定される必要があります。PVC を正しくフォーマット設定するには、マウントされていて書き込まれている必要があります。ロー・ブロック・ボリュームのバックアップ操作はサポートされていません。
- PVC に割り当てる SLA ポリシーを決定します。使用可能な SLA ポリシーを表示する手順については、[311 ページの『SLA ポリシー』](#)を参照してください。

このタスクについて

スケジュールされたバックアップ・ジョブが実行されると、クラスター・リソースのインベントリーが自動的に実行され、永続ボリュームのスナップショットが、SLA で定義された頻度で作成されます。SLA によってコピー・バックアップ・ポリシーが指定される場合、ボリュームのスナップショットは IBM Spectrum Protect Plus vSnap サーバーにコピーされます。

オンデマンド・バックアップ・ジョブを除き、すべてのバックアップ・ジョブがスケジュールされます。PVC のバックアップ・ジョブをスケジュールするには、ジョブ仕様を使用して YAML 構成ファイルを作成し、Kubernetes 環境のコマンド・ラインで要求を適用します。

PVC ごとに 1 つ以上の SLA ポリシーを指定できます。

手順

1. オプション: 以下のコマンドを発行して、名前空間内の PVC のリストを表示します。

```
kubect1 get pvc -n namespace
```

PVC のリストから、バックアップしたい PVC を識別します。

2. スケジュール済みバックアップの要求を定義する YAML ファイルを作成します。YAML ファイルには、次のプロパティが含まれている必要があります。

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: request_name  
  namespace: namespace  
spec:  
  requesttype: Backup  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name
```

ここで、

filename

YAML 構成ファイルの名前を示します。ファイル・タイプは .yaml です。

request_name

バックアップ要求の名前を指定します。この名前は、バックアップしたいボリュームの PVC の名前と一致しなければなりません。例えば、dbvol-01 という名前の PVC のバックアップ要求を作成するには、要求の名前が dbvol-01 でなければなりません。

namespace

PVC が存在する名前空間を指定します。

[sla_policy]

バックアップ操作のスケジュールを決定する SLA ポリシーを指定します。コンマ区切りリストを大括弧で囲むことで、複数の SLA ポリシーを指定できます。

例えば、daily ポリシーを PVC に割り当てるには、次のステートメントを指定します。

```
sla: [daily]
```

ポリシー every4hours、daily_midnight、および weekly を PVC に割り当てるには、YAML ファイルで次のステートメントを指定します。

```
sla: [every4hours,daily_midnight,weekly]
```

あるいは、次の形式を使用して、単一の SLA ポリシーを指定することができます。

```
sla:  
- daily
```

または、次の形式を使用して、複数の SLA ポリシーを指定します。

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

SLA ポリシー名を指定する際、必ず、大/小文字を正しく使用してください。YAML ファイルではポリシー名の大/小文字は区別されます。

すべての SLA の割り当てを PVC から削除するには、次のステートメントに示されるように、大括弧で囲まれた SLA ポリシー名を削除します。

```
sla: []
```

空の大括弧を指定することが、すべての SLA の割り当てを PVC から削除するための唯一の手段です。

`snapshot_class_name`

ボリュームのスナップショット・クラスを指定します。スナップショット・クラスを指定しないと、デフォルトのスナップショット・クラス内のサイドカー・コンテナ `csi-snapshotter` がボリュームのプロビジョナーと一致する場合、デフォルトのスナップショット・クラスが使用されます。そうでない場合、バックアップ要求は無効です。

3. 以下のコマンドを発行して、バックアップ要求を実行依頼します。

```
kubectl create -f filename.yaml
```

ここで、`filename` は YAML 構成ファイルの名前です。

タスクの結果

バックアップ要求を実行依頼した後、最初にスケジュールされたバックアップ操作が、SLA ポリシーで定義されている時間枠内に開始します。バックアップの開始時刻は、バックアップ状況に記録されます。

次のタスク

バックアップ操作に関する情報を表示するには、要求名または PVC 名を使用して **`kubectl describe`** コマンドを発行します。手順については、[342 ページの『バックアップ・ジョブとリストア・ジョブの状況の表示』](#)を参照してください。

YAML ファイル内のパラメーターの変更：

スケジュールされたバックアップ・ジョブが開始した後、YAML ファイル内のパラメーターを変更して、必要に応じて同じ PVC に適用することができます。例えば、次のようにします。

- 別の SLA ポリシーを PVC に割り当てるか、または SLA 割り当てを除去するには、YAML ファイルの **`sla`** フィールドの値を編集します。次に、**`kubectl`** コマンド・ライン・インターフェースを使用して YAML ファイルを適用します。
- スケジュールされたバックアップ・ジョブに PVC が参加する必要がなくなった場合は、YAML ファイル内の **`sla`** フィールドを更新して、SLA ポリシーの割り当てを除去します。すべての SLA から PVC を除去するには、**`sla`** フィールドを次のように変更します。

```
sla: []
```

次に、**`kubectl`** コマンド・ライン・インターフェースを使用して YAML ファイルを適用します。

関連概念

[310 ページの『バックアップおよびリストアのタイプ』](#)

Kubernetes Backup Support は、複数のタイプのバックアップ機能とリストア機能を提供します。IBM Spectrum Protect Plus ユーザー・インターフェースまたは Kubernetes コマンド・ラインを使用して、バックアップ操作とリストア操作を開始できます。

[311 ページの『SLA ポリシー』](#)

SLA ポリシーは、スナップショット・バックアップとコピー・バックアップの操作が実行される頻度、およびスナップショットとコピー・バックアップが保存される期間を定義します。運用上の要件を満たすカスタムの SLA をセットアップできます。

[327 ページの『Kubernetes Backup Support 要求』](#)

コンテナ・データを保護するために、Kubernetes コマンド・ライン・インターフェースを使用して Kubernetes Backup Support 要求を実行依頼することができます。

[520 ページの『Kubernetes Backup Support のトラブルシューティング』](#)

Kubernetes Backup Support の問題のトラブルシューティングを行うために、デバッグ・ログ・ファイルを収集して、トレース・ログを表示することができます。問題を診断するための手順に従うこともできます。

コマンド・ラインを使用した、オンデマンドでの永続ボリュームのバックアップ

スケジュールされたバックアップ・ジョブの実行を待つことなく即時にスナップショットを作成するには、Kubernetes コマンド・ライン・インターフェースでオンデマンド・バックアップ・ジョブを実行します。

始める前に

バックアップ要求は、保護する Persistent Volume Claim (PVC) に送信されます。バックアップ・ジョブをスケジュールする前に、以下のアクションを実行してください。

- 指定された名前空間に PVC が存在していることを確認してください。
- PVC がフォーマット設定されていることを確認してください。PVC は、バックアップされる前にフォーマット設定される必要があります。PVC を正しくフォーマット設定するには、マウントされていて書き込まれている必要があります。ロー・ブロック・ボリュームのバックアップ操作はサポートされていません。
- PVC に割り当てる SLA ポリシーを決定します。使用可能な SLA ポリシーを表示する手順については、[311 ページの『SLA ポリシー』](#)を参照してください。

このタスクについて

オンデマンド・バックアップ操作中、1つのスナップショットのみが作成されます。最初のオンデマンド・バックアップ操作が完了すると、指定された SLA ポリシーに従ってボリュームが保護されます。

スケジュールされたバックアップに対する要求とは異なり、オンデマンド要求の名前は固有でなければなりません。つまり、要求の名前は PVC の名前と同じであってはなりません。

手順

1. オプション: 以下のコマンドを発行して、名前空間内の PVC のリストを表示します。

```
kubectl get pvc -n namespace
```

PVC のリストから、バックアップしたい PVC を識別します。

2. オンデマンド・バックアップ操作の要求を定義する YAML ファイルを作成します。YAML ファイルには、次のプロパティが含まれている必要があります。

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: name_of_request  
  namespace: namespace  
spec:  
  requesttype: OnDemandBackup  
  pvcname: pvc_name  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name
```

ここで、

filename

YAML 構成ファイルの名前を示します。ファイル・タイプは .yaml です。

name_of_request

オンデマンド・バックアップ要求の名前を指定します。この名前は固有のものでなければならず、PVC の名前と一致してはなりません。

同じ PVC の後続のオンデマンド・バックアップごとに、新規のオンデマンド・バックアップ要求が作成されなければなりません。つまり、PVC の 2 番目のオンデマンド・バックアップを作成するには、新しい要求を作成し、YAML ファイルに別の要求名 (*name_of_request*) を指定します。

namespace

PVC が存在する名前空間を指定します。

pvc_name

バックアップしたいボリュームの PVC の名前を指定します。

[sla_policy]

バックアップ操作のスケジュールを決定する SLA ポリシーを指定します。例えば、daily ポリシーを PVC に割り当てるには、次のステートメントを指定します。

```
sla: [daily]
```

SLA ポリシー名を指定する際、必ず、大/小文字を正しく使用してください。YAML ファイルではポリシー名の大/小文字は区別されます。

PVC に対応するスケジュール済みバックアップ要求にない SLA は、その要求の SLA のリストに追加されます。

snapshot_class_name

ボリュームのスナップショット・クラスを指定します。スナップショット・クラスを指定しないと、デフォルトのスナップショット・クラス内のサイドカー・コンテナ `csi-snapshotter` がボリュームのプロビジョナーと一致する場合、デフォルトのスナップショット・クラスが使用されます。そうでない場合、バックアップ要求は無効です。

3. 以下のコマンドを発行して、オンデマンド・バックアップ操作を開始します。

```
kubect1 create -f filename.yaml
```

ここで、*filename* は YAML 構成ファイルの名前です。

タスクの結果

バックアップに関する情報を表示するには、要求名または PVC 名を使用して **kubect1 describe** コマンドを発行します。手順については、[342 ページの『バックアップ・ジョブとリストア・ジョブの状況の表示』](#)を参照してください。

関連概念

[310 ページの『バックアップおよびリストアのタイプ』](#)

Kubernetes Backup Support は、複数のタイプのバックアップ機能とリストア機能を提供します。IBM Spectrum Protect Plus ユーザー・インターフェースまたは Kubernetes コマンド・ラインを使用して、バックアップ操作とリストア操作を開始できます。

[327 ページの『Kubernetes Backup Support 要求』](#)

コンテナ・データを保護するために、Kubernetes コマンド・ライン・インターフェースを使用して Kubernetes Backup Support 要求を実行依頼することができます。

[520 ページの『Kubernetes Backup Support のトラブルシューティング』](#)

Kubernetes Backup Support の問題のトラブルシューティングを行うために、デバッグ・ログ・ファイルを収集して、トレース・ログを表示することができます。問題を診断するための手順に従うこともできます。

コマンド・ラインを使用した、ラベルによる永続ボリュームのバックアップ

ラベルを指定することにより、永続ボリュームのバックアップ要求を作成できます。ラベルは、ポッドや PVC などのオブジェクトに付加されているキーと値のペアです。バックアップ要求で 1 つ以上のラベルを指定することにより、それらのラベルに関連付けられているすべての PVC をバックアップすることができます。

始める前に

バックアップ要求は、保護する Persistent Volume Claim (PVC) に送信されます。バックアップ・ジョブをスケジュールする前に、以下のアクションを実行してください。

- 指定された名前空間に PVC が存在していることを確認してください。
- PVC がフォーマット設定されていることを確認してください。PVC は、バックアップされる前にフォーマット設定される必要があります。PVC を正しくフォーマット設定するには、マウントされていて書き込まれている必要があります。ロー・ブロック・ボリュームのバックアップ操作はサポートされていません。
- PVC に割り当てる SLA ポリシーを決定します。使用可能な SLA ポリシーを表示する手順については、[311 ページの『SLA ポリシー』](#)を参照してください。

手順

1. オプション: 以下のコマンドを発行して、指定された名前空間内の PVC のリストを表示します。

```
kubectl get pvc -n namespace --show-labels
```

PVC のリストから、バックアップしたい PVC に付加されているラベルを識別します。

2. ラベル別のバックアップ操作の要求を定義する YAML ファイルを作成します。YAML ファイルには、次のプロパティが含まれている必要があります。

```
#-----
# Filename: filename.yaml
#-----

apiVersion: "baas.io/v1alpha1"
kind: BaaSReq

metadata:
  name: name_of_request
  namespace: namespace
spec:
  requesttype: BackupLabel
  sla: [sla_policy]
  volumesnapshotclass: snapshot_class_name
  backuplabels:
    - label_key: value
```

ここで、

filename

YAML 構成ファイルの名前を示します。ファイル・タイプは .yaml です。

name_of_request

ラベル別のバックアップ要求の名前を指定します。この名前は固有のものでなければならず、PVC 名と一致してはなりません。

namespace

バックアップ要求の名前空間を指定します。

[sla_policy]

バックアップ操作のスケジュールを決定する SLA ポリシーを指定します。コンマ区切りリストを大括弧で囲むことで、複数の SLA ポリシーを指定できます。

例えば、daily ポリシーを PVC に割り当てるには、次のステートメントを指定します。

```
sla: [daily]
```

ポリシー every4hours、daily_midnight、および weekly を PVC に割り当てるには、YAML ファイルで次のステートメントを指定します。

```
sla: [every4hours,daily_midnight,weekly]
```

あるいは、次の形式を使用して、単一の SLA ポリシーを指定することができます。

```
sla:
- daily
```

または、次の形式を使用して、複数の SLA ポリシーを指定します。

```
sla:
- every4hours
- daily_midnight
- weekly
```

SLA ポリシー名を指定する際、必ず、大/小文字を正しく使用してください。YAML ファイルではポリシー名の大/小文字は区別されます。

ラベルからすべての SLA 割り当てを除去するには、次のステートメントに示されているように、大括弧内の SLA ポリシー名を削除します。

```
sla: []
```

snapshot_class_name

ボリュームのスナップショット・クラスを指定します。スナップショット・クラスを指定しないと、デフォルトのスナップショット・クラス内のサイドカー・コンテナ `csi-snapshotter` がボリュームのプロビジョナーと一致する場合、デフォルトのスナップショット・クラスが使用されます。そうでない場合、バックアップ要求は無効です。

label_key: value

バックアップしたい PVC に付加されているラベルの、キーと値のペアを指定します。複数のラベルを指定することができます。

ラベル・レベルで SLA ポリシーを割り当てた後、そのラベルで作成した新規 PVC はすべて、自動的にその SLA に割り当てられます。

例えば、`color: red` ラベルと `department: sales` ラベルに関連付けられているすべての PVC をバックアップするには、以下のステートメントを指定します。

```
backuplabels:
- color: red
- department: sales
```

制約事項:

- PVC ラベルはキーと値のペアです。異なる値を持つ重複キーはすべて、最後のキーと値のペアによって上書きされます。
- ラベル別のバックアップ操作は、クラスター全体で特定のラベルを持つすべての PVC に適用されます。バックアップされている PVC のいずれかが、アクセス権限がない名前空間に属している場合は、コマンド・ラインを使用してそれらの PVC をリストアすることはできません。ただし、PVC がどの名前空間に属しているかに関係なく、IBM Spectrum Protect Plus ユーザー・インターフェースを使用して PVC をリストアすることができます。詳しくは、[320 ページの『コンテナ・データのリストア』](#)を参照してください。

3. 以下のコマンドを発行して、バックアップ要求を実行依頼します。

```
kubectl create -f filename.yaml
```

ここで、`filename` は YAML 構成ファイルの名前です。

タスクの結果

バックアップ要求を実行依頼した後、最初にスケジュールされたバックアップ操作が、SLA ポリシーで定義されている時間枠内に開始します。バックアップの開始時刻は、バックアップ状況に記録されます。

次のタスク

バックアップ要求に関する情報を表示するには、要求名を使用して **kubectl describe** コマンドを発行します。例えば、`baas` 名前空間で `backup-red-label` という名前のバックアップ要求に関する情報を表示するには、次のコマンドを発行します。

```
kubectl describe baasreq backup-red-label -n baas
```


手順については、[342 ページの『バックアップ・ジョブとリストア・ジョブの状況の表示』](#)を参照してください。

YAML ファイル内のパラメーターの変更:

スケジュールされたラベル別のバックアップ・ジョブが開始した後、YAML ファイル内の SLA パラメーターを変更して、必要に応じて同じラベルに適用することができます。例えば、次のようにします。

- 別の SLA ポリシーをラベルに割り当てるか、または SLA 割り当てを除去するには、YAML ファイルの **sla** フィールドの値を編集します。次に、**kubect1** コマンド・ライン・インターフェースを使用して YAML ファイルを適用します。
- スケジュールされたバックアップ・ジョブに、ラベルに関連付けられている PVC が参加する必要がなくなった場合は、YAML ファイル内の **sla** フィールドを更新して、SLA ポリシーの割り当てを除去します。すべての SLA からラベルを除去するには、**sla** フィールドを次のように変更します。

```
sla: []
```

次に、**kubect1** コマンド・ライン・インターフェースを使用して YAML ファイルを適用します。

- 他のパラメーターを変更する必要がある場合は、新しい要求を作成し、YAML ファイルに別の要求名 (*name_of_request*) を指定する必要があります。

関連概念

[310 ページの『バックアップおよびリストアのタイプ』](#)

Kubernetes Backup Support は、複数のタイプのバックアップ機能とリストア機能を提供します。IBM Spectrum Protect Plus ユーザー・インターフェースまたは Kubernetes コマンド・ラインを使用して、バックアップ操作とリストア操作を開始できます。

[311 ページの『SLA ポリシー』](#)

SLA ポリシーは、スナップショット・バックアップとコピー・バックアップの操作が実行される頻度、およびスナップショットとコピー・バックアップが保存される期間を定義します。運用上の要件を満たすカスタムの SLA をセットアップできます。

[327 ページの『Kubernetes Backup Support 要求』](#)

コンテナ・データを保護するために、Kubernetes コマンド・ライン・インターフェースを使用して Kubernetes Backup Support 要求を実行依頼することができます。

[520 ページの『Kubernetes Backup Support のトラブルシューティング』](#)

Kubernetes Backup Support の問題のトラブルシューティングを行うために、デバッグ・ログ・ファイルを収集して、トレース・ログを表示することができます。問題を診断するための手順に従うこともできます。

コマンド・ラインを使用した、名前空間による永続ボリュームのバックアップ

名前空間を指定することにより、永続ボリュームのバックアップ要求を作成できます。物理クラスターは、名前空間と呼ばれる複数の仮想クラスターに分割できます。バックアップ要求で名前空間を指定することにより、その名前空間内のすべての PVC をバックアップすることができます。

始める前に

バックアップ要求は、保護する Persistent Volume Claim (PVC) に送信されます。バックアップ・ジョブをスケジュールする前に、以下のアクションを実行してください。

- 指定された名前空間に PVC が存在していることを確認してください。
- PVC がフォーマット設定されていることを確認してください。PVC は、バックアップされる前にフォーマット設定される必要があります。PVC を正しくフォーマット設定するには、マウントされていて書き込まれている必要があります。ロー・ブロック・ボリュームのバックアップ操作はサポートされていません。
- PVC に割り当てる SLA ポリシーを決定します。使用可能な SLA ポリシーを表示する手順については、[311 ページの『SLA ポリシー』](#)を参照してください。

手順

1. オプション: 以下のコマンドを発行して、バックアップしたい名前空間内の PVC のリストを表示します。


```
kubectl get pvc -n namespace
```

2. 名前空間別のバックアップ操作の要求を定義する YAML ファイルを作成します。YAML ファイルには、次のプロパティが含まれている必要があります。

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: name_of_request  
  namespace: namespace  
spec:  
  requesttype: BackupNamespace  
  sla: [sla_policy]  
  volumesnapshotclass: snapshot_class_name
```

ここで、

filename

YAML 構成ファイルの名前を示します。ファイル・タイプは .yaml です。

name_of_request

名前空間別のバックアップ要求の名前を指定します。この名前は固有のものでなければならず、PVC 名と一致してはなりません。

namespace

SLA ポリシーを割り当てる先の名前空間を指定します。

名前空間レベルで SLA を割り当てた後、その名前空間で作成した新規 PVC はすべて、自動的にその SLA に割り当てられます。

[sla_policy]

バックアップ操作のスケジュールを決定する SLA ポリシーを指定します。コンマ区切りリストを大括弧で囲むことで、複数の SLA ポリシーを指定できます。

例えば、daily ポリシーを PVC に割り当てるには、次のステートメントを指定します。

```
sla: [daily]
```

ポリシー every4hours、daily_midnight、および weekly を PVC に割り当てるには、YAML ファイルで次のステートメントを指定します。

```
sla: [every4hours,daily_midnight,weekly]
```

あるいは、次の形式を使用して、単一の SLA ポリシーを指定することができます。

```
sla:  
- daily
```

または、次の形式を使用して、複数の SLA ポリシーを指定します。

```
sla:  
- every4hours  
- daily_midnight  
- weekly
```

SLA ポリシー名を指定する際、必ず、大/小文字を正しく使用してください。YAML ファイルではポリシー名の大/小文字は区別されます。

名前空間からすべての SLA 割り当てを除去するには、次のステートメントに示されているように、大括弧内の SLA ポリシー名を削除します。

```
sla: []
```

snapshot_class_name

ボリュームのスナップショット・クラスを指定します。スナップショット・クラスを指定しないと、デフォルトのスナップショット・クラス内のサイドカー・コンテナ **csi-snapshotter** がボリュームのプロビジョナーと一致する場合、デフォルトのスナップショット・クラスが使用されます。そうでない場合、バックアップ要求は無効です。

3. 以下のコマンドを発行して、バックアップ要求を実行依頼します。

```
kubectl create -f filename.yaml
```

ここで、*filename* は YAML 構成ファイルの名前です。

タスクの結果

バックアップ要求を実行依頼した後、最初にスケジュールされたバックアップ操作が、SLA ポリシーで定義されている時間枠内に開始します。バックアップの開始時刻は、バックアップ状況に記録されます。

次のタスク

バックアップ要求に関する情報を表示するには、要求名を使用して **kubectl describe** コマンドを発行します。例えば、**baas** 名前空間で **backup-namespace1** という名前のバックアップ要求に関する情報を表示するには、次のコマンドを発行します。

```
kubectl describe baasreq backup-namespace1 -n baas
```

手順については、[342 ページの『バックアップ・ジョブとリストア・ジョブの状況の表示』](#)を参照してください。

YAML ファイル内のパラメーターの変更：

スケジュールされた名前空間別のバックアップ・ジョブが開始した後、YAML ファイル内の SLA パラメーターを変更して、必要に応じて同じ名前空間に適用することができます。例えば、次のようにします。

- 別の SLA ポリシーを名前空間に割り当てるか、または SLA 割り当てを除去するには、YAML ファイルの **sla** フィールドの値を編集します。次に、**kubectl** コマンド・ライン・インターフェースを使用して YAML ファイルを適用します。
- スケジュールされたバックアップ・ジョブに名前空間内の PVC が参加する必要がなくなった場合は、YAML ファイル内の **sla** フィールドを更新して、SLA ポリシーの割り当てを除去します。すべての SLA から名前空間を除去するには、**sla** フィールドを次のように変更します。

```
sla: []
```

次に、**kubectl** コマンド・ライン・インターフェースを使用して YAML ファイルを適用します。

- 他のパラメーターを変更する必要がある場合は、新しい要求を作成し、YAML ファイルに別の要求名 (*name_of_request*) を指定する必要があります。

関連概念

[310 ページの『バックアップおよびリストアのタイプ』](#)

Kubernetes Backup Support は、複数のタイプのバックアップ機能とリストア機能を提供します。IBM Spectrum Protect Plus ユーザー・インターフェースまたは Kubernetes コマンド・ラインを使用して、バックアップ操作とリストア操作を開始できます。

[311 ページの『SLA ポリシー』](#)

SLA ポリシーは、スナップショット・バックアップとコピー・バックアップの操作が実行される頻度、およびスナップショットとコピー・バックアップが保存される期間を定義します。運用上の要件を満たすカスタムの SLA をセットアップできます。

[327 ページの『Kubernetes Backup Support 要求』](#)

コンテナ・データを保護するために、Kubernetes コマンド・ライン・インターフェースを使用して Kubernetes Backup Support 要求を実行依頼することができます。

[520 ページの『Kubernetes Backup Support のトラブルシューティング』](#)

Kubernetes Backup Support の問題のトラブルシューティングを行うために、デバッグ・ログ・ファイルを収集して、トレース・ログを表示することができます。問題を診断するための手順に従うこともできます。

コマンド・ラインを使用したコンテナ・データのリストア

Kubernetes コマンド・ライン・インターフェースを使用して、スナップショット・バックアップまたはコピー・バックアップから永続ボリュームをリストアすることができます。通常、スナップショット・リストア操作は、コピー・リストア操作より高速です。

始める前に

以下の制約事項を確認してください。

- どのタイプのリストア操作の場合も、別の名前空間またはクラスターにボリュームをリストアすることはできません。
- スナップショットまたはコピー・バックアップは、新しい永続ボリュームにのみリストアすることができます。新しいボリュームの Persistent Volume Claim (PVC) は、スナップショット・バックアップまたはコピー・バックアップのリストア時に自動的に作成されます。
- リストア要求が確実に正しく機能するように、Kubernetes Backup Support によって保護されているボリュームのスナップショットを手動で削除しないでください。

このタスクについて

目標復旧時点および目標復旧時間に応じて、**fast** リストア操作または **copy** リストア操作を実行できます。

- 最短の時間でボリュームをリストアするには、高速リストア操作を実行してスナップショットをリストアします。別の操作が同じボリューム上で進行中である場合、高速リストア操作に時間がかかる場合があります。
- IBM Spectrum Protect Plus vSnap サーバーから、指定された特定時点からのボリュームをリストアするには、コピー・リストア操作を実行します。

手順

1. PVC に使用できるリストア・ポイントを表示するには、以下のコマンドを実行して、PVC のすべてのバックアップを照会します。

```
kubectl describe BaaSReq pvc_name -n namespace
```

リストア・ポイントは、スナップショット・バックアップまたはコピー・バックアップのタイム・スタンプで識別されます。

2. 表示される状況出力で、リストアしたいソース・スナップショットまたはコピー・バックアップのタイム・スタンプを識別します。タイム・スタンプは、出力の **Status** セクションでバックアップのタイプの前に表示されます。

例えば、以下の出力は、異なるタイプのバックアップのタイム・スタンプを示しています。

```
Status:
Timestamp: 2019-05-30 13:27:21
Type:      FAST
Timestamp: 2019-05-30 13:32:21
Type:      COPY
```

ここで、

FAST

スナップショット・バックアップ操作中に実行されるスナップショットのバックアップ・タイプを示します。

COPY

IBM Spectrum Protect Plus vSnap サーバー上に保管されているコピー・バックアップのバックアップ・タイプを示します。

3. リストア要求を指定するには、以下のプロパティを使用してYAML ファイルを作成します。
restorepoint パラメーターにソース・スナップショットのタイム・スタンプを挿入します。

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: name_of_restore_request  
  namespace: namespace  
spec:  
  requesttype: restore  
  pvcname: pvc_name  
  targetvolume: target_volume_for_restore  
  storageclass: storage_class_of_target_volume  
  restorepoint: timestamp_of_backup  
  restoretype: fast | copy
```

ここで、

filename

YAML 構成ファイルの名前を示します。

name_of_restore_request

リストア・ジョブに対する要求の名前を指定します。この名前は固有のものでなければならず、PVC の名前と一致してはなりません。

同じ PVC の後続のリストアごとに、新規のリストア要求を作成する必要があります。つまり、PVC をもう一度リストアするには、新しい要求を作成し、YAML ファイルに別の要求名 (**name_of_request**) を指定します。

namespace

要求の名前空間を指定します。

pvc_name

リストアしたい PVC の名前を指定します。

target_volume_for_restore

ボリュームのリストア先の PVC の名前を指定します。

高速リストアまたはコピー・リストアの場合、ボリュームは常に新しい PVC にリストアされます。この場合は、新しい PVC の名前を指定してください。

storage_class_of_target_volume

ターゲット・ボリュームに定義されているストレージ・クラスを指定します。

高速リストア操作の場合、ストレージ・クラスは無視されます。元の PVC のストレージ・クラスが使用されます。

コピー・リストア操作の場合、元の PVC と同じストレージ・クラスを指定するか、または別のストレージ・クラスを指定することができます。ストレージ・クラスを指定しない場合は、元の PVC のストレージ・クラスが使用されます。

ストレージ・クラスを指定しても、**restoretype** パラメーターを使用してリストア・タイプを指定しないと、コピー・リストア操作が実行されます。

timestamp_of_backup

リストア元のソース・スナップショットまたはコピー・バックアップのタイム・スタンプを指定します。タイム・スタンプは、協定世界時 (UTC) 形式で表示されます。

タイム・スタンプを指定しない場合は、最新のスナップショットまたはコピー・バックアップがリストアされます。

restoretype: fast | copy

使用するリストア操作のタイプを指定します。

fast

スナップショット・バックアップからボリュームをリストアします。

copy

コピー・バックアップからボリュームをリストアします。

このパラメーターはオプションです。 リストア・タイプを指定しない場合、リストアのタイプが自動的に判別されます。指定されたタイム・スタンプにスナップショットが存在する場合は、そのスナップショットをリストアするために高速リストアが実行されます。指定された時刻にコピー・バックアップのみが使用可能な場合は、そのコピー・バックアップをリストアするためにコピー・リストアが実行されます。

4. 以下のコマンドを発行して、リストア要求を開始します。

```
kubectl create -f filename.yaml
```

ここで、*filename* は YAML 構成ファイルの名前です。

次のタスク

新しい永続ボリュームにデータをリストアした場合は、スナップショット・バックアップまたはコピー・バックアップのリストア後に新規ボリュームをマウントするようにアプリケーション・コンテナを再構成します。

Kubernetes Backup Support 要求をより効率よく管理するには、次のコマンドを発行して、完了した要求を削除します。

```
kubectl delete baasreq name_of_restore_request -n namespace
```

完了した要求を削除すると、以下の利点があります。

- etcd データベースのサイズが縮小され、要求の名前を別の操作に再使用することができます。
- トラブルシューティング・プロセスが簡素化されます
- バックアップ要求とリストア要求のトラッキングが簡素化されます。以下のコマンドを発行すると、どの時点でも、クラスターで実行されている要求の正確なリストを取得できます。

```
kubectl get baasreq -n namespace
```

関連概念

[310 ページの『バックアップおよびリストアのタイプ』](#)

Kubernetes Backup Support は、複数のタイプのバックアップ機能とリストア機能を提供します。IBM Spectrum Protect Plus ユーザー・インターフェースまたは Kubernetes コマンド・ラインを使用して、バックアップ操作とリストア操作を開始できます。

[327 ページの『Kubernetes Backup Support 要求』](#)

コンテナ・データを保護するために、Kubernetes コマンド・ライン・インターフェースを使用して Kubernetes Backup Support 要求を実行依頼することができます。

[520 ページの『Kubernetes Backup Support のトラブルシューティング』](#)

Kubernetes Backup Support の問題のトラブルシューティングを行うために、デバッグ・ログ・ファイルを収集して、トレース・ログを表示することができます。問題を診断するための手順に従うこともできます。

関連タスク

[342 ページの『バックアップ・ジョブとリストア・ジョブの状況の表示』](#)

バックアップまたはリストア要求を実行依頼した後は、**kubectl get** コマンドと **kubectl describe** コマンドを使用して、要求に関する情報を表示することができます。

コンテナのバックアップ・ジョブとリストア・ジョブの管理

バックアップ・ジョブとリストア・ジョブに関する情報を照会して、不要になったスナップショット・バックアップとコピー・バックアップを削除することができます。

バックアップ・ジョブとリストア・ジョブの状況の表示

バックアップまたはリストア要求を実行依頼した後は、**kubectl get** コマンドと **kubectl describe** コマンドを使用して、要求に関する情報を表示することができます。

手順

1. 名前空間内のすべての Kubernetes Backup Support 要求のリストを表示するには、次のように **kubectl get** コマンドを発行します。

```
kubectl get baasreq -n namespace
```

例えば、production-01 名前空間内のすべての要求を表示するには、次のコマンドを発行します。

```
kubectl get baasreq -n production-01
```

出力は、以下の例のようになります。

NAME	AGE
vol08-adhoc	17d
inv-adhoc2	17d
db-vol08	18d
db-vol09	17d

要求名は、出力の NAME 列にリストされます。

2. ステップ 342 ページの『[1](#)』の結果を使用して、**kubectl describe** コマンドを発行してジョブの状況を表示します。例えば、次のようにします。
 - スケジュール済みバックアップ要求とオンデマンド・バックアップ要求からのバックアップを含めて、要求のすべてのバックアップのリストを表示するには、次のコマンドで要求の名前と名前空間を指定します。

```
kubectl describe baasreq request_name -n namespace
```

ここで、*request_name* は要求の名前です。オンデマンド・バックアップの場合は、要求名として PVC 名を使用します。

例えば、production-01 名前空間内の PVC db-vol08 のすべてのバックアップを表示するには、次のコマンドを発行します。

```
kubectl describe baasreq db-vol08 -n production-01
```

出力は、以下の例のようになります。


```
kubectl describe baasreq db-vol08 -n production-01
Name:          db-vol08
Namespace:     production-01
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  Ready
Kind:          BaaSReq
Metadata:
  Creation Timestamp: 2020-05-20T20:28:33Z
  Generation:        9
  Resource Version:   2955966
  Self Link:          /apis/baas.io/v1alpha1/namespaces/production-01/baasreqs/db-vol08
  UID:                0e8d4412-522f-44b3-932c-1e6239f7bf8e
Spec:
  Inprogress:  None
  Instanceid:  e05c400868ab9151e3c792d28edfbb18
  Origreqtype: backup
  Requesttype: backup
  Size:        1073741824
  Sla:
    joanne-copy2
  Spppvname:      cluster01:production-01:db-vol08
  Volumesnapshotclass: cirrus-csi-rbdplugin-snapclass
Status:
  Snapshotname: spp-1005-2161-172342eb32d
  Timestamp:    2020-05-20 22:24:25
  Type:        FAST
  Snapshotname: 2000.snapshot.824
  Timestamp:    2020-05-20 21:13:27
  Type:        COPY
  Snapshotname: spp-1005-2161-17233c4e7a0
  Timestamp:    2020-05-20 20:28:14
  Type:        FAST
```

- ・ リストア・ジョブに関する情報を表示するには、次のコマンドを発行します。

```
kubectl describe baasreq request_name -n namespace
```

ここで、*request_name* はリストア・ジョブの要求名であり、*namespace* はリストアされた PVC の名前空間です。

タスクの結果

コマンド出力で、**Backupstatus** フィールドはバックアップ・ジョブの状況を示します。リストア・ジョブの場合、**Restorestatus** フィールドはリストア・ジョブの状況を示します。詳しくは、[344 ページの『バックアップ・ジョブおよびリストア・ジョブの状況』](#)を参照してください。

instanceid フィールドには、IBM Spectrum Protect Plus でボリュームを一意的に識別するランダムに生成されたストリングが含まれます。

Spppvname フィールドは、IBM Spectrum Protect Plus 「**ジョブと操作**」 ウィンドウで報告された PVC の名前を示します。*namespace:pvc_name* フォーマットは、PVC の識別に使用されます。**instanceid** フィールドと **Spppvname** フィールドの値は、IBM Spectrum Protect Plus 内のバックアップを一意的に識別します。

バックアップ要求では、**Status** セクションは、完了したバックアップのリストを示します。バックアップごとに、バックアップのタイム・スタンプがリストされ、その後に実行されたバックアップのタイプがリストされます。バックアップのタイプは、以下のように定義されます。

FAST

スナップショット・バックアップ操作中に実行されるスナップショットのバックアップ・タイプを示します。

COPY

IBM Spectrum Protect Plus vSnap サーバー上に保管されているコピー・バックアップのバックアップ・タイプを示します。

バックアップ・ジョブおよびリストア・ジョブの状況

バックアップ・ジョブとリストア・ジョブの状況に関する情報を表示するために **kubectl describe** コマンドを使用すると、バックアップ・ジョブとリストア・ジョブの状況がコマンド出力に表示されます。

特定の Kubernetes Backup Support 要求の状況を表示するには、次のコマンドを入力します。

```
kubectl describe baasreq request_name -n namespace
```

ここで、*request_name* は要求の名前、*namespace* は永続ボリュームが存在している名前空間です。詳しくは、[342 ページの『バックアップ・ジョブとリストア・ジョブの状況の表示』](#)を参照してください。

報告されるバックアップ状況

バックアップ・ジョブの状況は、コマンド出力の **Backupstatus** フィールドに表示されます。次の表に、バックアップ要求の考えられる状況を示します。

表 60. バックアップ・ジョブの状況	
バックアップ状況	説明
None	このスケジュールで開始されたバックアップ・ジョブはありませんでした。
Requested	このスケジュールでバックアップ・ジョブが開始されました。
Ready	このスケジュールで少なくとも 1 つのバックアップ・ジョブが完了しました。
Destroyed	Persistent Volume Claim のすべてのスナップショット・バックアップおよびコピー・バックアップが削除されました。
Invalid	要求で問題が発生しました。考えられる説明が Errmsg フィールドにリストされます。

報告されるリストア状況

リストア・ジョブの状況は、コマンド出力の **Restorestatus** フィールドに表示されます。次の表に、リストア・ジョブの考えられる状況を示します。

表 61. リストア・ジョブの状況	
リストア状況	説明
None	リストア・ジョブは要求されませんでした。
Requested	スナップショット・バックアップまたはコピー・バックアップのリストア・ジョブが要求されました。
Restored	スナップショット・バックアップまたはコピー・バックアップは正常にリストアされました。
Invalid	要求で問題が発生しました。考えられる説明が Errmsg フィールドにリストされます。

コンテナ・バックアップの削除

destroy 要求を実行依頼することにより、Persistent Volume Claim (PVC) のスナップショットおよびコピー・バックアップに削除のマークを付けることができます。

始める前に

コンテナ・バックアップを削除するための **destroy** 要求を実行依頼する前に、以下の影響を考慮してください。

- PVC の SLA ポリシーによって定義されているとおり、PVC のすべてのスナップショットは、有効期限に達すると削除されます。
- IBM Spectrum Protect Plus vSnap サーバー上のスナップショットおよびコピー・バックアップには、削除のマークが付けられます。削除は IBM Spectrum Protect Plus によって管理されます。
- 元のバックアップ要求は、**destroy** 要求では削除されません。それを削除するには、**kubectl delete** コマンドを実行する必要があります。
- **destroy** 要求は、オンデマンド・バックアップではサポートされていません。オンデマンド・バックアップ要求を削除するには、**kubectl delete** コマンドを使用します。オンデマンド・スナップショットが削除されるのは、スナップショットの有効期限が切れるか、スケジュールされたバックアップが破棄されるときです。

手順

1. 以下のプロパティを含む、**destroy** 要求の YAML ファイルを作成します。

```
#-----  
# Filename: filename.yaml  
#-----  
  
apiVersion: "baas.io/v1alpha1"  
kind: BaaSReq  
  
metadata:  
  name: request_name  
  namespace: namespace  
spec:  
  requesttype: Destroy
```

ここで、

filename

YAML 構成ファイルの名前。

request_name

要求の名前。この名前は、バックアップされた PVC の名前と一致しなければなりません。例えば、db-vol01 という名前の PVC のすべてのスナップショットおよびコピー・バックアップを削除した場合は、要求の名前も db-vol01 でなければなりません。

namespace

PVC が存在する名前空間。

2. コマンド・ラインで次のコマンドを入力して、**destroy** 要求を実行依頼します。

```
kubectl apply -f filename.yaml
```

ここで、**filename** は YAML 構成ファイルの名前です。

3. PVC のスナップショットおよびコピー・バックアップが削除されたことを確認するには、次のコマンドを発行します。

```
kubectl describe baasreq request_name -n namespace | grep Backupstatus
```

ここで、**request_name** は、バックアップされた PVC の名前です。

コマンド出力では、以下の状況は、バックアップが削除されたことを示します。

```
Backupstatus: Destroyed
```

次のタスク

ベスト・プラクティスとして、以下のコマンドを発行して、完了した要求を削除します。

```
kubect1 delete baasreq request_name -n namespace
```

ここで、*request_name* は、バックアップされた PVC の名前です。

完了した要求を削除すると、以下の利点があります。

- etcd データベースのサイズが縮小され、要求の名前を別の操作に再使用することができます。
- トラブルシューティング・プロセスが簡素化されます
- バックアップ要求とリストア要求のトラッキングが簡素化されます。以下のコマンドを発行すると、どの時点でも、クラスターで実行されている要求の正確なリストを取得できます。

```
kubect1 get baasreq -n namespace
```

最初にバックアップを破棄せずにバックアップ要求を削除すると、バックアップ要求は実行され続け、Kubernetes Backup Support が再始動されるまで、指定された SLA ポリシーに従ってバックアップが行われます。

関連情報

[327 ページの『Kubernetes Backup Support における要求のタイプ』](#)

第 13 章 クラウド・システム上のデータの保護

Microsoft Office 365 などのクラウド・システムを IBM Spectrum Protect Plus に登録して、データの保護を開始することができます。Office 365 を IBM Spectrum Protect Plus に登録すると、バックアップ・ジョブや定期的にスケジュールされる SLA ポリシーをセットアップすることができます。

Microsoft Office 365 を IBM Spectrum Protect Plus で保護する場合、IBM Spectrum Protect Plus for Microsoft Office 365 Entity ID Monthly License (パーツ・ナンバー D25ZELL) を購入する必要があります。この資格について詳しくは、[IBM Spectrum Protect Plus V10.1.5 の発表レター](#)を参照してください。

Microsoft Office 365

Microsoft Office 365 の E メール、カレンダー、連絡先、およびデータを OneDrive クラウド・ストレージで保護するには、最初に Office 365 アプリケーションを Azure Active Directory に登録する必要があります。次に、アプリケーション・サーバーをデプロイして、IBM Spectrum Protect Plus に登録します。その後、Office 365 テナントを追加して、SLA ポリシーを定義し、バックアップ・ジョブを作成する必要があります。

IBM Spectrum Protect Plus を使用して Office 365 データを非実動環境に登録してテストすることができます。IBM Spectrum Protect Plus を使用して実動環境で Microsoft Office 365 を保護する場合、IBM Spectrum Protect Plus for Microsoft Office 365 Entity ID Monthly License (パーツ・ナンバー D25ZELL) を購入する必要があります。この資格について詳しくは、[IBM Spectrum Protect Plus V10.1.5 の発表レター](#)を参照してください。これは外部リンクであることに注意してください。

Azure Active Directory への登録

Office 365 アプリケーションを保護するには、Azure Active Directory にアプリケーションを登録し、適切な許可を付与する必要があります。新しいアプリケーションを Azure Active Directory に登録すると、アプリケーション ID やアプリケーション・シークレットなどのアプリケーション資格情報が Azure Active Directory ポータルで使用可能になります。

始める前に

次のアクションを実行してください。

- アクティブな Office 365 サブスクリプションがあることを確認します。
- Office 365 管理ユーザー ID とパスワードがあることを確認します。

手順

1. Office 365 のウェルカム・ページに進み、Office 365 管理ユーザー ID とパスワードを使用して Microsoft アカウントにサインインします。
2. Azure Active Directory 管理センターを開くには、左側のペインで省略符号をクリックして「すべて表示」メニューを展開してから、「管理センター」>「**Azure Active Directory**」をクリックします。
3. テナント・ダッシュボードを開くには、Azure Active Directory 管理センターの左側ペインで「**Azure Active Directory**」をクリックします。
4. テナントのダッシュボード・メニューで、「アプリの登録」をクリックしてから、「新規登録」をクリックします。
5. ユーザーに表示される名前を Office 365 アプリケーションに指定するには、「アプリの登録」ページの「名前」フィールドに名前を入力します。
6. その他のフィールドにはデフォルト・オプションを使用し、「登録」をクリックします。アプリの登録は、ユーザーに表示される入力済みの名前を使用してセットアップされます。
7. アプリケーション (クライアント) ID、およびディレクトリー (テナント) ID スtring を取得するには、「**Azure Active Directory**」>「テナント - アプリの登録」>「アプリ名」をクリックします。次に、アプリケーション ID スtring とディレクトリー ID をコピーします。これらの String は、後で Office 365 アプリケーションを IBM Spectrum Protect Plus に登録するときに必要になります。

8. このアプリケーション ID のクライアント・シークレットを作成するには、「証明書 & シークレット」>「新しいクライアント シークレット」をクリックします。
9. 「クライアント シークレットの追加」ペインで、「説明」フィールドに任意のユーザー名を入力し、「追加」をクリックします。クライアント・シークレットが生成され、「クライアント シークレット」ペインに値が表示されます。
10. 「クライアント シークレットの値」フィールドの横にあるコピー機能を使用して、クライアント・シークレットをクリップボードにコピーします。この文字ストリングは、IBM Spectrum Protect Plus への登録にも使用されます。
11. このアプリケーション ID の許可を追加するには、「API のアクセス許可」>「アクセス許可の追加」をクリックします。
12. 以下のアクションを実行して、以下の表に API ごとに許可を指定します。API 名 (例: Azure Active Directory Graph など) を選択します。
 - a) 許可名 User.Read.All の場合は、「委任されたアクセス許可」タイプを選択します。
 - b) 残りの許可については、表内の API の許可名ごとに「アプリケーションのアクセス許可」タイプを選択します。

API	許可名
Azure Active Directory Graph	User.Read.All
Azure Active Directory Graph	Directory.Read.All
Exchange	full_access_as_app
Microsoft Graph	Calendars.ReadWrite
Microsoft Graph	Contacts.ReadWrite
Microsoft Graph	Files.ReadWrite.All
Microsoft Graph	Mail.ReadWrite
Microsoft Graph	Sites.Read.All
Microsoft Graph	User.Read
Microsoft Graph	User.Read.all

13. 選択した許可を保存するには、「<your organization name> の管理者の同意の付与」をクリックします。

次のタスク

348 ページの『[IBM Spectrum Protect Plus への Office 365 テナントの登録](#)』の指示に従ってください。

IBM Spectrum Protect Plus への Office 365 テナントの登録

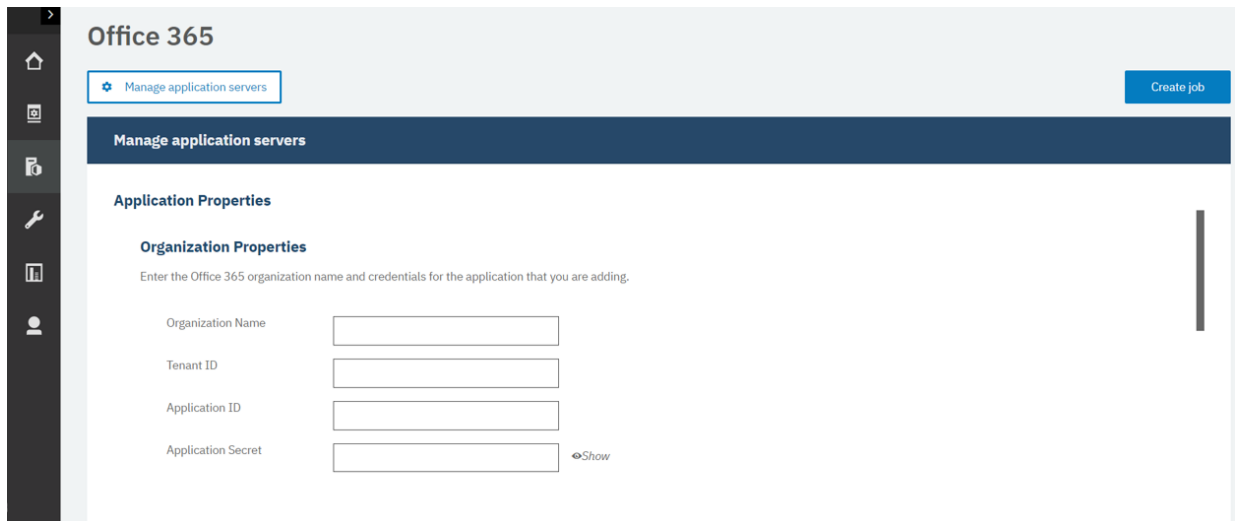
IBM Spectrum Protect Plus エージェントが Office 365 テナントに接続できることを確実にするには、Office 365 テナント資格情報とプロキシ・ホスト・サーバーを IBM Spectrum Protect Plus に登録する必要があります。この手順は、Office 365 データを IBM Spectrum Protect Plus にバックアップできるようにするために必要です。

始める前に

クラウド・プロキシ・マシンとして機能できる Linux システムがあることを確認します。IBM Spectrum Protect Plus は、バックアップ・エージェントをこのマシンにデプロイします。詳しくは、Office 365 の要件を参照してください。Office 365 アプリケーションが Azure Active Directory に登録されていることを確認します。手順については、[347 ページの『Azure Active Directory への登録』](#)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」>「クラウド管理 (Cloud Management)」>「Office 365」を展開します。



2. 「Office 365」 ページで、「アプリケーション・サーバーの管理」をクリックしてから、「アプリケーション・サーバーの追加」をクリックします。
3. 「組織のプロパティ (Organization Properties)」 ページで、以下のフィールドに入力します。
 - a. 「組織名」 フィールドに、Azure Active Directory 管理センターでセットアップした組織の名前を入力します。

注: これは、*tenantname.onmicrosoft.com* などの組織/テナント名であり、Azure アプリケーションの登録時に表示されません。
 - b. 「テナント ID」 フィールドに、Azure Active Directory アプリケーション登録の「ディレクトリー (テナント) ID」 フィールドからのストリングを入力します。
 - c. 「アプリケーション ID」 フィールドに、Azure Active Directory アプリケーション登録の「アプリケーション (クライアント) ID」 フィールドからのストリングを入力します。
 - d. 「アプリケーション秘密鍵 (Application Secret)」 フィールドに、Azure Active Directory アプリケーション登録時に生成されたパスワード・ストリングを入力します。
4. 「プロキシ・プロパティ」 ページで、以下のフィールドに入力します。
 - a. 「ホスト・アドレス」 フィールドに、プロキシ・ホストとして使用されている Linux サーバーのホスト名または IP を入力します。
 - b. ホスト・サーバー認証の場合、以下のいずれかのオプションを選択します。
 - ・ **ユーザー**: 既存のユーザーを選択するか、ユーザー ID と関連パスワードを入力します。
 - ・ **SSH 鍵**: ドロップダウン・リストからセキュア・シェル (SSH) 鍵を選択します。
5. 「保存」をクリックします。

タスクの結果

プロキシ・ホストが IBM Spectrum Protect Plus に登録されると、インベントリーが Office 365 組織で自動的に実行されます。これにより、そのリソースの Office 365 ユーザーが戻されます。

詳細なプロセス・ログ

詳細なプロセス・ログは、問題のトラブルシューティングに役立つ追加の Microsoft O365 プロセス・ログ・ファイルです。このログは、トラブルシューティングと追跡のためにすべてのバックアップ・プロセスとリストア・プロセスを追跡するために収集されます。

詳細なプロセス・ログは、保護されている Office 365 項目ごとにプロセスを追跡します。ジョブ・ログの .zip ファイルをダウンロードすると、詳細なプロセス・ログ・ファイルを標準の診断ファイルとともに表示できます。

注: このログを見つけるには、joblog.zip ファイルをダウンロードします。diag.tar.gz ファイルを解凍したら、Audit.log ファイルを見つけます。これは、O365 の処理情報が入ったファイルです。

詳細なプロセス・ログの内容と例

詳細なプロセス・ログ・ファイルには、以下の情報が入っています。

- 操作の日時
- 操作のタイプ
- 操作に関連付けられているアカウント
- イベントが OneDrive、メッセージ、イベント、または連絡先のいずれに関連しているかの標識
- 通知メッセージ:
 - OneDrive の場合、処理されたオブジェクトのパスとファイル名がリストされます。操作が、リダイレクトされたリストア操作である場合は、そのことが示されます。
 - メッセージの場合、メッセージの日時がリストされます。操作が、リダイレクトされたリストア操作である場合は、関連するメッセージがリストされます。
 - イベントの場合、イベントの件名がリストされます。
 - 連絡先の場合、連絡先の名前がリストされます。

詳細なプロセス・ログの例

詳細なプロセス・ログの情報は以下の形式で提供されます。

```
[date time] [operation] [account] [relation] [message1] optional: [message2]
```

以下に例を示します。

```
2020-02-13 19:15:27.805 Backup Completed username@example.com OneDrive
"my_new_document.pdf"
2020-02-13 19:13:46.754 Backup Completed username@example.com Message "1/20/2020 10:52:01
PM +01:00" "Welcome!"
2020-02-13 19:16:14.196 Backup Completed username@example.com Contact "John Smith"
2020-02-13 19:14:48.847 Backup Completed username@example.com Event "Monday meeting"
2020-02-13 19:18:22.544 Backup Failed username@example.com OneDrive "my_folder
\inventory.pdf"
2020-02-13 19:15:27.805 Restore Completed username@example.com OneDrive
"my_new_document.pdf" "my_new_document_2020-02-11_19_15.pdf"
2020-02-13 19:22:28.238 Backup Failed username@example.com OneDrive "my_folder\inv
\inventory.pdf"
```

Office 365 データのバックアップ

Office 365 組織が IBM Spectrum Protect Plus に登録されると、SLA ポリシーを適用して、Office 365 データの保護を開始することができます。

手順

1. IBM Spectrum Protect Plus ナビゲーション・ペインで、「保護の管理」 > 「クラウド管理 (Cloud Management)」 > 「Office 365」を展開します。
2. 組織のチェック・ボックスを選択します。
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。
SLA ポリシーについて詳しくは、[157 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。
4. 選択内容を保存します。カスタムの保存期間またはバックアップ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」をクリックします。「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。
注：「SLA ポリシーのステータス」セクションの「ポリシー・オプション」フィールドにある一部のオプションは、バックアップ・タイプに基づいて可用性が異なります。
5. 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、以下のアクションを実行します。
 - a. すべての組織データをバックアップするには、組織のチェック・ボックスを選択します。

- b. アカウントからのデータをバックアップするには、「組織」をクリックし、そのアカウントに関連付けられているユーザー名のチェック・ボックスを選択します。
 - c. アカウントの E メール、カレンダー、連絡先、または OneDrive データをバックアップするには、「組織」をクリックしてから、ユーザー名をクリックし、バックアップする E メール、カレンダー、連絡先、または OneDrive のチェック・ボックスを選択します。
6. 「実行」をクリックします。選択した SLA の状況が「実行」に代わります。ログでジョブの進行状況を確認できます。

Office 365 の永久差分バックアップ

IBM Spectrum Protect Plus では、永久差分バックアップ 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、一連の継続的な差分バックアップ・ジョブが行われます。

永久差分バックアップ・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
- すべての差分バックアップには、新規のオブジェクトまたは前回のバックアップ以降に変更されたオブジェクト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 永久差分バックアップ・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、選択された Office 365 アカウントからすべてのデータがバックアップされます。
2. 後続のすべてのバックアップ・ジョブでは、選択されたアカウントから新規データまたは変更されたデータのみがバックアップされます。

Office 365 データのリストア

vSnap サーバーまたはリモート・ストレージ上のバックアップ・コピーから Office 365 データをリストアすることができます。メールボックスを Office 365 にリストアする準備ができれば、IBM Spectrum Protect Plus でタスクを完了できます。

始める前に

少なくとも 1 つの Office 365 バックアップ・ジョブが正常に実行されている必要があります。バックアップ・ジョブのセットアップについての説明は、[350 ページの『Office 365 データのバックアップ』](#)を参照してください。



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。

- オリジナル・アカウントへのデータのリストア
- 別のアカウントへのデータのリストア
- 指定されたパスへのデータのリストア

手順

1. ナビゲーション・ペインで、「保護の管理」 > 「クラウド管理 (Cloud Management)」 > 「Office 365」を展開します。
2. 「ジョブの作成」をクリックします。
3. 「リストア」を選択します。
4. 「ソースの選択」ペインで、以下のステップを実行します。
 - a) リストア内のソースをクリックして、選択した組織についてリストアできるデータを表示します。検索機能を使用して使用可能なデータを検索し、表示されたデータを「表示」フィルターを使用して切り替えることもできます。

- b) リストアするデータを選択するために、データの横にある「リストア・リストに追加」アイコン  をクリックします。リストから複数の項目を選択することができます。選択した項目がリストア・リストに追加されます。ソース・リストから項目を削除するには、データの横にある「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。
5. 「ソース・スナップショット」ページで、リストア・タイプと、リストアするデータがバックアップされた時刻を選択します。「次へ」をクリックして先に進みます。
6. 「宛先の選択」ページで、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
宛先の選択	データのリストア先の場所を選択します。 オリジナル・アカウントにリストアする 元の Office 365 アカウントにデータをリストアします 別のアカウントにリストアする 別 Office 365 アカウントにデータをリストアします
リストア・パス	Office 365 アカウントで選択したディレクトリー・パスにデータをリストアします

7. 「ジョブ・オプション」ページで、並列ストリームでリストア操作を実行する場合は「最大並列ストリーム数」フィールドに値を指定します。「次へ」をクリックして先に進みます。
8. 「確認」ページで、リストア・ジョブの設定を確認します。
9. リストア・ジョブを開始するには、「実行」をクリックします。

タスクの結果

「実行」をクリック後しばらくして、オンデマンド・リストア・ジョブが「ジョブと操作」ページの「実行中のジョブ」タブに追加されます。ジョブ・レコードをクリックすると、操作の詳細を表示できます。「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。

リストアされたデータのアカウント名は、リストア操作のログ・ファイルで見つかります。リストア操作のログを見つけるには、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、「実行中のジョブ」タブをクリックします。

第 14 章 データベースの保護

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。

制約事項 : IBM Spectrum Protect Plus は、アプリケーションが IBM Spectrum Protect Plus に登録される際に、アプリケーション・サーバー上にフォルダーを作成することがあります。製品が適切に機能するために、IBM Spectrum Protect Plus によって作成されたフォルダーを保持する必要があります。ただし、IBM Spectrum Protect Plus によって作成され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登録抹消してください。IBM Spectrum Protect Plus が、登録に関連したフォルダーをクリーンアップします。

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ないでください。例えば、Microsoft SQL Server と Microsoft Exchange Server が同じマシンを占有し、両方が IBM Spectrum Protect Plus 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。

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、[56 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、[356 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。

IP アドレスは、IBM Spectrum Protect Plus サーバーおよび vSnap サーバーから到達可能でなければなりません。両方のサーバーで、Windows Remote Management サービスがポート 5985 で listen している必要があります。

完全修飾ドメイン名は、解決可能で、IBM Spectrum Protect Plus アプライアンス・サーバーおよび vSnap サーバーから経路指定できる必要があります。

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。

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、[356 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・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。

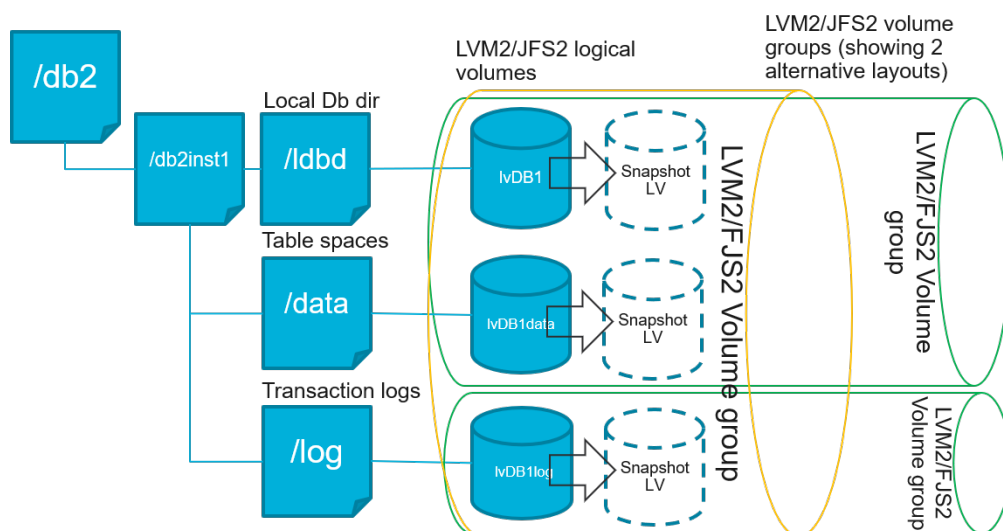


図 35. 論理ボリュームのレイアウト例

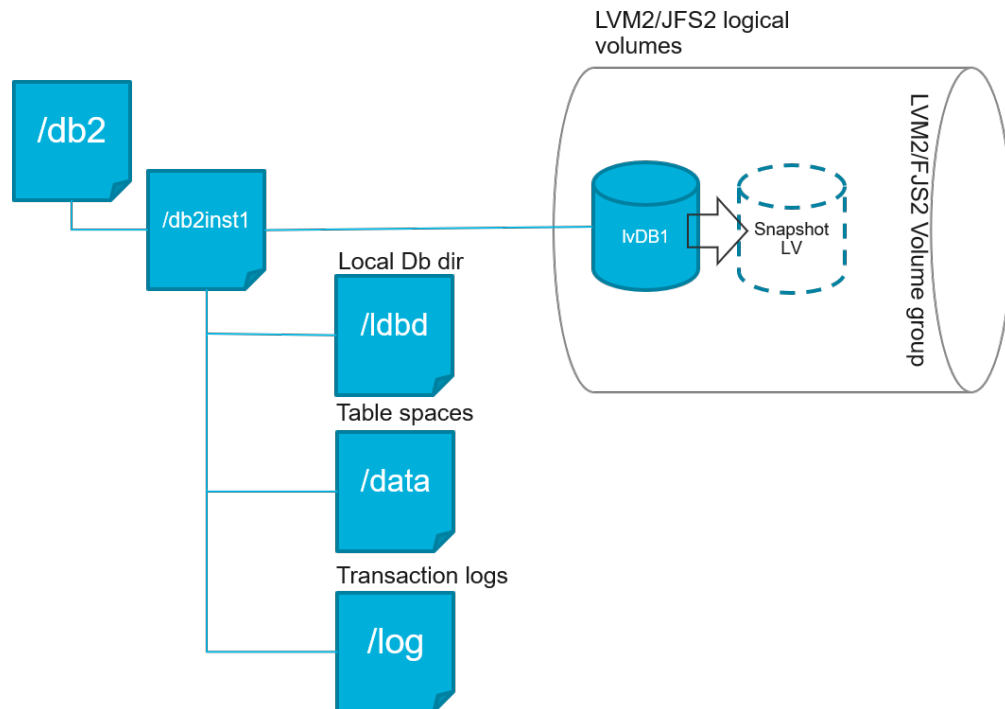


図 36. 単一論理ボリュームのレイアウト例

- 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 37. Db2 エージェントの追加

3. 「アプリケーション・プロパティ」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。

A screenshot of the Db2 web interface. The left sidebar shows navigation icons. The main area is titled "Db2" and contains a "Manage application servers" section. Below this is the "Application Properties" form. It includes fields for "Host Address" (77.00.999.12), "User" (selected with a radio button), "SSH Key" (unselected), "Use existing user" (checkbox), "User ID" (domain\user), and "Password" (Password). At the bottom are "Cancel" and "Save" buttons.

図 38. 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。

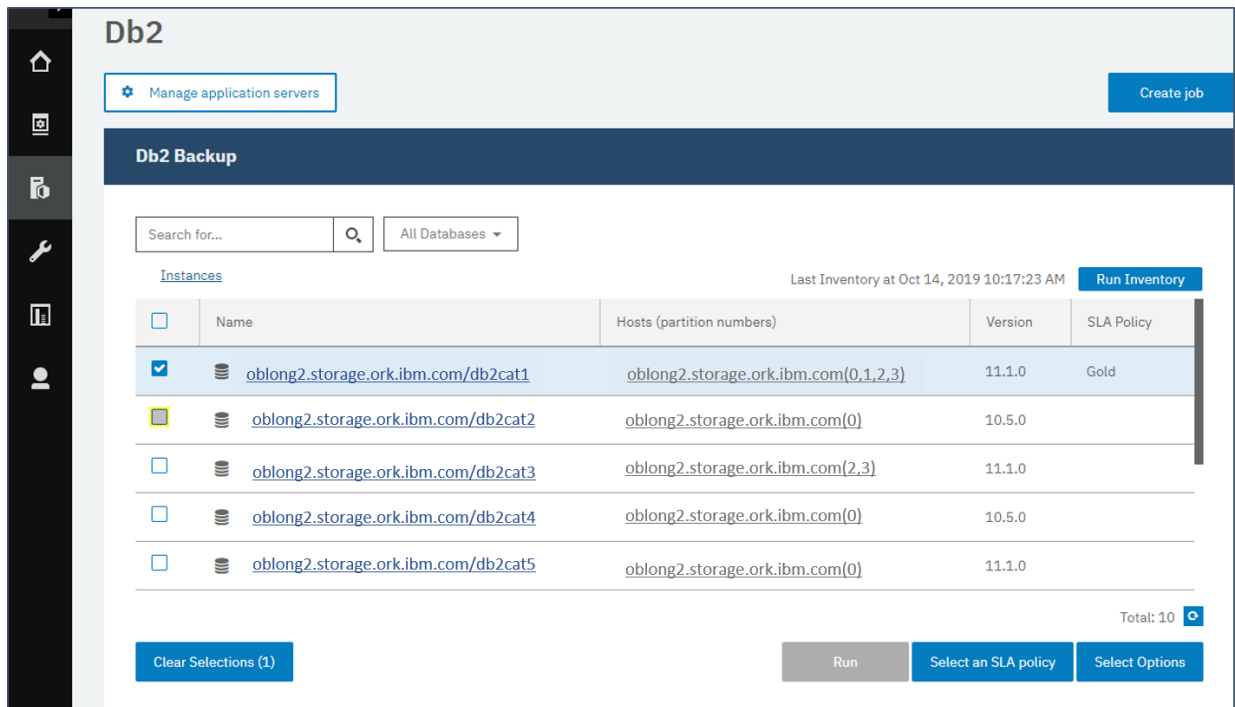


図 39. Db2 リソースの検出

インベントリの実行中、ボタンが「インベントリが進行中」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を実行できますが、インベントリ・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・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切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

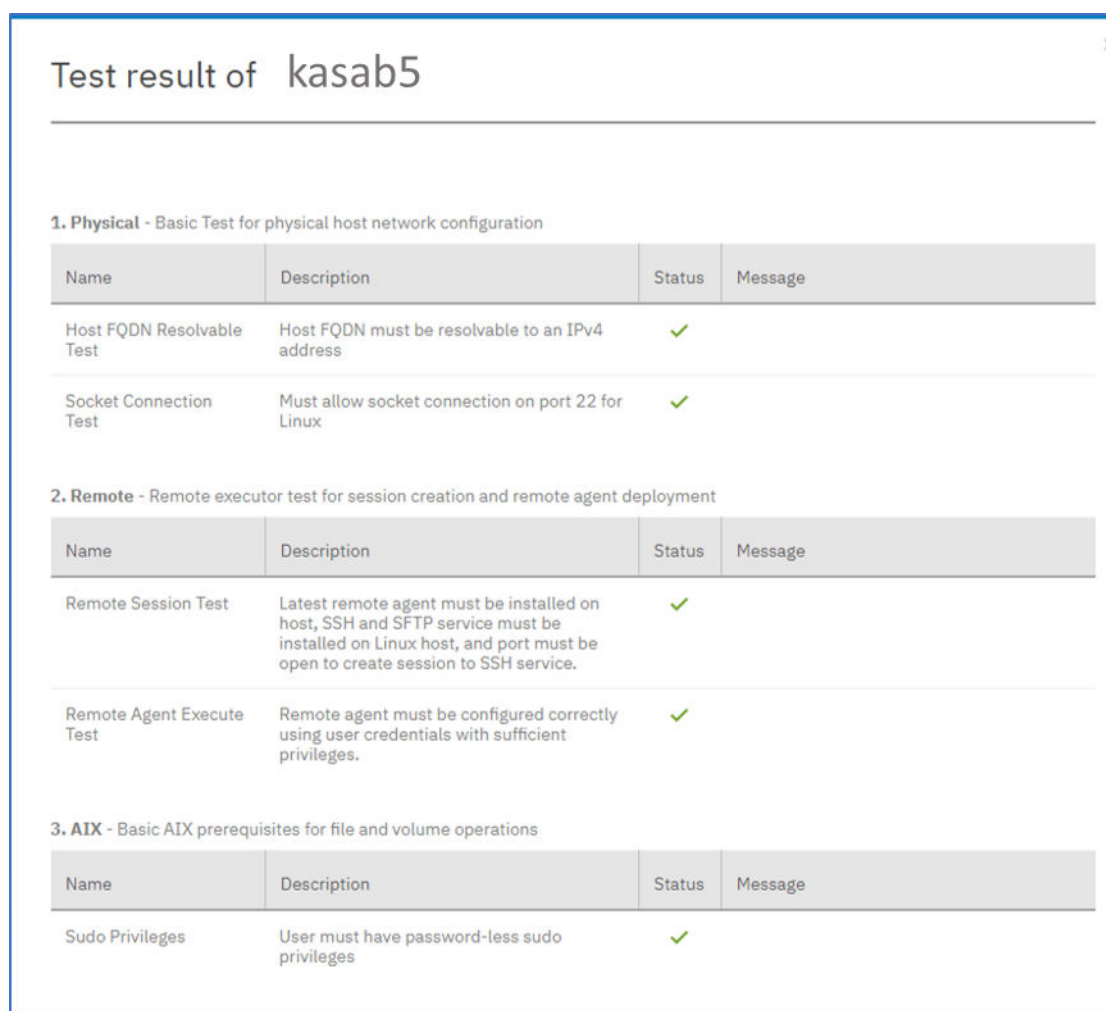
Db2 アプリケーション・サーバーを追加した後、接続をテストできます。テストでは、サーバーとの通信と、IBM Spectrum Protect Plus と Db2 サーバーの間の DNS 設定が検証されます。ユーザーの正しい sudo 権限も検査されます。

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。



The screenshot shows a window titled "Test result of kasab5". It contains three sections of test results, each with a table. All tests passed, indicated by green checkmarks.

1. Physical - Basic Test for physical host network configuration

Name	Description	Status	Message
Host FQDN Resolvable Test	Host FQDN must be resolvable to an IPv4 address	✓	
Socket Connection Test	Must allow socket connection on port 22 for Linux	✓	

2. Remote - Remote executor test for session creation and remote agent deployment

Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient privileges.	✓	

3. AIX - Basic AIX prerequisites for file and volume operations

Name	Description	Status	Message
Sudo Privileges	User must have password-less sudo privileges	✓	

図 40. 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。差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、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)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。

このタスクについて

以下のステップでは、SLA ポリシーに割り当てられているリソースをバックアップする方法を説明しています。リソースが既に SLA ポリシーに関連付けられているかどうかに関係なく、1 つ以上のリソースに対してオンデマンド・バックアップ・ジョブを実行するには、「**ジョブの作成**」をクリックして、「**アドホック・バックアップ (Ad hoc backup)**」を選択し、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の説明に従ってください。

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**」を展開します。
2. バックアップするリソースを選択します。
 - 「**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。
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**」を選択しています。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。

The screenshot shows a configuration window titled "Options". Inside, there is a checkbox labeled "Enable Log Backup" which is currently unchecked. Below this checkbox is a label "Maximum Parallel Streams per Database" followed by a text input field containing the number "1". At the bottom left of the window is a blue button labeled "Save".

図 41. 「ログ・バックアップの有効化 (Enable Log Backup)」オプションが示されている「バックアップ」ペイン

「ログ・バックアップを有効にする」オプションを有効にしてオンデマンド・ジョブを実行すると、ログ・バックアップが実施されます。ただし、ジョブが再びスケジュールで実行されると、バックアップのチェーンでセグメントが欠落する可能性を防止するために、そのジョブ実行に対してこのオプションは無効になります。

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 が保存された後、そのポリシーの「**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。

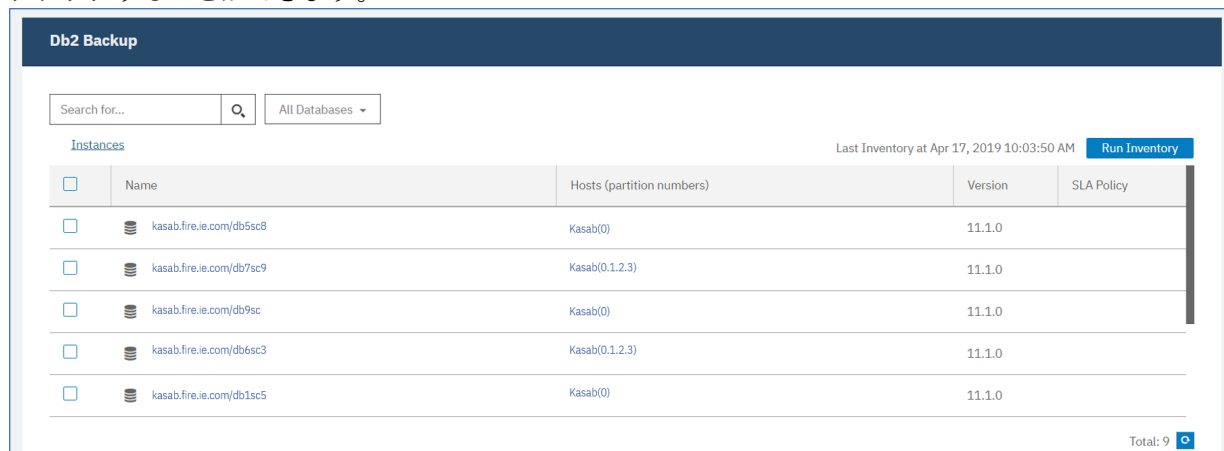
SLA バックアップ・ジョブの定義






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。

インスタンス全体をすべての関連データとともに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。



Db2 Backup				
Search for...		Q	All Databases ▾	
Instances				
Last Inventory at Apr 17, 2019 10:03:50 AM Run Inventory				
<input type="checkbox"/>	Name	Hosts (partition numbers)	Version	SLA Policy
<input type="checkbox"/>	 kasab.fire.ie.com/db5sc8	Kasab(0)	11.1.0	
<input type="checkbox"/>	 kasab.fire.ie.com/db7sc9	Kasab(0.1.2.3)	11.1.0	
<input type="checkbox"/>	 kasab.fire.ie.com/db9sc	Kasab(0)	11.1.0	
<input type="checkbox"/>	 kasab.fire.ie.com/db6sc3	Kasab(0.1.2.3)	11.1.0	
<input type="checkbox"/>	 kasab.fire.ie.com/db1sc5	Kasab(0)	11.1.0	


Total: 9 

図 42. インスタンスを示す「Db2 バックアップ」ペイン

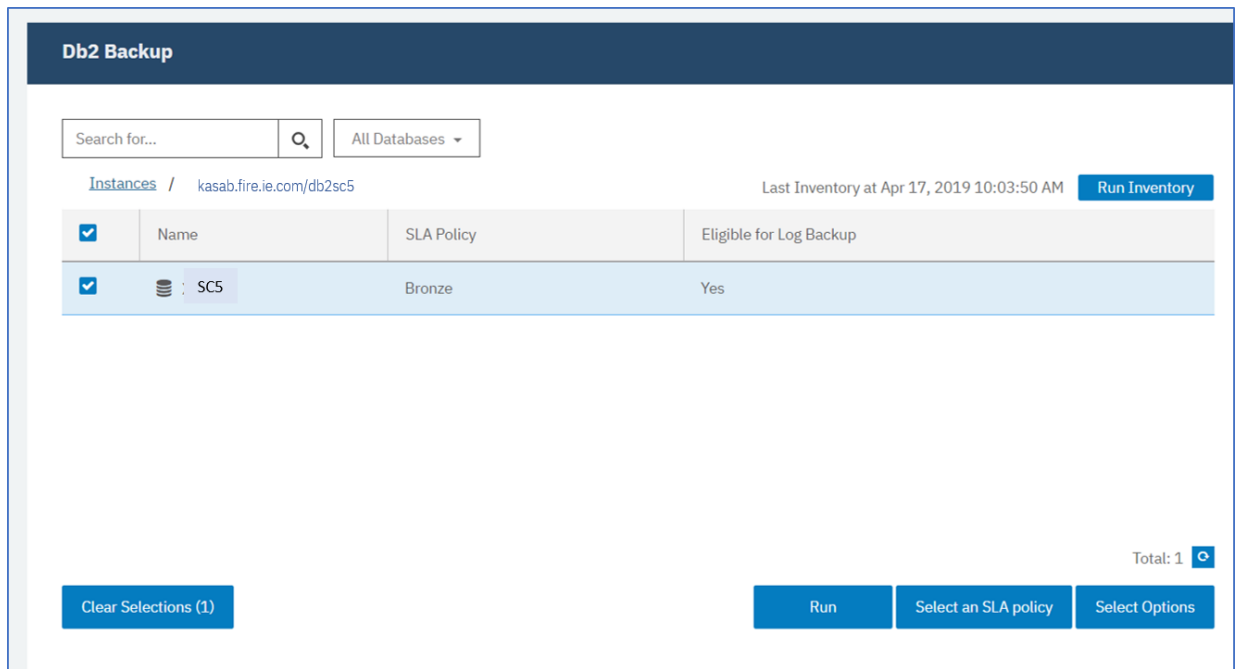


図 43. インスタンスのデータベースを示す Db2 バックアップ・ペイン

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。

事前定義された「ゴールド」、「シルバー」、および「ブロンズ」の各ポリシーの頻度と保存率はそれぞれ異なります。「**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。

SLA Policy Status									
Filter Job Log: INFO x WARN x ERROR x SUMMARY x									
Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options		
Demo	Every 1 Days at 6:05:00 AM	0	0	0	Apr 24, 2019 6:05:00 AM	IDLE		Actions	
Bronze	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions	
Silver	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions	
Gold	Every 4 Hours	0	0	0	Apr 23, 2019 2:05:00 PM	IDLE		Actions	

図 44. 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、364 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。

SLA Policy Status

Filter Job Log: INFO x WARN x ERROR x SUMMARY x v

Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	
> Demo	Every 1 Days at 6:05:00 AM	0	0	0	Apr 24, 2019 6:05:00 AM	IDLE		Actions v
> Bronze	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Actions v
> Silver	Every 1 Days at 6:10:00 AM	0	0	0	Apr 24, 2019 6:10:00 AM	IDLE		Start Pause Schedule
> Gold	Every 4 Hours	0	0	0	Apr 23, 2019 2:05:00 AM	IDLE		Actions v

Auto Refresh

Total: 4

図 45. SLA ポリシー

ヒント: 選択された SLA ポリシーのジョブが実行されると、その SLA ポリシーに関連付けられているすべてのリソースがバックアップ操作に含まれます。選択されたリソースのみをバックアップする場合、オンデマンド・ジョブを実行します。オンデマンド・ジョブはバックアップ操作を即時に実行します。

- 単一リソースのオンデマンド・バックアップ・ジョブを実行するには、リソースを選択し、「実行」をクリックします。リソースが SLA ポリシーに関連付けられていない場合、「実行」ボタンは使用できません。
- 1 つ以上のリソースに対してオンデマンド・バックアップ・ジョブを実行するには、「ジョブの作成」をクリックし、「アドホック・バックアップ」を選択して、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の指示に従います。

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。

Configure Options [X]

☐ Pre-Script

☐ Post-Script

☐ Continue job/task on script error

Exclude Resources

Force full backup of resources.

Forcing a full backup of a resource, runs a new full base backup of that resource.

Save

図 46. 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差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、[362 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・ペインにリストアされます。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、[360 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するユーザーに 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、[503 ページの『第 18 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、「ジョブの作成」 > 「リストア」をクリックします。
「リストア」ウィザードが開きます。
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** をクリックし、「次へ」をクリックします。

ヒント:

- 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「**リストアのプレビュー (Preview Restore)**」をクリックします。
 - ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「**拡張セットアップ (Advanced Setup)**」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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。そのデータベース名のプラス・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一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. 「**ソース・スナップショット**」 ページのフィールドに入力して、「**次へ**」をクリックします。
表示されるフィールドは、「**ソースの選択**」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none">・ リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。・ 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。

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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」 > 「サイト」 ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」 > 「バックアップ・ストレージ」 > 「オブジェクト・ストレージ」 ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」 ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」 > 「バックアップ・ストレージ」 > 「オブジェクト・ストレージ」 ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」 ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1 次 スナップショットのリストア元の 1 次サイト。</p> <p>2 次 スナップショットのリストア元の 2 次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

6. 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・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利用できる唯一の「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。

7. 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。

8. 「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。

9. 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。
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。
 - 11.「**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。
- 12.「**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。
- 13.「**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・ペインにリストアされます。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、360 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するユーザーに 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、503 ページの『第 18 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、「ジョブの作成」 > 「リストア」をクリックします。
「リストア」ウィザードが開きます。
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** をクリックし、「次へ」をクリックします。

ヒント:

- 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「リストアのプレビュー (Preview Restore)」をクリックします。
 - ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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。そのデータベース名のプラス・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一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. 「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> • リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <p>バックアップ vSnap サーバーにバックアップされているデータをリストアします。</p> <p>複製 vSnap サーバーに複製されているデータをリストアします。</p>

オプション	説明
	<p>オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。</p> <p>アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ(テープ)にコピーされているデータをリストアします。</p> <ul style="list-style-type: none"> 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p>

オプション	説明
	1 次 スナップショットのリストア元の 1 次サイト。 2 次 スナップショットのリストア元の 2 次サイト。 クラウドまたはリポジトリ・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・サービスまたはリポジトリ・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・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。

6. 「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・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。

7. 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。
8. 367 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。
9. 「**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。
10. 「**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、[360 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するユーザーに 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、[503 ページの『第 18 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・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、「**ジョブの作成**」 > 「**リストア**」をクリックします。
「リストア」ウィザードが開きます。
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** をクリックし、「**次へ**」をクリックします。

ヒント:

- 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「**リストアのプレビュー (Preview Restore)**」をクリックします。

- ・ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「**拡張セットアップ (Advanced Setup)**」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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。そのデータベース名のプラス・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一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. 「**ソース・スナップショット**」ページのフィールドに入力して、「**次へ**」をクリックします。
表示されるフィールドは、「**ソースの選択**」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> ・ リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <p>バックアップ vSnap サーバーにバックアップされているデータをリストアします。</p> <p>複製 vSnap サーバーに複製されているデータをリストアします。</p> <p>オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。</p> <p>アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。</p> <ul style="list-style-type: none"> ・ 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
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・サービスまたはリポジトリ・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・サーバーへコピーされたリストア・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、バックアップとコピー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。

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1 次 スナップショットのリストア元の 1 次サイト。</p> <p>2 次 スナップショットのリストア元の 2 次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
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、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	クラウド・サービスまたはリポジトリ・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
サーバーを使用します	クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。

6. 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・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。

7. 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。

8. 367 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。


9. 「**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。

10. 「**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。

Exchange Server

Exchange アプリケーション・サーバー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。

Exchange Server の前提条件

IBM Spectrum Protect Plus を使用して 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、62 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 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

Exchange エージェントが IBM Spectrum Protect Plus 環境で機能するには、Exchange ユーザー・アカウント用に適切な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

ローカル管理者特権と正しい役割ベースのアクセス制御 (RBAC) 権限を持つ Exchange ユーザーを使用して Exchange Server を IBM Spectrum Protect Plus に登録する必要があります。

高細分度リストア操作でも、ローカル管理者特権と正しい RBAC 権限を持つ Exchange ユーザーを使用する必要があります。

Exchange ユーザーの最小要件を満たすには、以下のステップを実行します。

1. Exchange ユーザーが、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・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 ユーザーについては、以下のいずれかのアクションを実行して、ユーザー・アカウントをローカルの Administrators 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、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。「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ます。

2. 役割とスコープを設定します。

- Exchange ユーザーに正しい RBAC 権限があることを確認します。

メールボックス・リストア操作を実行する各 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。

- Active Directory 許可
- アプリケーション偽装
- 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・タスクを実行するユーザーを、上記の役割が含まれている Exchange Server 役割グループに配置します。

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。Organization Management 役割グループには、デフォルトで、上記の役割のすべてではなくとも、ほとんどが含まれています。

複数のメールボックス・リストア・タスクを実行する必要があるユーザーを、**Organization Management** 役割グループに配置します (グループに上記のすべての役割が含まれていることを確認してください)。

あるいは、そのユーザーを、既に作成してある別の役割グループや、上記の役割が含まれている他の組み込み役割グループに配置することも可能です。**Organization Management** 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。

重要: 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

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。

Exchange 証明書

高細分度リストア操作時にメールボックス・ブラウザーが機能するには、Exchange デジタル証明書がインストールされ、構成されている必要があります。ご使用の環境で現行の Exchange 証明書が正しくインストールされ、構成されていることを確認してください。

注: Exchange 2016 および Exchange 2019 では、Exchange Server は、デフォルトで Transport Layer Security (TLS) を使用するように構成されます。この TLS セキュリティーは、ローカル・サーバー上の内部 Exchange Server 間および Exchange サービス間の通信を暗号化します。

Exchange アプリケーション・サーバーの追加

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

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

Exchange アプリケーション・サーバーを追加するには、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」 > 「データベース」 > 「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」 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. Active Directory 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、[380 ページの『特権』](#)を参照してください。

5. 「**最大同時データベース数**」フィールドで、SLA ポリシーごとに同時にバックアップできるデータベースの最大数を設定します。デフォルトは 10 です。有効な値は 1 から 99 です。

この値は、SLA ポリシーに関連付けられているデータベースの数より高い場合も低い場合もあります。例えば、SLA ポリシーに 10 個のデータベースが関連付けられていて、この値が 2 に設定される場合、10 個のうち 2 個のみのデータベースに対してバックアップ操作が同時に実行されます。すべてのデータベースがバックアップされるまで、各バックアップ操作が完了すると、2 番目のバックアップ操作が開始されます。SLA ポリシーに 5 個のデータベースが関連付けられていて、この値が 10 に設定される場合、5 個のすべてのデータベースのバックアップ操作が同時に実行されます。

このオプションは、複数のデータベースに関連付けられている SLA ポリシーにのみ適用されます。1 個のデータベースのみに関連付けられている SLA ポリシーの場合、このオプションは機能しません。

同時データベース・バックアップ操作の最大数は、環境によって制限されます。考慮すべき点は、vSnap サーバー構成、ネットワーク帯域幅、および IBM Spectrum Protect Plus サーバーの物理ディスク構成です。

最適なパフォーマンスを得るための IBM Spectrum Protect Plus 環境のチューニング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。

6. 「**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 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を実行する手順については、[382 ページの『インベントリの実行による 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、[384 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。

インベントリの実行による Exchange データベースの検出

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、[381 ページの『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**」 > 「**データベース**」 > 「**Exchange**」を展開します。

2. 「**インベントリの実行**」をクリックします。

インベントリの実行中、ボタンのラベルが「**インベントリが進行中**」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を実行できますが、インベントリ・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・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・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。ジョブを名前を検索するには、「**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、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。

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**」 > 「**データベース**」 > 「**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。

Exchange データベースのバックアップ

Exchange データベースを保護する目的で、差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 IBM Spectrum Protect Plus に登録されていることを確認してください。詳しくは、[381 ページの『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**」 > 「**データベース**」 > 「**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。
SLA ポリシーに関連付けられている複数のデータベースに対してオンデマンド・バックアップ・ジョブを実行するには、「**ジョブの作成**」をクリックして、「**アドホック・バックアップ (Ad hoc backup)**」を選択し、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の説明に従ってください。
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、[384 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 Server インスタンスごとに 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 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 to 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」 > 「データベース」 > 「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、228 ページの『ハイパーバイザー、データベース、およびファイル・システムの 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、384 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差分バックアップされます。
7. 「保存」をクリックします。

Exchange データベース・ログのバックアップ

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」>「データベース」>「Exchange」を展開します。
2. 保護する Exchange Server 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。
「ログ・バックアップを有効にする」オプションを有効にしてオンデマンド・ジョブを実行すると、ログ・バックアップが実施されます。ただし、ジョブが再びスケジュールで実行されると、バックアップのチェーンでセグメントが欠落する可能性を防止するために、そのジョブ実行に対してこのオプションは無効になります。
4. **制約事項:** 「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

「分」、「時間」、「日」、「週」、「月」、または「年」でログ・バックアップの頻度を入力します。「週」が選択されている場合、1つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。
5. 「開始時刻」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 Exchange Server 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

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」 > 「データベース」 > 「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 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。

永久差分バックアップ戦略

IBM Spectrum Protect Plus では、永久差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、一連の継続的な差分バックアップ・ジョブが行われます。

永久差分バックアップ・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
- すべての差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 永久差分バックアップ・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。

Exchange データベースのリストア

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。「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 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、[384 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、[503 ページの『第 18 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

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 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、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 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、[503 ページの『第 18 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。

- ナビゲーション・ペインで、「保護の管理」 > 「データベース」 > 「Exchange」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。
ヒント:
 - 「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Exchange」をクリックしても、ウィザードを開くことができます。
 - 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「リストアのプレビュー (Preview Restore)」をクリックします。
 - ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
- 「ソースの選択」 ページで、以下のアクションを実行します。
 - 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。
 - 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。
 - 「次へ」 をクリックして先に進みます。
- 「ソース・スナップショット」 ページで、作成する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

1 回限りのリストア操作を実行します。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。

- 「ソース・スナップショット」 ページのフィールドに入力して、「次へ」をクリックします。
 表示されるフィールドは、「ソースの選択」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <p>バックアップ vSnap サーバーにバックアップされているデータをリストアします。</p> <p>複製 vSnap サーバーに複製されているデータをリストアします。</p>

オプション	説明
	<p>オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。</p> <p>アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ(テープ)にコピーされているデータをリストアします。</p> <ul style="list-style-type: none"> 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p>

オプション	説明
	1 次 スナップショットのリストア元の 1 次サイト。 2 次 スナップショットのリストア元の 2 次サイト。 クラウドまたはリポジトリ・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・サービスまたはリポジトリ・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・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。

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 リポジトリから直接データ・ファイルを使用して新規リカバリー・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、[391 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. 「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。
7. 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。

8. 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。
9. 「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。
10. 「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

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か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」 > 「データベース」 > 「Exchange」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。


ヒント:


- ・ 「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Exchange」をクリックしても、ウィザードを開くことができます。
- ・ 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「リストアのプレビュー (Preview Restore)」をクリックします。

- ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「**拡張セットアップ (Advanced Setup)**」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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。

- 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。

- 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。

- 「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、作成する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

1 回限りのリストア操作を実行します。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。

4. 「ソース・スナップショット」 ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <p>バックアップ vSnap サーバーにバックアップされているデータをリストアします。</p> <p>複製 vSnap サーバーに複製されているデータをリストアします。</p> <p>オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。</p> <p>アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。</p> <ul style="list-style-type: none"> 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、

オプション	説明
	および「 アーカイブ 」が表示されている場合、「 バックアップ 」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1 次 スナップショットのリストア元の 1 次サイト。</p> <p>2 次 スナップショットのリストア元の 2 次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セレクト	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。

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・サービスまたはリポジトリ・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・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。

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。

- 「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。
- 「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。
- 「宛先パス」フィールドに、サーバー上のデータベース・ファイルの新規ディレクトリーのロケーション (.edb の名前を含む) およびログのロケーションを入力します。



警告: 「宛先パス」フィールドに入力する宛先ディレクトリーは、既にアプリケーション・ホストに存在している必要があります。そうでない場合は、リストア操作を実行する前に、サーバーに必要なディレクトリーを作成してください。

例えば、データベース名が Database_A の場合は、C:\%<new_destination_path>%Database_A.edb と入力して、ログのロケーションとして C:\%<new_logs_path> と入力します。

6. 「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。
7. 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。

8. 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。
9. 「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。
10. 「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 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」 > 「データベース」 > 「Exchange」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。

ヒント:

- ・ 「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Exchange」をクリックしても、ウィザードを開くことができます。
 - ・ 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「リストアのプレビュー (Preview Restore)」をクリックします。
 - ・ ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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。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、作成する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

1 回限りのリストア操作を実行します。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。

4. 「ソース・スナップショット」 ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <ul style="list-style-type: none"> バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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</p>

オプション	説明
	に使用される vSnap サーバーは、バックアップとコピー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。

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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</p>

オプション	説明
	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、バックアップとコピー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。

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 リポジトリから直接データ・ファイルを使用して新規リカバリー・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、ソースと宛先のパス情報を表示します。「宛先パス」 フィールドに、代替ホスト上の Exchange データベース・ファイルのディレクトリーのロケーション (.edb の名前を含む) およびログのロケーションを入力します。



警告: 「宛先パス」 フィールドに入力する宛先ディレクトリーは、既に代替ホストに存在している必要があります。そうでない場合は、リストア操作を実行する前に、代替ホストに必要なディレクトリーを作成してください。

例えば、データベース名が Database_A の場合は、C:\<new_destination_path>\Database_A.edb と入力して、ログのロケーションとして c:\<new_logs_path> と入力します。

6. 「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。
7. 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。

8. 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。
9. 「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。
10. 「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、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 (380 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 403 ページの『[15](#)』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」 > 「データベース」 > 「Exchange」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。

ヒント:

- ・「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Exchange」をクリックしても、ウィザードを開くことができます。
 - ・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「リストアのプレビュー (Preview Restore)」をクリックします。
 - ・ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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、作成する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**
1 回限りのリストア操作を実行します。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。
4. 「ソース・スナップショット」 ページのフィールドに入力して、「次へ」 をクリックします。
- 表示されるフィールドは、「ソースの選択」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。
- オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド**

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> ・ リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <p>バックアップ vSnap サーバーにバックアップされているデータをリストアします。</p> <p>複製 vSnap サーバーに複製されているデータをリストアします。</p>

オプション	説明
	<p>オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。</p> <p>アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ(テープ)にコピーされているデータをリストアします。</p> <ul style="list-style-type: none"> 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p>

オプション	説明
	1 次 スナップショットのリストア元の 1 次サイト。 2 次 スナップショットのリストア元の 2 次サイト。 クラウドまたはリポジトリ・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・サービスまたはリポジトリ・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・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。

- 「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。
- 「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。
- 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。
- 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。
- 「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。
- 「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。
- 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。
- 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 (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。

13. 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。
14. 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。
15. 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。
16. 「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 62. 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	<ol style="list-style-type: none"> 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 62. 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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>「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。</p> <p>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。</p> <p>d. 「値」フィールドで、フィルター値を指定します。</p> <p>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。</p> <p>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。</p>

17. 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。

18. 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 63. 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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>
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	<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>

表 63. 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	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 親フォルダー内のサブフォルダーをリストアするには、<code>parent_folder_name/sub_folder_name</code> 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、<code>parent_folder_name/*</code> 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。 <p>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。</p>

19. 「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)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>)。

20. 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 Management Console (MMC) GUI を使用して、Exchange 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 (380 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 410 ページの『[15](#)』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」 > 「データベース」 > 「Exchange」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。


ヒント:

- 「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Exchange」をクリックしても、ウィザードを開くことができます。
- 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「リストアのプレビュー (Preview Restore)」をクリックします。
- ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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、作成する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

1 回限りのリストア操作を実行します。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。

4. 「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <ul style="list-style-type: none"> バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」 > 「サイト」 ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」 > 「バックアップ・ストレージ」 > 「オブジェクト・ストレージ」 ペインで定義されます。</p>

オプション	説明
	<p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

- 「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。
- 「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。
- 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。
- 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。
- 「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。
10. 「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。
 11. 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。
 12. 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。
 13. 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。
 14. 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。
 15. 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。
 16. 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。
 17. 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 64. 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。

表 64. リストア・オプション (続き)	
オプション	アクション
代替ロケーションにメールをリストア	<p>メール項目を別のメールボックスにリストアします。</p> <ul style="list-style-type: none"> 「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。 <p>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。</p>
<p>非 Unicode の PST ファイルにメールをリストア</p> <p>制約事項:</p> <ul style="list-style-type: none"> 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。 	<p>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</p> <p>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。</p> <p>.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。</p>
Unicode の PST ファイルにメールをリストア	<p>メール項目を Unicode の .pst ファイルにリストアする</p> <p>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。</p> <p>ヒント:</p> <p>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。</p> <p>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。</p>

表 64. リストア・オプション (続き)	
オプション	アクション
パブリック・フォルダー・メールボックスのリストア	<p>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。</p> <p>「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。</p> <ul style="list-style-type: none"> 親フォルダー内のサブフォルダーをリストアするには、<i>parent_folder_name/sub_folder_name</i> 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、<i>parent_folder_name/*</i> 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。 <p>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。</p>
アーカイブ・メールボックスへのメールのリストア	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 親フォルダー内のサブフォルダーをリストアするには、<i>parent_folder_name/sub_folder_name</i> 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、<i>parent_folder_name/*</i> 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。 <p>「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。</p>

表 64. リストア・オプション (続き)	
オプション	アクション
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	<p>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。</p> <p>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。</p>

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)(<http://www.ibm.com/support/docview.wss?uid=ibm10882270>)。

18. 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」 > 「データベース」 > 「Exchange」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。

ヒント:

- ・「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Exchange」をクリックしても、ウィザードを開くことができます。
 - ・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「リストアのプレビュー (Preview Restore)」をクリックします。
 - ・ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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、作成する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

1 回限りのリストア操作を実行します。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。

- 4.「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <ul style="list-style-type: none"> バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピーの操作を完了するため</p>

オプション	説明
	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。

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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</p>

オプション	説明
	に使用される vSnap サーバーは、バックアップとコピー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。

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. 「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。

7. 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。

8. 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。
9. 「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。
10. 「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 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」 > 「データベース」 > 「Exchange」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。

ヒント:

- ・ 「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Exchange」をクリックしても、ウィザードを開くことができます。
 - ・ 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「リストアのプレビュー (Preview Restore)」をクリックします。
 - ・ ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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。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、作成する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

1 回限りのリストア操作を実行します。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。

4. 「ソース・スナップショット」 ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none">リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

5. 「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。
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。

6. 「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。
7. 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。
8. 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。
9. 「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。
10. 「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。
11. 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。
12. 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、[68 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、68 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、423 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、421 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。

A blue rectangular button with a white plus icon on the left and the text "Add application server" in white.

3. 「アプリケーション・プロパティ」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 47. 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、[503 ページの『第 18 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。

保護のための MongoDB Ops Manager Application Database の登録

MongoDB Ops Manager Application Database を保護するには、最初に Ops Manager のホスト・アドレスを IBM Spectrum Protect Plus に登録する必要があります。

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**」 > 「**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**」をクリックします。

 Add application server

3. 「**アプリケーション・プロパティ**」フォームに、Ops Manager Application Database のホスト・アドレスを入力します。[423 ページの『MongoDB アプリケーション・サーバーの追加』](#)で概要が説明されている手順に従って、インスタンスを取得し、資格情報を設定します。

次の例に示されているように、Ops Manager Application Database は「**インスタンス**」表にリストされます。

```
metali8.limerick.ie.ibm.com Connection: '333.0.5.1:88888' Ops Manager Application Database
```

次のタスク

MongoDB Ops Manager Application Database はバックアップに使用できます。データを保護するためのバックアップ・ジョブとリストア・ジョブを定義することができます。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。詳細については、[427 ページの『MongoDB データのバックアップ』](#)および [429 ページの『通常の SLA ジョブの定義』](#)を参照してください。

MongoDB リソースの検出

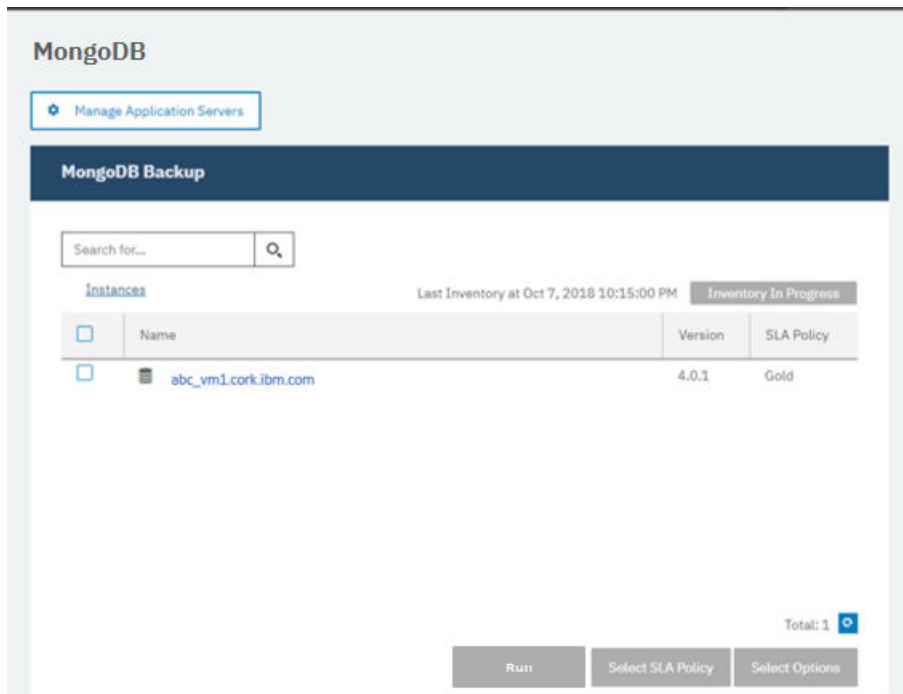
MongoDB アプリケーション・サーバーを IBM Spectrum Protect Plus に追加した後、インベントリーが自動的に実行され、MongoDB インスタンスおよびデータベースがすべて検出されます。選択したホストのすべての MongoDB データベースの検出、リスト、および保管を行うために、任意のアプリケーション・サーバーでインベントリーを手動で実行できます。

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。ジョブを名前を検索するには、「**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。

1. Physical - Basic Test for physical host network configuration

Name	Description	Status	Message
Host FQDN Resolvable Test	Host FQDN must be resolvable to an IPv4 address	✓	
Socket Connection Test	Must allow socket connection on port 22 for Linux	✓	

2. Remote - Remote executor test for session creation and remote agent deployment

Name	Description	Status	Message
Remote Session Test	Latest remote agent must be installed on host, SSH and SFTP service must be installed on Linux host, and port must be open to create session to SSH service.	✓	
Remote Agent Execute Test	Remote agent must be configured correctly using user credentials with sufficient privileges.	✓	

3. LINUX - Basic Linux prerequisites for file and volume operations

Name	Description	Status	Message
Sudo Privileges	User must have password-less sudo privileges	✓	

OK

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

MongoDB データを保護するためのバックアップ・ジョブを定義することができます。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、vSnap ボリュームおよび NFS 共有を作成します。差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、503 ページの『[第 18 章 ユーザー・アクセスの管理](#)』および 421 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。

SLA ポリシーに関連付けられている複数のデータベースに対してオンデマンド・バックアップ・ジョブを実行するには、「**ジョブの作成**」をクリックし、「**アドホック・バックアップ (Ad hoc backup)**」を選択し、487 ページの『[アドホック・バックアップ・ジョブの実行](#)』の手順を実行します。

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、そのポリシー名に対する「**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、そのポリシー名に対する「**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。

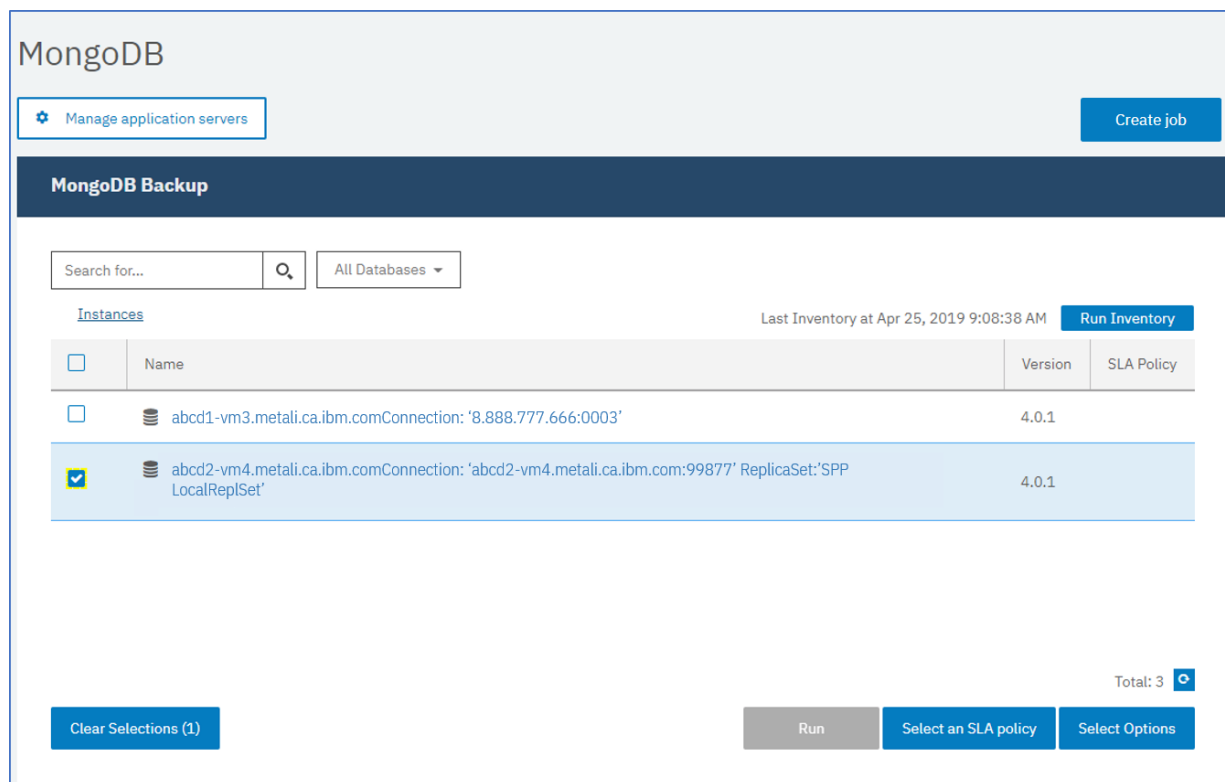


図 48. インスタンスを示す「MongoDB バックアップ」ペイン

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。

The screenshot shows the 'Options' section with a 'Maximum Parallel Streams per Database' input field set to '1' and a 'Save' button. Below this is the 'SLA Policy Status' section, which includes a 'Filter Job Log' dropdown menu and a table with columns: Policy, Frequency, Total, Succeeded, Failed, Next Run, Status, Policy Options, and Actions.

Policy	Frequency	Total	Succeeded	Failed	Next Run	Status	Policy Options	Actions
Gold	Every 4 Hours	1	1	0	Apr 25, 2019 10:05:00 AM	Idle		

図 49. 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、[430 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、そのポリシー名に対する「**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、そのポリシー名に対する「**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。

Configure Options ×

☐ Pre-Script

☐ Post-Script

☐ Continue job/task on script error

Exclude Resources

Force full backup of resources.

Forcing a full backup of a resource, runs a new full base backup of that resource.

Save

図 50. 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差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。臨時的な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行われるように、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、[427 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、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)および [421 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」 > 「ジョブの作成」をクリックしてから、「リストア」を選択して「リストア」ウィザードを開きます。

ヒント:

- 「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「MongoDB」をクリックしてウィザードを開くこともできます。
- 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。
- ウィザードはデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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) リストア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、作成する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

1 回限りのリストア操作を実行します。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。

- 4.「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <ul style="list-style-type: none"> バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピーの操作を完了するため</p>

オプション	説明
	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。

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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</p>

オプション	説明
	に使用される vSnap サーバーは、バックアップとコピー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。

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. 「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。

7. 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。

8. 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。

9. 「スケジュール」 ページで、「次へ」 をクリックして、「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。
10. 「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。

11. 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・ジョブを見つけて、「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、[427 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、[503 ページの『第 18 章 ユーザー・アクセスの管理』](#)および [421 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」>「ジョブの作成」をクリックしてから、「リストア」を選択して「リストア」ウィザードを開きます。


ヒント:


- 「ジョブと操作」>「ジョブの作成」>「リストア」>「MongoDB」をクリックしてウィザードを開くこともできます。
- 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。

- ・ウィザードはデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「**拡張セットアップ (Advanced Setup)**」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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。

- 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。

- 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。

- 「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、作成する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

1 回限りのリストア操作を実行します。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。

4. 「ソース・スナップショット」 ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> ・ リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <p>バックアップ vSnap サーバーにバックアップされているデータをリストアします。</p> <p>複製 vSnap サーバーに複製されているデータをリストアします。</p> <p>オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。</p> <p>アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。</p> <ul style="list-style-type: none"> ・ 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、

オプション	説明
	および「 アーカイブ 」が表示されている場合、「 バックアップ 」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1 次 スナップショットのリストア元の 1 次サイト。</p> <p>2 次 スナップショットのリストア元の 2 次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セレクト	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。

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・サービスまたはリポジトリ・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・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。

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、このオプションを選択して、上書きのアプリケーション・オプションを指定する方法をお勧めします。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. 「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。

7. 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。

8. 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。

9. 「スケジュール」 ページで、「次へ」をクリックして、「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。
10. 「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。

11. 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、427 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、503 ページの『第 18 章 ユーザー・アクセスの管理』および 421 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」 > 「ジョブの作成」をクリックしてから、「リストア」を選択して「リストア」ウィザードを開きます。

ヒント:

- 「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「MongoDB」をクリックしてウィザードを開くこともできます。
 - 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。
 - ウィザードはデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「拡張セットアップ (Advanced Setup)」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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。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、作成する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

1 回限りのリストア操作を実行します。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。

- 4.「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <ul style="list-style-type: none"> バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピーの操作を完了するため</p>

オプション	説明
	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。

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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</p>

オプション	説明
	に使用される vSnap サーバーは、バックアップとコピー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。

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. 「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。

7. 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。

8. 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。

9. 「スケジュール」 ページで、「次へ」 をクリックして、「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。
10. 「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。

11. 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」 > 「ジョブの作成」をクリックしてから、「リストア」を選択して「リストア」ウィザードを開きます。
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。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. 「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。
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」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。
6. 「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。

7. 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。
8. MongoDB システム・コマンド `ps -ef | grep mongod` を実行して、一時的なりかばりー MongoDB インスタンスのロケーションを見つけます。
9. 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>
```

10. **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>
```

11. 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。
12. 「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。

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のジョブを作成します。

ご使用の Oracle 環境が [78 ページの『Oracle サーバー・データベースのバックアップ要件とリストア要件』](#) 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」 > 「データベース」 > 「Oracle」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」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	<p>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。</p> <p>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」リストでユーザー名を選択します。</p> <p>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 <code>domain\username</code> 形式に従います。ユーザーがローカル管理者の場合は、<code>local_administrator</code> 形式を使用します。</p> <p>Kerberos ベースの認証の場合に限り、ユーザー ID は <code>username@FQDN</code> 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する必要があります。</p> <p>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。</p>
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 鍵の選択 (Select a SSH key) 」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) 「**データベースの取得**」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。	509 ページの『 役割の作成 』を参照してください。

関連概念

503 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

450 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。

453 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」 > 「データベース」 > 「Oracle」 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 Plus 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」 > 「データベース」 > 「Oracle」 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、[503 ページの『第 18 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、[448 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、[157 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。差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 つのノードから実行されます。バックアップ・ジョブが完了すると、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、[448 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**」 > 「**データベース**」 > 「**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: 選択された SLA ポリシーのジョブが実行されると、その SLA ポリシーに関連付けられているすべてのリソースがバックアップ操作に含まれます。選択されたリソースのみをバックアップする場合、オンデマンド・ジョブを実行します。オンデマンド・ジョブはバックアップ操作を即時に実行します。

- 単一リソースのオンデマンド・バックアップ・ジョブを実行するには、リソースを選択し、「**実行**」 をクリックします。リソースが SLA ポリシーに関連付けられていない場合、「**実行**」 ボタンは使用できません。
 - 1 つ以上のリソースに対してオンデマンド・バックアップ・ジョブを実行するには、「**ジョブの作成**」 をクリックし、「**アドホック・バックアップ**」 を選択して、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の指示に従います。
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する**」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。

「**ログ・バックアップを有効にする**」オプションを有効にしてオンデマンド・ジョブを実行すると、ログ・バックアップが実施されます。ただし、ジョブが再びスケジュールで実行されると、バックアップのチェーンでセグメントが欠落する可能性を防止するために、そのジョブ実行に対してこのオプションは無効になります。

「**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**」セクションのジョブに関連付けられ

ている「**ポリシー・オプション**」クリップボード・アイコン  アイコ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、バックアップや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、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。	453 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

487 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、450 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、503 ページの『第 18 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」 > 「データベース」 > 「Oracle」 > 「ジョブの作成」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。

ヒント：

- ウィザードは、「ジョブと操作」 > 「ジョブの作成」 > 「リストア」 > 「Oracle」をクリックして開くこともできます。
 - 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・ペインで「リストアのプレビュー (Preview Restore)」をクリックします。
 - ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「**拡張セットアップ (Advanced Setup)**」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。
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。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、作成する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

1 回限りのリストア操作を実行します。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。

4. 「ソース・スナップショット」 ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」 ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none">リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 バックアップ vSnap サーバーにバックアップされているデータをリストアします。 複製 vSnap サーバーに複製されているデータをリストアします。 オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。 アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピー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。</p>

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. 「**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。

7. 「**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ます。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。

8. 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、バックアップや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。

9. 「**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。

10. 「**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

487 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

448 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。

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 85 ページの『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』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・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 Microsoft SQL Server ホストは、特定のユーザー・アカウントを使用して、その特定の 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。

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: [Task Scheduler Error "A specified logon session does not exist"](#)

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」 > 「データベース管理」 > 「SQL」 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」 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する必要があります。

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。	509 ページの『役割の作成』 を参照してください。

関連概念

[503 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

[463 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。

[467 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」 > 「データベース管理」 > 「SQL」 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 Plus 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」 > 「データベース管理」 > 「SQL」 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 vSnap LUN ボリュームを作成し、その iSCSI LUN 上に NTFS 共有を作成します。差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 LUN を SQL Server のサーバーにマップし、バックアップが完了した場所に NTFS ボリュームをマウントします。ログ・バックアップが有効な場合、IBM Spectrum Protect Plus は別個の vSnap ボリュームを作成し、そのボリューム上に CIFS を作成します。ログ・バックアップ・トランザクション・ファイルは、ログ・バックアップ用に作成されたスケジュールに従ってこの共有にコピーされます。

バックアップ・ジョブが完了すると、IBM Spectrum Protect Plus エージェントは、SQL Server の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。

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/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、[503 ページの『第 18 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 サーバーとの間で iSCSI 経路が使用可能でなければなりません。詳しくは、[Microsoft iSCSI Initiator Step-by-Step Guide](#)。
- 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。
- 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 つ追加が必要です。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。
- IBM Spectrum Protect Plus は、データベース・バックアップとトランザクション・ログ・バックアップをサポートします。IBM Spectrum Protect Plus から開始されたバックアップによって作成されたレコードの msdb.dbo.backupset に製品名が取り込まれます。
- SQL のログ・バックアップについて詳しくは、[466 ページの『ログ・バックアップ』](#)を参照してください。

注：Volume Shadow Copy Services (VSS) フレームワークの制限事項により、先行スペース、末尾スペース、および印刷不能文字は、データベース名には使用できません。詳しくは、<https://>

support.microsoft.com/en-sg/help/2014054/backing-up-a-sql-server-database-using-a-vss-backup-application-may-fa を参照してください。

次のアクションを実行してください。

- バックアップする SQL Server を登録します。詳しくは、[461 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、[157 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・ジョブをセットアップして実行する前に、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してください。この設定は、ボリュームごとに 1 つ構成されます。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基づいて、「最大サイズ」を「無制限」または妥当なサイズに設定し、次に「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・ジョブ中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」 > 「データベース管理」 > 「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: 選択された SLA ポリシーのジョブが実行されると、その SLA ポリシーに関連付けられているすべてのリソースがバックアップ操作に含まれます。選択されたリソースのみをバックアップする場合、オンデマンド・ジョブを実行します。オンデマンド・ジョブはバックアップ操作を即時に実行します。
 - 単一リソースのオンデマンド・バックアップ・ジョブを実行するには、リソースを選択し、「実行」をクリックします。リソースが SLA ポリシーに関連付けられていない場合、「実行」ボタンは使用できません。
 - 1 つ以上のリソースに対してオンデマンド・バックアップ・ジョブを実行するには、「ジョブの作成」をクリックし、「アドホック・バックアップ」を選択して、[487 ページの『アドホック・バックアップ・ジョブの実行』](#)の指示に従います。
5. 「オプションの選択」をクリックして追加のオプションを指定してから、バックアップ・ジョブを保存してください。

ログ・バックアップの有効化

トランザクション・ログのバックアップを有効にするには、このオプションを選択します。これらのログは、特定時点リストア操作などのリカバリー・オプションに使用されます。バックアップ・ジョブでログ・バックアップが有効になっている場合、バックアップ中はトランザクションが継続してログに記録されます。ログ・ファイルのバックアップで中断が検出された場合には、通知が送信されます。

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。ログ・バックアップの処理のためにステージング領域は必須ではありません。

「ログ・バックアップを有効にする」オプションを有効にしてオンデマンド・ジョブを実行すると、ログ・バックアップが実施されます。ただし、ジョブが再びスケジュールで実行されると、バックアップ

のチェーンでセグメントが欠落する可能性を防止するために、そのジョブ実行に対してこのオプションは無効になります。

以下のオプションのいずれかを選択してください。

「**並列ストリームを使用して一度に1つずつデータベース・ファイルをバックアップする (Back up database files one at a time using parallel streams)**」このオプションを選択すると、並列ストリームを使用して、データベースを順次バックアップします。


「**並列ストリームを使用してデータベース・ファイルをバックアップする (Back up database files in parallel using parallel streams)**」このオプションを選択すると、並列ストリームを使用して、データベースを並列でバックアップします。

最後に、バックアップ・プロセス中にデータベースごとに使用するデータ・ストリームの最大数を選択して、「**データベースごとの最大並列ストリーム数**」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を使用すると、場合によってはバックアップ速度が向上する可能性があります。

6. 「**保存**」をクリックして、バックアップ・ジョブのオプションを保存します。

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、「**ジョブと操作**」ウィンドウから手動で実行することもできます。

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**」セクションのジョブに関連付けられ

ている「**ポリシー・オプション**」クリップボード・アイコン  アイコ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、スクリプトが実行される予定のアプリケーション・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。

このオプションが有効になっていない場合は、バックアップや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、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、標準の英数字に加えて、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・ジョブ定義を作成します。	467 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

[487 ページの『バックアップ操作とリストア操作のスキプトの構成』](#)

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

[481 ページの『オンデマンドでのジョブの開始』](#)

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。

ログ・バックアップ

データベースのアーカイブ・ログ・ファイルには、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、リストア操作の一環としてロールフォワード・リカバリー・プロセスを実行できます。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。Microsoft SQL Server データをリストアするときに、ロールフォワード・リカバリーを実行できるように、バックアップ・ジョブでログ・バックアップが有効になっていることを確認してください。

初めてログ・バックアップを有効にする場合、SLA ポリシーに対するバックアップ・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 リポジトリに別個のボリュームが作成されます。このボリュームは、SQL 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。このボリュームは、「**ログ・バックアップを有効にする**」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、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。ログ・バックアップを有効にするには、[463 ページの『SQL Server データのバックアップ』](#)の説明に従ってください。

ログ・バックアップ操作をセットアップする前に、以下の基準を確認してください。

- ログ・バックアップを実行するには、SQL Server エージェント・ユーザーはローカル Windows 管理者でなければなりません。このユーザーには、SQL Server エージェント・ジョブを管理するために sysadmin 権限が必要です。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。各 SQL Server インスタンスで、SQL Server エージェント・ユーザーは、SQL Server サービスおよび SQL Server エージェント・サービス・アカウントのユーザーでもある必要があります。この規則は、保護されるすべての SQL Server インスタンスに適用されます。
- IBM Spectrum Protect Plus は、単純リカバリー・モデルのログ・バックアップ操作をサポートしていません。
- 複数のバックアップ・ジョブを使用して単一の SQL 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。このオーバーラップが原因で、特定時点リストア・ジョブが失敗する可能性があります。
- ログが vSnap リポジトリにコピーされる前に、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。
- IBM Spectrum Protect Plus は、データベース・バックアップとトランザクション・ログ・バックアップをサポートします。IBM Spectrum Protect Plus から開始されたバックアップによって作成されたレコードの msdb.dbo.backupset に製品名が取り込まれます。

- 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る状態で SQL バックアップ・ジョブが完了すると、そのジョブが完了するまでのすべてのトランザクション・ログは SQL Server 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・バックアップがバックアップされていないと、ログ・パージは発生しません。
- 2 次 SQL Server Always On データベースに対するログ・バックアップ操作は、次のエラーで失敗することがあります。

```
Log backup for database 'DatabaseName' on a secondary replica failed because a
synchronization point could not be established on the primary database.
```

このエラーが発生した場合は、可用性グループのバックアップ設定を「Primary」に変更してください。こうすると、ログは、1 次レプリカから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後、バックアップ設定を変更できます。

- 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以前のトランザクション・ログはすべて、オリジナル・データベースがリストアされた後で *condense* ディレクトリに置かれます。SQL Server バックアップ・ジョブの次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。

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、[463 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、[503 ページの『第 18 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・ファイルで使用する必要があります。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、<https://docs.microsoft.com/en-us/sql/t-sql/language-reference?view=sql-server-2017> 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」>「データベース管理」>「**SQL**」をクリックします。「**ジョブの作成**」をクリックして、「リストア」を選択して「リストア」ウィザードを開きます。


ヒント:


- ウィザードは、「ジョブと操作」>「ジョブの作成」>「リストア」>「**SQL**」をクリックして開くこともできます。
- 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・ペインで「**リストアのプレビュー (Preview Restore)**」をクリックします。
- ウィザードがデフォルトのセットアップ・モードで開きます。拡張セットアップ・モードでウィザードを実行するには、「**拡張セットアップ (Advanced Setup)**」を選択します。拡張セットアップ・モードでは、リストア・ジョブにさらに多くのオプションを設定できます。

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、作成する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

1 回限りのリストア操作を実行します。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。

- 4.「ソース・スナップショット」ページのフィールドに入力して、「次へ」をクリックします。

表示されるフィールドは、「ソースの選択」ページで選択された項目の数とリストア・タイプによって異なります。また、一部のフィールドは、関連フィールドを選択するまで表示されません。

オンデマンド・スナップショット、単一リソース・リストアの場合に表示されるフィールド

オプション	説明
日付範囲	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。
バックアップ・ストレージ・タイプ	<p>選択した日付範囲内のすべてのバックアップが行にリストされ、バックアップ操作が行われた時刻、およびバックアップのサービス・レベル・アグリーメント (SLA) ポリシーが表示されています。目的のバックアップ時刻と SLA ポリシーが含まれている行を選択して、以下のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> ・ リストア元となるバックアップ・ストレージ・タイプをクリックします。表示されるストレージ・タイプは、ご使用の環境で使用可能なタイプによって異なり、以下の順序で表示されます。 <p>バックアップ vSnap サーバーにバックアップされているデータをリストアします。</p> <p>複製 vSnap サーバーに複製されているデータをリストアします。</p> <p>オブジェクト・ストレージ クラウド・サービスまたはリポジトリ・サーバーにコピーされているデータをリストアします。</p> <p>アーカイブ クラウド・サービス・アーカイブまたはリポジトリ・サーバー・アーカイブ (テープ) にコピーされているデータをリストアします。</p> <ul style="list-style-type: none"> ・ 行の任意の場所をクリックします。行の左側から順に表示されているバックアップ・タイプのうち、最初のバックアップ・タイプがデフォルトで選択されているものです。例えば、ストレージ・タイプの「バックアップ」、「複製」、および「アーカイブ」が表示されている場合、「バックアップ」がデフォルトで選択されています。
リストア・ジョブに代替 vSnap サーバーを使用します	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・リソースまたはリポジトリ・サーバーへコピーされたリストア・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、バックアップとコピーの操作を完了するため</p>

オプション	説明
	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。

オンデマンド・スナップショットと複数リソース・リストア、特定時点リストア、または反復リストアの場合に表示されるフィールド

オプション	説明
リストア・ロケーションのタイプ	<p>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。</p> <p>サイト スナップショットがバックアップされた先のサイト。サイトは、「システム構成」>「サイト」ペインで定義されます。</p> <p>クラウド・サービス スナップショットがコピーされた先のクラウド・サービス。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー スナップショットがコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p> <p>クラウド・サービス・アーカイブ スナップショットがコピーされた先のクラウド・サービス・アーカイブ。クラウド・サービスは、「システム構成」>「バックアップ・ストレージ」>「オブジェクト・ストレージ」ペインで定義されます。</p> <p>リポジトリ・サーバー・アーカイブ スナップショットがテープにコピーされた先のリポジトリ・サーバー。リポジトリ・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・サーバー」ペインで定義されます。</p>
ロケーションの選択	<p>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。</p> <p>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。</p> <p>1次 スナップショットのリストア元の1次サイト。</p> <p>2次 スナップショットのリストア元の2次サイト。</p> <p>クラウドまたはリポジトリ・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。</p>
日付セクター	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、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	<p>クラウド・サービスまたはリポジトリ・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。</p> <p>クラウド・サービスまたはリポジトリ・サーバーへコピーされたリストア・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</p>

オプション	説明
	に使用される vSnap サーバーは、バックアップとコピー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。

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。

オプションで、「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。SQL データベースの名前を変更する場合、ID のための命名規則が適用されます。詳しくは、<https://docs.microsoft.com/en-us/sql/relational-databases/databases/database-identifiers> を参照してください。

「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. 「**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。

7. 「**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。

スタンバイ・モード

「スタンバイ・モード (Standby mode)」オプションが選択されている場合、SQL データベースは読み取り専用状態のままになります。コミットされていないトランザクションは取り消され、取り消しファイルに保存されます。これはその後データベースをオンラインにする際に使用できます。スタンバイ・ファイルに保管されたトランザクションは、データベースをリカバリーする準備ができると適用できます。

注：スタンバイ・モードを使用してリストアされたデータベースの場所は、SQL Management Studio でデータベースを表示すると、元のデータベースの場所にあると報告される場合があります。この場所は実際には、実動モードのリストア用にユーザーが指定したディレクトリーであり、テスト・モードのリストアの場合には `C:\ProgramData\mnt\uuid_subdirectory` になります。

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。

8. 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。


9. 「**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。

10. 「**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

[487 ページの『バックアップ操作とリストア操作のスキプトの構成』](#)

事前スキプトと事後スキプトは、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キプトです。サポートされるスキプトには、Linux ベースのマシンの場合はシェル・スキプトが、また、Windows ベースのマシンの場合はバッチ・スキプトと PowerShell スキプトがあります。スキプトはローカル側で作成され、「スキプト」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

[461 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。

[463 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。

第 15 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、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、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、[228 ページの『ハイパーバイザー、データベース、およびファイル・システムの SLA ポリシーの作成』](#)の手順に従います。

制約事項：IBM Spectrum Protect Plus をバックアップするための 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。IBM Spectrum Protect Plus をバックアップするための 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、以下のようになります。

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。
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、[164 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、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。

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。

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・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。

カタログ・リストア・ジョブが開始されると、ジョブ・セッション ID (ID) が割り当てられます。初期段階では、リカバリー・ステップが内部データベース・リストアを開始するまで、ジョブ管理画面の IBM Spectrum Protect Plus UI でジョブをモニターすることが可能になります。ジョブがこの状態になると、IBM Spectrum Protect Plus は使用できなくなります。この段階では、ログ情報がロケーション / data/log/adminconsole/managedb-catalogrestore-time.log に書き込まれます。ここで、time はエポック時間です。このログに含まれているデータは、Mongo 構成とリカバリー・カタログのリストアに関連しています。プロセスが完了すると、virgo サービスが開始し、データが virgo ログに書き込まれます。ジョブが完了すると、IBM Spectrum Protect Plus ユーザー・インターフェースが再びアクセス可能になります。

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・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。

関連概念

479 ページの『ジョブ・タイプ』

ジョブは、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、インベントリ操作、およびレポート操作の実行に使用されます。

ジョブ・セッションを期限切れに設定

ジョブ・セッションを期限切れに設定して、バックアップの作成中に割り当てられたスナップショット保存設定をオーバーライドできます。


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コピー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。複製またはコピー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、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。
あるいは、「仮想マシン / データベース」タブで、「アプリケーション」または「ハイパーバイザー」のいずれかを選択し、名前を入力して目的のカatalog・エントリを検索します。名前は、アスタリスク(*)をワイルドカード文字として入力するか、またはパターン・マッチングに疑問符(?)を使用して検索できます。

検索機能の使用法について詳しくは、537 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. 「バックアップ・セッション」タブから検索を行う場合は、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・ジョブの開始日の範囲で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。

IBM Spectrum Protect Plus カタログからのリソース・メタデータの削除

インベントリー・ジョブを実行すると、リソースが IBM Spectrum Protect Plus カタログに追加されます。カタログ内のスペースを解放するには、リソースに関連付けられているリストア・ポイントからメタデータを期限切れにすることができます。



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、537 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

479 ページの『ジョブ・タイプ』

ジョブは、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、インベントリー操作、およびレポート操作の実行に使用されます。

第 16 章 ジョブと操作の管理

「ジョブと操作」ウィンドウでジョブを管理して、モニターすることができます。ジョブの実行前または実行後に実行するスクリプトを構成することもできます。

ジョブ・タイプ

ジョブは、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、インベントリー操作、およびレポート操作の実行に使用されます。

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、インベントリー、およびレポートの各ジョブは事前定義されているので、変更できません。ただし、メンテナンス、インベントリー、およびレポートのジョブのスケジュールは変更できます。

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。

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。

SLA ポリシーに関連付けられているすべてのリソースをバックアップするのではなく、ポリシーに関連付けられている単一のリソースまたは選択した複数のリソースのバックアップ・ジョブを実行することもできます。

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。

リストア・ジョブは、スケジュールまたはオンデマンドで実行されます。

スケジュールされたジョブの場合、ジョブ名は、ジョブを作成するユーザーによって定義されます。

オンデマンド・ジョブの場合、ジョブの実行時にジョブ名 `onDemandRestore` が自動的に生成されます。

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。

報告書

レポート・ジョブは、スケジュールされたレポートを実行します。ジョブ名は、レポート名の前に Report_ が付けられたものです。

レポート名は次の例のようになります。

Report_VM Backup History

関連概念

241 ページの『仮想化システムの保護』

IBM Spectrum Protect Plus で保護する仮想化システムを登録してから、システムに関連した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。

353 ページの『データベースの保護』

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。

関連タスク

228 ページの『ハイパーバイザー、データベース、およびファイル・システムの SLA ポリシーの作成』

カスタム・サービス・レベル・アグリーメント (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、およびコピーのポリシーを定義できます。

487 ページの『アドホック・バックアップ・ジョブの実行』

アドホック・バックアップ・ジョブを使用すると、SLA ポリシーに関連付けられている 1 つ以上のリソースを選択し、それらのリソースに対してオンデマンド・バックアップ操作を実行できます。

ジョブおよびジョブ・スケジュールの作成

ジョブおよびジョブ・スケジュールを作成する方法は、ジョブ・タイプに応じて異なります。

バックアップ・ジョブとリストア・ジョブのためのジョブおよびスケジュールを作成できます。次の表では、使用できるバックアップ・ジョブとリストア・ジョブについて説明し、ジョブおよびジョブ・スケジュールの作成またはオンデマンドでのジョブの実行に必要な手順へのリンクを示しています。

メンテナンス・ジョブはデフォルトで作成されます。インベントリー操作が実行されるとき、またはレポートがスケジュールされるときに、インベントリー・ジョブおよびレポート・ジョブが作成されます。

ジョブ・タイプ	説明	ジョブの作成方法
バックアップ	ジョブ定義を作成して、その定義に 1 つ以上の SLA ポリシーを割り当てることができます。ジョブ定義は、バックアップするリソースを定義して、SLA ポリシーは、バックアップ操作のスケジュール、ターゲット、およびその他のオプションを定義します。	<p>以下のセクションで、リソース・タイプ別のデータのバックアップ手順が記載されているトピックを参照してください。</p> <ul style="list-style-type: none">• 241 ページの『第 10 章 仮想化システムの保護』• 291 ページの『第 11 章 ファイル・システムの保護』• 309 ページの『第 12 章 コンテナの保護』• 347 ページの『第 13 章 クラウド・システム上のデータの保護』• 353 ページの『第 14 章 データベースの保護』 <p>例えば、VMware のバックアップに関するトピックは、245 ページの『VMware データのバックアップ』です。</p>

ジョブ・タイプ	説明	ジョブの作成方法
アドホック・バックアップ	選択された SLA ポリシーに対してジョブが実行されると、その SLA ポリシーに関連付けられているすべてのリソースがバックアップ操作に組み込まれます。選択した SLA ポリシーを使用して、選択したリソースのみをバックアップする場合は、バックアップ操作を即時に実行するアドホック・ジョブを実行できます。	487 ページの『アドホック・バックアップ・ジョブの実行』を参照してください。
リストア	少なくとも 1 回、バックアップ・ジョブを実行した後、リストア・ジョブを実行してデータをリストアすることができます。 スケジュールに従って実行されるか、オンデマンドで実行されるリストア・ジョブを作成できます。	以下のセクションで、リソース・タイプ別のデータのリストア手順が記載されているトピックを参照してください。 <ul style="list-style-type: none"> • 241 ページの『第 10 章 仮想化システムの保護』 • 291 ページの『第 11 章 ファイル・システムの保護』 • 309 ページの『第 12 章 コンテナの保護』 • 347 ページの『第 13 章 クラウド・システム上のデータの保護』 • 353 ページの『第 14 章 データベースの保護』 例えば、VMware のリストアに関するトピックは、256 ページの『VMware データのリストア』です。

関連概念

479 ページの『ジョブ・タイプ』

ジョブは、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、インベントリ操作、およびレポート操作の実行に使用されます。

関連タスク

228 ページの『ハイパーバイザー、データベース、およびファイル・システムの SLA ポリシーの作成』


カスタム・サービス・レベル・アグリーメント (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、およびコピーのポリシーを定義できます。

オンデマンドでのジョブの開始

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。

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. 実行したいジョブを選択し、「アクション」メニュー・アイコン  をクリックしてから、「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

ジョブのジョブ・ログを表示するには、「実行中のジョブ」タブでジョブを選択し、「ジョブ・ログ」をクリックします。ジョブのログをダウンロードするには、**Download.zip** をクリックします。

そのジョブと同時に実行されているジョブ、または同時に実行されたジョブをすべて表示するには、「**同時ジョブ**」をクリックします。

ジョブの表示

実行中のジョブの状況、そして正常に完了したジョブまたは失敗や警告で完了したジョブの全体的な状況に関する情報を表示します。

手順

ジョブを表示するには、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、「**ジョブと操作**」をクリックします。
2. 「**実行中のジョブ**」ページで、以下の例に示すように、現在実行中のジョブの状況を表示します。

The screenshot shows the 'Jobs and Operations' dashboard with the 'Running Jobs' tab selected. It displays a summary of running jobs: 7 Total Jobs, 0 Backup, 0 Inventory, 0 Maintenance, and 7 Restore. A CPU Usage bar shows 4% usage. Below the summary, there are three job cards for 'onDemandRestore' jobs. The first card shows a job with ID 'onDemandRestore_1590032799201' that is 'Resource active' and 'Databases Completed: 1/1'. The second card shows a job with ID 'onDemandRestore_1589411636416' that is 'Resource active' and 'Databases Completed: 1/1'. The third card shows a job with ID 'onDemandRestore_1589257013247' that is 'Resource active' and 'Databases Completed: 1/1'. On the right, there is a detailed view for the first job, showing its 'Type: Restore', 'Start Time: May 20, 2020 8:46:40 PM', and a table of job logs.



3. 完了したジョブを表示するには、「**ジョブ・ヒストリー**」をクリックします。

この画面のリボンには、ヒストリカル・ジョブの状況が表示されます。表示するジョブ・ヒストリーの期間を定義するには、フィルターを使用します。

The screenshot shows the 'Jobs and Operations' dashboard with the 'Job History' tab selected. It displays a summary of job history: 51.14% Success Rate, 2710 Total Jobs, 741 Failed, 583 Warning, and 1386 Successful. A 'Job history period' dropdown is set to 'Last 30 days'. Below the summary, there are three job cards for 'vmware_SLA1_1object_policy', 'vmware_SLA3_1object_policy', and 'sql_bigdb-cd2-dedup'. The first card shows a job with ID 'vmware_SLA1_1object_policy' that is 'Partial' and 'Total VMs: 2'. The second card shows a job with ID 'vmware_SLA3_1object_policy' that is 'Failed'. The third card shows a job with ID 'sql_bigdb-cd2-dedup' that is 'Failed'. On the right, there is a detailed view for the first job, showing its 'Type: Backup', 'Start Time: Jun 6, 2020 3:00:01 PM', and a table of job logs.

4. ご使用の環境内のアクティブ・リソースを表示するには、「**アクティブ・リソース**」をクリックします。

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。ハイパーバイザーの場合、表示されるフィールドは、リソース、タイプ、宛先、および前回の更新です。ターゲット・ソースが vDisk の場合は vDisk ラベル情報も表示されます。

- すべてのジョブのスケジュール全体を表示するには、「スケジュール」をクリックします。
「アクション」メニューを使用すると、ジョブを開始するか、スケジュールを停止するかを選択できます。また、スケジュール・アイコン  をクリックし、変更を保存することで、一部の反復ジョブとメンテナンス・ジョブのスケジュールを編集することも可能です。リストア・ジョブを編集するには、そのジョブの編集アイコン  をクリックします。
- オプション: ジョブ・ログ、および「ジョブと操作」ウィンドウに表示されている情報を反映する他のファイルをダウンロードするには、**Download.zip** をダウンロードします。

リソース・レベルでのバックアップ・ジョブ進行状況の表示

バックアップ・ジョブの個別リソースの状況を表示します。リソース・レベルでジョブを表示すると、バックアップ・パフォーマンスをリソースごとに判別できます。この機能が提供する情報は、バックアップ・パフォーマンスの最適化、また起こりうる問題の解決に役立ちます。

このタスクについて

この機能は、バックアップ・ジョブでのみ使用可能です。その他のジョブ・タイプでは、個別リソースの進行状況は表示されません。


手順

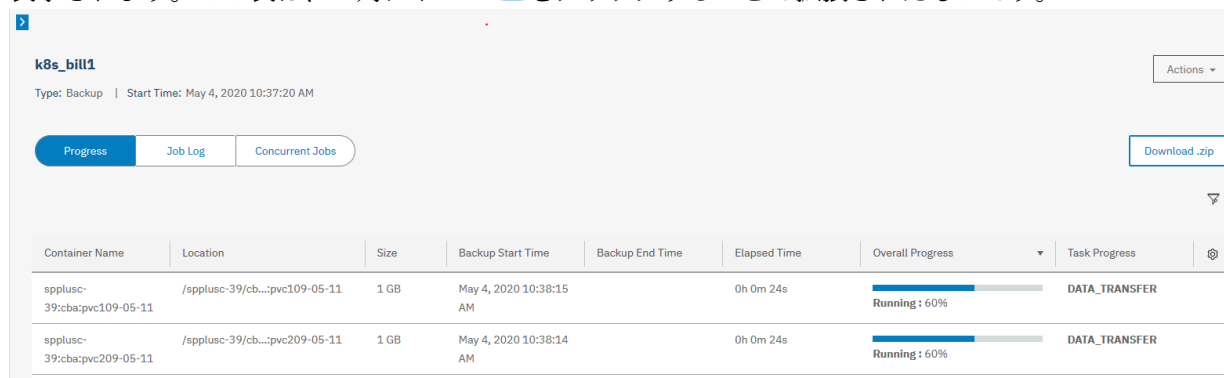
バックアップ・ジョブの個別リソースの進行状況を表示するには、以下のステップを実行します。

- ナビゲーション・ペインで、「ジョブと操作」をクリックします。
- 現在進行中のジョブを表示するには「実行中のジョブ」を、完了したジョブには「ジョブ・ヒストリー」をクリックします。
- 表示するリソースが含まれているジョブを選択して、「進行状況」をクリックします。

リソースごとの情報がテーブルに示されます。この情報には、「全体の進行状況」列に示される各リソースのバックアップ操作の進行状況などがあります。

該当するリソース・タイプの実行中場合、バックアップ操作で実行中のタスクも、「タスクの進行状況 (Task Progress)」列に表示されます。この列は、一部のリソース・タイプ (バックアップ操作に個々のタスクが含まれないハイパーバイザーなど) では含まれません。


以下の例は、Kubernetes バックアップ・ジョブの進行状況の情報を示しています。この例では、「全体の進行状況」列に示されているように、リソースの全体的なバックアップの進行状況は 60% です。現在実行中のバックアップ・タスク、つまり「data transfer (データ転送)」が「タスクの進行状況」列に表示されます。この表は、三角アイコン  をクリックすることで拡張されたものです。




Container Name	Location	Size	Backup Start Time	Backup End Time	Elapsed Time	Overall Progress	Task Progress
spplusc-39:cbaspvc109-05-11	/spplusc-39/cb...:pvc109-05-11	1 GB	May 4, 2020 10:38:15 AM		0h 0m 24s	Running : 60%	DATA_TRANSFER
spplusc-39:cbaspvc209-05-11	/spplusc-39/cb...:pvc209-05-11	1 GB	May 4, 2020 10:38:14 AM		0h 0m 24s	Running : 60%	DATA_TRANSFER

図 51. リソース・レベルでのジョブ情報の表示

- オプション: テーブルに示されている列をカスタマイズし、進行状況によって表示されるリソースをフィルターに掛けることができます。

列をカスタマイズするには、設定  アイコンをクリックして列を選択します デフォルトではすべての列が表示されます。

進行状況によってリソースをフィルターに掛ける場合、フィルター  アイコンをクリックして、希望する状況値を選択します。例えば、実行中のリソースのみを表示したい場合は、「実行」チェック・ボックスを選択し、その他のリソースをクリアします。

ジョブ・ログの表示

ジョブを実行するたびに、ジョブの状況、ジョブの開始時刻と終了時刻、およびジョブに関連付けられたメッセージなどの情報を表示するログが提供されます。

手順

ジョブ・ログを表示するには、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、「**ジョブと操作**」をクリックします。
2. 現在進行中のジョブを表示するには「**実行中のジョブ**」を、完了したジョブには「**ジョブ・ヒストリー**」をクリックします。
3. ジョブを選択して、「**ジョブ・ログ**」をクリックします。

選択したジョブのジョブ・ログが表示されます。

同時ジョブの表示

他のジョブと並行するジョブは、同時ジョブと呼ばれます。別のジョブと同時に実行されているジョブ、または同時に実行されたジョブを表示できます。

手順

別のジョブと同時に実行されているジョブ、または同時に実行されたジョブを表示するには、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、「**ジョブと操作**」をクリックします。
2. 現在進行中のジョブを表示するには「**実行中のジョブ**」を、完了したジョブには「**ジョブ・ヒストリー**」をクリックします。
3. ジョブを選択して、「**同時ジョブ**」をクリックします。

「**実行中のジョブ**」タブに表示されるジョブの場合、選択したジョブと同時に実行されているすべてのジョブのリストが表示されます。「**ジョブ・ヒストリー**」タブに表示されるジョブの場合、選択したジョブと同時に実行されていたすべてのジョブのリストが表示されます。


制約事項: 複数のバックアップ・ジョブが、同時に同じリソースをバックアップすることはできません。複数のジョブがリソース (複数の場合あり) を共有する場合、リソースを最初に処理するジョブが実行され、同じ期間に開始される他のジョブは失敗します。


ジョブの一時停止と再開

スケジュール済みのジョブは一時停止して再開することができます。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. 一時停止したいジョブを選択し、「**アクション**」メニュー・アイコン  をクリックしてから、「**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、 をクリックし、「スケジュールの保留解除」をクリックしてください。

ジョブとジョブ・スケジュールの編集

ジョブ・オプションとスケジュールは、ジョブ・タイプによって編集可能です。

このタスクについて

リストア・ジョブの場合は、「リストア」ウィザードを使用してジョブ・オプションを編集できます。



以下のジョブ・タイプではジョブ・スケジュールを編集することができます。

- リストア (反復ジョブ)
- インベントリ
- 報告書
- メンテナンス

手順

ジョブまたはジョブ・スケジュールを編集するには、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、「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. 編集アイコンまたはスケジュール・アイコンをクリックします。

オプション	説明
	この編集アイコンをクリックして「リストア」ウィザードを開き、ジョブのオプションを変更します。ウィザードの使用方法については、 241 ページの『第 10 章 仮想化システムの保護』 および 353 ページの『第 14 章 データベースの保護』 で該当するリソースのリストアに関するトピックの指示を参照してください。
	この編集アイコンをクリックして、ジョブ・スケジュールを変更します。

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

ジョブをキャンセルするには、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、「ジョブと操作」をクリックして、「実行中のジョブ」タブをクリックします。
2. 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。

ジョブの削除


「アイドル」状況のリストア・ジョブまたはレポート・ジョブを削除できます。

このタスクについて

この手順はリストア・ジョブとレポート・ジョブにのみ適用されます。バックアップ・ジョブを削除するには、そのジョブに関連付けられているサービス・レベル・アグリーメント (SLA) ポリシーを削除する必要があります。

手順

リストア・ジョブまたはレポート・ジョブを削除するには、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、「**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. ジョブに関連付けられている削除アイコン  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 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。

ヒント: 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 がない。

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。
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。

タスクの結果

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。部分的に完了した最後のバックアップ操作以降に適用されたオプションまたは除外事項の変更はすべて無視されます。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。

アドホック・バックアップ・ジョブの実行

アドホック・バックアップ・ジョブを使用すると、SLA ポリシーに関連付けられている 1 つ以上のリソースを選択し、それらのリソースに対してオンデマンド・バックアップ操作を実行できます。

このタスクについて



この機能は、即時のオンデマンド・バックアップ操作を実行する目的で、選択した SLA ポリシーとリソースをアドホック・ジョブに関連付けます。これにより、スケジュール済みジョブに関連付けられているリソースに対する SLA ポリシー割り当ては変更されません。

手順

アドホック・バックアップ・ジョブを実行するには、次のステップを完了します。

1. ナビゲーション・ペインで、「ジョブと操作」 > 「ジョブの作成」をクリックします。
2. 「アドホック・バックアップ (Ad hoc backup)」を選択して、バックアップ・ウィザードを開きます。

ヒント:

- 「保護の管理」 > 「ハイパーバイザー」または「保護の管理」 > 「アプリケーション」をクリックして、個別のハイパーバイザーやアプリケーションの管理ページからウィザードを開くことも可能です。
 - 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・ペインで「バックアップのプレビュー (Preview Backup)」をクリックします。
3. 「ソース・タイプ」 ページで、ジョブに組み込みたいリソースとして、ハイパーバイザーまたはアプリケーションをクリックします。
 4. 「SLA ポリシーの選択」 ページで、SLA ポリシーを選択し、「次へ」をクリックします。
 5. 「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) 使用可能なリソースを確認します
フィルター・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リソース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) ジョブに追加するリソースの横にあるプラス・アイコン  をクリックします。
リストからリソースを削除するには、そのリソース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。
 6. 「確認」 ページで、ジョブの設定を確認してから、「実行」をクリックし、ジョブを作成して実行します。

次のタスク

ジョブに関する状況やその他の情報を表示するには、ナビゲーション・ペインで「ジョブと操作」をクリックし、「実行中のジョブ」タブでそのジョブをクリックします。

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。	488 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、そのスクリプトが実行されるサーバーに追加できます。

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追加します。

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」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 17 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・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」タブをクリックします。
3. 「カテゴリによるフィルター (Filter by category)」ドロップダウン・メニューで「バックアップ・ストレージの使用状況」を選択します。
4. 目的のレポートの横にある「レポートの実行」() アイコンをクリックして、レポートを実行します。

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レポート

仮想マシンは、「ハイパーバイザー・タイプ」、「ハイパーバイザー」、および「VM タグ (VM tags)」の選択ボックスを使用して絞り込むことができます。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。

VM のバックアップ使用率レポートには、VM 名、ロケーション、ハイパーバイザー・タイプ、VM の保護に使用されている SLA ポリシー、および使用されているバックアップ・ストレージのロケーションが示されます。このバックアップ・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・サーバーの名前が示される場合があります。各 VM のバックアップ・サイズおよび各 VM で使用できるリカバリー・ポイントの数が表示されます。最後に、保護されている仮想マシンの総数がレポートの下部に表示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

vSnap ストレージの使用状況レポート

レポート・オプションを使用して、「vSnap ストレージ」選択ボックスで、表示する特定の vSnap サーバーをフィルターに掛けます。レプリカ宛先ボリュームをフィルターに掛けて除外するには、「レプリカ宛先ボリュームの除外」を選択します。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 サーバーの圧縮および重複排除率が表示されます。

vSnap ストレージの使用状況レポートには、vSnap サーバー、サイト、状況、合計スペース、フリー・スペース、および使用スペースが表示されます。展開すると、該当する場合には、重複排除率と圧縮率が vSnap サーバーごとに表示されます。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。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

注：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

498 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。

491 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」タブをクリックします。
3. 「カテゴリによるフィルター (Filter by category)」ドロップダウン・メニューで「保護」を選択します。
4. 目的のレポートの横にある「レポートの実行」() アイコンをクリックして、レポートを実行します。

使用可能なレポートは次のとおりです。

コンテナ永続ボリューム・バックアップ・ヒストリー・レポート

コンテナ永続ボリューム・バックアップ・ヒストリー・レポートには、永続コンテナ・ボリュームのバックアップ・ジョブのヒストリーが表示されます。レポート・オプションを使用して、Persistent Volume Claim (PVC) タイプでフィルターに掛けたり、表示する特定の「PVC」を選択します。このレポートは、「状況」フィールドの失敗したジョブまたは成功したジョブや、「SLA ポリシー」フィールドの 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。「バックアップ・ヒストリーの経過日数」フィールドに整数値を設定して、指定した日数のバックアップ・ヒストリーを表示します。

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で「状況」をフィルターに掛けます。このレポートは、「SLA ポリシー」フィールドを使用して特定の 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。「バックアップ・ヒストリーの経過日数」フィールドに整数値を指定して、結果を絞り込むことができます。

レポートの「詳細の表示」で、関連したジョブを展開して、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。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

データベース SLA ポリシー RPO 適合レポート

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、「以下に該当するデータベースを表示」フィールドの定義されている RPO に準拠しているデータベースまたは準拠していないデータベースや、複製、オブジェクト・ストレージ・コピー、またはアーカイブを使用して vSnap にバックアップされたデータなどの「保護タイプ」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。クイック・ビューには、vSnap へのバックアップのうち、準拠しているものと準拠していないものの数の円グラフが表示されます。要約表示には、SLA ポリシー、SLA スケジュール、vSnap へのバックアップのうち、準拠している数と準拠していない数、準拠している複製と準拠していない複製が表示されます。また、データベース名、アプリケーション・サーバー、アプリケーション・タイプ、最後の正常保護時刻、非準拠の理由など、保護タイプについて準拠していないデータベースも表示されます。

ファイル・システム・バックアップ・ヒストリー・レポート

ファイル・システム・バックアップ・ヒストリー・レポートを実行して、特定のファイル・システムの保護ヒストリーを検討します。レポートを実行するには、「サーバー」オプションで少なくとも 1 つのサーバーを指定して、「ファイル・システム」オプションで 1 つのファイル・システムを選択する必要があります。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で「状況」をフィルターに掛けます。このレポートは、「SLA ポリシー」フィールドを使用して特定の 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。4 つのオプションのすべてのデフォルト設定は「すべて」です。「バックアップ・ヒストリーの経過日数」フィールドに整数値を指定して、結果を絞り込むことができます。

「レポート・プロパティ」には、作成日とレポートの生成に使用されたアカウントが表示されます。レポートの生成時に使用されたレポート・フィルターも表示されます。レポートの「詳細の表示」には、ファイル・システムがサーバーおよび実行の総数とともにリストされます。SLA ポリシー、ジョブの時刻、およびジョブの状況が表示されます。関連したジョブの情報を展開して、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できます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

ファイル・システム SLA ポリシー RPO 適合レポート

レポート・オプションを使用して、表示する特定の「サーバー」を選択します。このレポートは、複製、オブジェクト・ストレージ・コピー、またはアーカイブを使用して vSnap にバックアップされたデータなどの「保護タイプ」でさらにフィルターに掛けることができます。これらの 2 つのフィルターのデフォルト設定は「すべて」です。定義されている RPO に準拠しているファイル・システムまたは準拠していないファイル・システムは、「以下に該当するファイル・システムを表示」フィールドでさらにフィルターに掛けることができます。

ファイル・システム 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ファイル・システムを表示します。「レポート・プロパティ」には、作成日とレポートの生成に使用されたアカウントが表示されます。レポートの生成時に使用されたレポート・フィルターも表示されます。クイック・ビューには、vSnap へのバックアップのうち、準拠しているものと準拠していないものの数の円グラフが表示されます。要約表示には、SLA ポリシー、SLA スケジュール、vSnap へのバックアップの数、複製を使用したジョブが表示されます。非準拠フィルターが選択されている場合、準拠していないファイル・システムの SLA ポリシーのジョブが表示されます。表示される情報は、vSnap へのバックアップ、複製、オブジェクト・ストレージ・コピー、およびアーカイブを使用した非準拠 SLA ジョブです。準拠していないファイル・システムの SLA ポリシーのジョブの場合、SLA ポリシーと SLA スケジュールが、各ファイル・システム、サーバー、最後の正常保護時刻、および非準拠の理由とともにリストされます。

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」、および「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。データベース・タイプごとに「詳細の表示」が表示され、データベース名、アプリケーション・サーバー、およびホスティング VM などの詳細情報が表示されます。「詳細の表示」では、無保護のデータベースに関する情報が「詳細の表示」の「無保護のデータベース」セクションに表示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

保護されたファイル・システムと無保護のファイル・システム・レポート

保護されたファイル・システムと無保護のファイル・システム・レポートを実行して、ファイル・システムの保護状況を表示します。このレポートには、バックアップ・ジョブの開始前に IBM Spectrum Protect Plus インベントリに追加された、保護されたファイル・システムと無保護のファイル・システム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「サーバー」、「オペレーティング・システム・タイプ (Operating System Type)」、および「ファイル・システム・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ファイル・システムを除外するには、「ハイパーバイザー・バックアップの一環として保護されたファイル・システムを表示しない (Hide File Systems protected as part of Hypervisor Backup)」を選択します。レポートで無保護のファイル・システムを除外するには、「無保護のファイル・システムを表示しない (Hide Unprotected File Systems)」を選択します。

「レポート・プロパティ」には、作成日とレポートの生成に使用されたアカウントが表示されます。レポートの生成時に使用されたレポート・フィルターも表示されます。要約表示には、登録されているファイル・システムの保護状況が表示されます。2つの詳細ビューが表示されます。1つは、保護されたファイル・システムに関するもので、もう1つは無保護のファイル・システムに関するものです。情報はファイル・システム、パス、ファイル・システム・タイプ、OS タイプ、およびサーバーごとに編成され、保護されたファイル・システムと無保護のファイル・システムの総数が表示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

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/アカウント」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、「オブジェクト・ストレージ・コピー・バックアップを使用した VM のみを表示 (Show only the VMs with Object Storage Copy Backups)」を選択します。「タグ」を使用して、レポートをフィルターに掛けることもできます。

「保護された VM」には、保護されている VM の総数、VM 名、ハイパーバイザー/アカウント、ハイパーバイザーのタイプ、ロケーション、および管理対象容量など、保護された仮想マシンの概要が表示されます。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。「無保護 VM」には、保護されていない仮想マシンに関する同じ情報が表示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

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履歴を検討します。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で「状況」をフィルターに掛けます。このレポートは、「SLA ポリシー」フィールドを使用して特定の 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。「バックアップ・ヒストリーの経過日数」フィールドに整数を指定して結果を絞り込んだり、「タグ」を使用してレポートをフィルターに掛けたりすることもできます。

「詳細の表示」では、VM、アカウント、実行の総数の下に SLA ポリシーがリストされます。各実行に関する情報を展開して、バックアップ・データのサイズをリストすることができます。保護時刻、状況、使用されたバックアップ・ストレージも表示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

VM SLA ポリシー RPO 適合レポート

レポート・オプションを使用して、「タイプ」、「ハイパーバイザー/アカウント」、複製、オブジェクト・ストレージ・コピー、アーカイブ、スナップショットを使用して vSnap にバックアップされたデータなどの「保護タイプ」でフィルターに掛けたり、「以下に該当する VM を表示」フィールドを使用して、定義されている RPO に準拠している仮想マシンまたは準拠していない仮想マシンを表示したりします。「タグ」のフィルターもあります。

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。クイック・ビューには、vSnap へのバックアップのうち、準拠しているものと準拠していないものの数の円グラフが表示されます。準拠しているスナップショットと準拠していないスナップショットの円グラフも表示されます。要約表示には、使用された SLA ポリシー、SLA スケジュール、vSnap へのバックアップのうち、準拠しているものと準拠していないものの比率、準拠しているスナップショットと準拠していないスナップショットの比率が表示されます。保護タイプごとに、準拠していない VM のビューも表示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

関連概念

491 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」タブをクリックします。
3. 「カテゴリーによるフィルター (Filter by category)」ドロップダウン・メニューで「システム」を選択します。
4. 目的のレポートの横にある「レポートの実行」() アイコンをクリックして、レポートを実行します。

使用可能なレポートは次のとおりです。

構成レポート

オプションの「構成タイプ」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。構成レポートには、アプリケーション・サーバー、仮想化システム、ディスク用、オブジェクト・ストレージ用、およびリポジトリ・サーバー用のバックアップ・ストレージ、VADP プロキシ、LDAP サーバー、および SMTP サーバーの構成が表示されます。このレポートには、リソースの名前、リソース・タイプ (OS またはアプリケーション)、プロバイダー、関連したサイト、SSL 接続状況が表示されます。構成レポートには、各コンポーネントのすべてのオプションが表示されるわけではありません。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

ジョブ・レポート

レポート・オプションを使用して、「ジョブ・タイプ」選択ボックスを選択することでジョブ・タイプをフィルターに掛け、「正常実行以降の日数」選択ボックスに指定する一定の期間に正常に実行されたジョブを表示します。クイック・ビューには、完了したジョブ、失敗したジョブ、およびその他のジョブの数を示す円グラフが表示されます。少なくとも 1 回実行されたジョブの要約表示には、ジョブのタイプ、そのタイプに関連付けられているジョブの数、実行回数、完了したジョブ、失敗したジョブ、およびその他のジョブの数が表示されます。少なくとも 1 回実行されたジョブの「詳細の表示」には、ジョブ、タイプ、実行の回数、完了したジョブ、失敗したジョブ、およびその他のジョブの数、最後の正常実行、および成功率が表示されます。いずれの場合も、その他のジョブとは、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のことです。「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、ジョブ ID、平均実行時間、最終実行時間の状況、最終実行時刻、ジョブがスケジュールされている場合の次にスケジュールされている実行時間、および保護されているリソースなどのジョブの詳細を表示します。レポートの最後には、実行されたことがないジョブの詳細が表示されます。

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。

Office 365 保護

「**Office 365 保護 (Office 365 Protection)**」フィールドには、Office 365 アプリケーションのバックアップ・ジョブによって保護されているユーザーが表示されます。「**フロントエンド容量**」フィールドには、保護されているユーザーの合計使用済みサイズが表示されます。

コンテナ永続ボリューム保護

「**コンテナ永続ボリューム保護 (Container Persistent Volume Protection)**」フィールドには、保護されているコンテナ永続ボリュームが表示されます。「**フロントエンド容量**」フィールドには、これらの保護されているコンテナ永続ボリュームの使用済み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


491 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 環境レポートの実行

IBM Spectrum Protect Plus で仮想マシン (VM) 環境のレポートを実行できます。レポートは、各ハイパーバイザー上の空きスペース量、論理装置番号 (LUN) のストレージ使用量、およびすべての VM の状況をモニターするのに役立ちます。

手順

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**」タブをクリックします。
3. 「**カテゴリによるフィルター (Filter by category)**」ドロップダウン・メニューで「**VM 環境**」を選択します。
4. 目的のレポートの横にある「**レポートの実行**」() アイコンをクリックして、レポートを実行します。
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

VM 環境内のデータ・ストアのストレージ使用率を確認するには、これを選択します。このレポートが提供する情報は、「**ハイパーバイザー・タイプ**」および「**ハイパーバイザー**」を使用してフィルタリングすることができます。「**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するデータ・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。

クイック・ビューには、空きスペースと使用スペースのストレージ使用率を示す円グラフが表示されます。要約表示には、ハイパーバイザー、データ・ストア・カウント、容量、および空きスペースが表示されます。詳細の表示は、データ・ストアを示し、VMが登録されていない孤立データ・ストアを表示します。また、関連付けられているハイパーバイザー、ハイパーバイザー・タイプ、データ・ストア・タイプ、容量、空きスペース、および使用済みパーセンテージも表示されます。3つのすべての表示には、データ・ストアの合計数、合計容量、および合計空きスペースが含まれています。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

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・タイプのフィルターには、「ハイパーバイザー・タイプ」と「ハイパーバイザー」が含まれます。「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。

レポートの要約表示には、ハイパーバイザー、ハイパーバイザーに関連付けられている LUN の数、および容量が表示されます。詳細の表示には、LUN ごとの LUN 名、LUN ID、ストレージ・ベンダー、ハイパーバイザー、データ・ストアまたはボリューム、容量、トランスポート・タイプ、およびロー・デバイス・マッピングが表示されます。どちらの表示にも、LUN 合計数と合計容量が表示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

VM スナップショット・スプロール・レポート

このスナップショット・スプロール・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。フィルターに使用できるレポート・オプションは、「ハイパーバイザー・タイプ」、「ハイパーバイザー」、および「タグ」です。「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。

このレポートには、スナップショット名とスナップショット作成時刻を表示する詳細の表示が含まれています。各スナップショットは、関連付けられている VM、ハイパーバイザー、およびハイパーバイザー・タイプの下に表示されます。VM およびスナップショットの合計数が、表示の終わりに示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

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。フィルターに使用できるレポート・オプションは、「ハイパーバイザー・タイプ」、「ハイパーバイザー」、「前回の電源オフ以降の日数」、「前回の中断状態以降の日数」、「前回の電源オン以降の日数」、および「タグ」です。

このレポートには、仮想マシンの電源状態 (電源オフの VM、電源オンの VM、テンプレート、および中断状態の VM) に基づいてストレージ使用率を表示する円グラフのクイック・ビューが含まれています。電源状態ごとの詳細の表示もあります。「詳細の表示 - 電源オフの VM」には、VM 名、電源がオフになった日付と日数、関連付けられているハイパーバイザー、ハイパーバイザーのタイプ、プロビジョンされたスペース、およびデータ・ストアまたはボリュームが表示されます。電源オフされた VM の合計数は、この表示の下部に、プロビジョンされたスペースの合計とともに表示されます。「詳細の表示 - 中断状態の VM」には、VM 名、VM が中断された日付と日数、関連付けられているハイパーバイザー、ハイパーバイザーのタイプ、プロビジョンされたスペース、およびデータ・ストアまたはボリュームが表示されます。中断状態の VM の合計数とプロビジョンされたスペースの合計は、表示の下部に示されます。「詳細の表示 - テンプレート」には、テンプレート名、関連付けられているハイパーバイザー、ハイパーバイザー・タイプ、プロビジョンされたスペース、およびデータ・ストアまたはボリュームが表示されます。合計テンプレート数とプロビジョンされたスペースの合計は、表示の下部に示されます。「詳細の表示 - 電源オンの VM」には、VM 名、VM の電源がオンになった日付と日数、関連付けられているハイパーバイザー、ハイパーバイザー・タイプ、プロビジョンされたスペース、およびデータ・ストアまたはボリュームが含まれています。表示の終わりには、電源オンの VM の合計数とプロビジョンされたスペースの合計が示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

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」でフィルタリングし、表示する「ハイパーバイザー」を選択します。

このレポートには、VM 名とプロビジョンされたスペースを表示する詳細の表示が含まれています。各 VM は、関連付けられているデータ・ストアまたはボリューム、ハイパーバイザー、およびハイパーバイザー・タイプの下に表示されます。データ・ストア/ボリュームおよび VM の合計数が、表示の終わりに示されます。「検索」ボックスを使用して、レポート結果をさらにフィルタリングすることができます。

関連概念

491 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。

始める前に

レポートを実行するユーザーに割り当てられているカスタム役割には、レポートを表示できるように適切な許可を設定する必要があります。役割、許可タイプ、および許可については、507 ページの『役割の管理』を参照してください。

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」タブをクリックします。
3. 目的のレポートの横にある「レポートの実行」()アイコンをクリックして、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、「レポートの実行」ウィンドウ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

491 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. 「レポート」 タブをクリックします。
3. 目的のレポートの横にある「カスタム・レポートの作成」 (+) アイコンをクリックして、カスタマイズします。
4. 「カスタム・レポートの作成」 ウィンドウで、「パラメーター」 タブを選択します。「名前」フィールドにレポートの名前を入力し、「説明」フィールドにカスタム・レポートの説明を入力します。選択したレポートに関連する、カスタマイズされたパラメーターを設定します。

注: レポート名には英数字と記号 \$-_.+!*() を含めることができます。レポート名にスペースを指定することはできません。

5. オプションで、「スケジュール」 タブの「スケジュールの定義」ボックスにチェック・マークを付けます。スケジュールを定義する場合は、以下の情報を指定します。

制約事項: 「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。

- 「頻度」には整数値を入力し、「分」、「時間」、「日」、「週」、「月」、または「年」を選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。
- 「開始時刻」には、日時を入力し、該当するタイム・ゾーンを選択します。表示されるデフォルトのタイム・ゾーンは、ブラウザの設定に基づいています。
- 「メール・アドレス」フィールドに、レポートのコピーを受け取る受信者の E メール・アドレスを入力します。少なくとも 1 人の受信者を追加する必要があります。さらに多くのアドレスが必要な場合は、「受信者の追加 (Add a recipient)」のプラス (+) アイコンをクリックします。

6. 「レポートを保存」 ボタンをクリックします。
7. カスタム・レポートを見つけるには、「カスタム・レポート」タブをクリックします。
8. レポートを実行するには、「カスタム・レポートの実行 (Run Custom Report)」 (▶) アイコンをクリックします。
9. オプションで、カスタム・レポートを更新するには、「カスタム・レポートの更新」 (✎) アイコンをクリックします。カスタム・レポートを削除するには、「レポートの削除」 (✕) アイコンをクリックします。

次のタスク

カスタム・レポートを実行し、レポート結果を確認します。

関連概念

491 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ルリング

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」タブをクリックします。
3. 目的のレポートの横にある「デフォルト・パラメーターを指定してレポートをスケジュールする (Schedule Report with default parameter)」 () アイコンをクリックし、レポートのスケジュールを定義します。
注: デフォルト以外のパラメーターを使用してレポートをスケジュールするには、カスタム・レポートを作成します。詳しくは、499 ページの『カスタム・レポートの作成』を参照してください。
4. 「デフォルト・パラメーターを指定してレポートをスケジュールする (Schedule Report with default parameter)」ウィンドウが表示されます。
制約事項: 「週」オプションの曜日は、IBM Spectrum Protect Plus 暫定修正 10.1.6 eFix2 以降をインストールした場合のみ使用できます。
 - ・「頻度」には整数値を入力し、「分」、「時間」、「日」、「週」、「月」、または「年」を選択します。「週」が選択されている場合、1 つ以上の曜日を選択できます。「開始時刻」は、選択した曜日に適用されます。
 - ・「開始時刻」には、日時を入力し、該当するタイム・ゾーンを選択します。表示されるデフォルトのタイム・ゾーンは、Web ブラウザーの設定に基づいています。
 - ・「メール・アドレス」フィールドに、レポートのコピーを受け取る受信者の E メール・アドレスを入力します。少なくとも 1 人の受信者を追加する必要があります。さらに多くのアドレスが必要な場合は、「受信者の追加 (Add a recipient)」のプラス () アイコンをクリックします。
5. 「スケジュール」ボタンをクリックします。

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

491 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

[512 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 18 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。

制約事項：役割ベースのアクセス制御 (RBAC) ユーザーを複数の VMware リソース・グループに割り当てないでください。ユーザーが「タグとカテゴリ」リソース・グループに割り当てられ、「ホストおよびクラスター」または「VM とテンプレート」のいずれかに割り当てられていると、「ホストおよびクラスター」ビューまたは「VM とテンプレート」ビューにデータが表示されなくなります。操作の実行時に、「タグとカテゴリ」がビューとして選択されている場合、その情報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 IBM Spectrum Protect Plus 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	<p>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。</p> <p>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。</p>
テンプレートから	<p>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。</p> <p>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。</p> <p>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、505 ページの『リソース・タイプ』を参照してください。</p>

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。	509 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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。
コンテナ	Kubernetes	コンテナ・リソースへのアクセス権を付与する場合に使用します。
ファイル・システム	Windows	ファイル・システム・リソース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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> VMware Hyper-V Amazon EC2 	仮想化システム・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。

リソース・タイプ	サブタイプ	説明
報告書	<ul style="list-style-type: none"> 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 インターフェイ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。
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。

リソース・タイプ	サブタイプ	説明
システム 構成	VADP プロキシ	VADP プロキシ・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 IBM Spectrum Protect Plus 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。


- 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。
- 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。
- 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。
- 「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。

- 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。
- 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。
- 「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」の役割の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作成、表示、および実行する。
- 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。

OC_MONITOR_ROLE

IBM Spectrum Protect Operations Center によって OC_MONITOR ユーザーが作成されると、OC_MONITOR_ROLE が作成されます。この役割およびユーザーは、Operations Center が IBM Spectrum Protect Plus 環境に接続するために必要です。OC_MONITOR_ROLE は、OC_MONITOR ユーザーのみが使用して、Operations Center を IBM Spectrum Protect Plus に接続するために必要な許可を提供します。この役割は編集しないでください。

リストアのみ

「リストアのみ」の役割の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」の役割のユーザーは、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、SUPERUSER 役割を割り当てられている 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。

VM 管理者

「VM 管理者」の役割の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	<p>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。</p> <p>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。</p> <p>使用可能な許可とその使用法を確認するには、509 ページの『許可タイプ』を参照してください。</p>

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。

名前	許可	説明
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。
オブジェクト・ストレージ	登録、表示、編集、登録取り消し	コピー操作のバックアップ・ストレージとして定義されるオブジェクト・ストレージとの対話に使用します。
クラウド	登録、表示、編集、登録取り消し	コピー操作のバックアップ・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」ページから使用できます。
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。
ジョブ	作成、表示、編集、実行、削除	インベントリ・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	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。

名前	許可	説明
スクリプト・サーバー	登録、表示、編集、登録取り消し	事前スクリプトと事後スクリプトが実行されるサーバー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	ユーザーと対話して、リソース・グループを役割に関連付け、IBM Spectrum Protect Plus ユーザー・インターフェースへのアクセスを提供するために使用します。

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。504 ページの『リソース・グループの作成』および 509 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 では、Lightweight Directory Access Protocol (LDAP) サーバーを使用してユーザーを管理できます。LDAP ユーザー・アカウントを作成すると、そのユーザー・アカウントをユーザー・グループに追加できます。

始める前に

以下のタスクを実行してください。

- LDAP プロバイダーを IBM Spectrum Protect Plus に登録していることを確認してください。LDAP プロバイダーを登録するには、201 ページの『LDAP サーバーの追加』の手順に従います。
- カスタムの役割とリソース・グループを使用する場合、その役割やグループが使用可能であることを確認してください。役割とグループの作成手順については、509 ページの『役割の作成』と 504 ページの『リソース・グループの作成』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**」 > 「**LDAP グループ**」をクリックします。
4. 「**LDAP グループの選択**」セクションの「**グループ名**」フィールドで、以下のいずれかのアクションを実行して LDAP グループを指定します。
 - LDAP グループ名を入力します。
 - 部分テキスト、単一のワイルドカード文字としてのアスタリスク (*)、またはパターン・マッチングのための疑問符 (?) を入力することで LDAP グループ名を検索します。すべての LDAP グループを表示するには、「**すべて表示**」ボタンをクリックします。
 - オプションで、「**グループ RDN**」フィールドに入力して相対識別名 (RDN) を設定することもできます。
5. LDAP グループは「**LDAP グループ**」テーブルに表示されます。LDAP グループを選択します。
6. 「**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。
7. 「**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。
8. 「**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。
9. 「**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。オプションで、使用可能な役割、アクセス権、およびリソース・グループを表示するには、ユーザー表でユーザーを選択します。

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**」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**」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 19 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 をアップグレードする場合は、メンテナンス・ジョブを実行して、既存の .slmtag ファイルを更新する必要があります。

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

[479 ページの『ジョブ・タイプ』](#)

ジョブは、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、インベントリー操作、およびレポート操作の実行に使用されます。

関連タスク

[481 ページの『オンデマンドでのジョブの開始』](#)

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 20 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 567387](#)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。

テープまたはクラウド・ストレージにデータを階層化するにはどうすればよいですか？

IBM Spectrum Protect Plus からテープ・ストレージにデータを階層化することはできません。データは IBM Spectrum Protect Plus からクラウド・ストレージに階層化できますが、データの迅速な再呼び出しをサポートするクラウド・ストレージ・クラスにのみ階層化が可能です。IBM Spectrum Protect Plus から IBM Spectrum Protect サーバーにデータをテープにコピーする場合、IBM Spectrum Protect の階層化機能を使用することはお勧めしません。テープにデータをアーカイブする場合は、コールド・キャッシュ・ストレージ・プールを使用する必要があります。

テープおよびクラウド・ストレージに関するガイドラインを確認してください。

- データを IBM Spectrum Protect Plus からテープに階層化することはできませんが、テープへの IBM Spectrum Protect Plus データのアーカイブまたはコピーは可能です。そのためには、『ステップ 1: テープにデータをコピーするためのテープ・ストレージ・プールおよびコールド・データ・キャッシュ・ストレージ・プールの作成』で説明されているように、コールド・データ・キャッシュ・ストレージ・プールを定義します。
- データは IBM Spectrum Protect Plus からクラウド・コンテナー・ストレージ・プールに階層化できますが、データの迅速な再呼び出しをサポートするクラウド・ストレージ・クラスにのみ階層化が可能です。Simple Storage Service (S3) プロトコルで Amazon Web Services (AWS) を使用してデータをクラウド・コンテナー・プールに移動する場合、Amazon S3 Glacier にデータを移動しないでください。クラウド・ストレージへのデータのコピーまたはアーカイブに関するシナリオと説明については、『データをコピーまたはアーカイブするための構成』を参照してください。クラウドへのデータの階層化の説明については、IBM Spectrum Protect 製品資料の [Tiering data to cloud or tape storage](#) を参照してください。

IBM Spectrum Protect Plus からテープにデータを階層化できません。IBM Spectrum Protect Plus データをテープに保管する場合は、データを IBM Spectrum Protect サーバーにコピーして、物理テープ・メディアまたは仮想テープ・ライブラリーに保管します。ストレージのセットアップのさまざまなシナリオおよび詳細については、[184 ページの『IBM Spectrum Protect にデータをコピーまたはアーカイブするための構成』](#)および [177 ページの『クラウドにデータをコピーまたはアーカイブするための構成』](#)を参照してください。

テープにデータをアーカイブまたはコピーするためにコールド・キャッシュ・ストレージ・プールをセットアップする場合は、[186 ページの『ステップ 1: テープにデータをコピーするためのテープ・ストレージ・プールおよびコールド・データ・キャッシュ・ストレージ・プールの作成』](#)を参照してください。

Kubernetes Backup Support のトラブルシューティング

Kubernetes Backup Support の問題のトラブルシューティングを行うために、デバッグ・ログ・ファイルを収集して、トレース・ログを表示することができます。問題を診断するための手順に従うこともできます。

トラブルシューティング用の Kubernetes Backup Support ログ・ファイルの収集

Kubernetes 環境でデバッグ・ログ・ファイルを生成して、Kubernetes Backup Support のデプロイメントおよび IBM Spectrum Protect Plus サーバー上の Kubernetes Backup Support 操作のトラブルシューティングを行うことができます。

このタスクについて

すべてのログは、ローカル・システム上の /tmp ディレクトリーで収集され、tar.gz アーカイブ・ファイルにパッケージされます。通常、このアーカイブ・ファイルの名前は baas_debug_logs_timestamp.tar.gz です。

手順

以下のいずれかの方法を使用して、トラブルシューティング用のログを収集します。

- デバッグの目的で Kubernetes ログのみを収集するには、次のコマンドを発行します。

```
./baas_install.sh -l
```

このコマンドは、baas_config.cfg 内のパラメーターで指定される Kubernetes Backup Support デプロイメントのデバッグ・ログを収集します。Kubernetes クラスター内の Kubernetes Backup Support コンポーネントの現在の状態情報およびログが収集されます。これらのログは、Kubernetes 基本ロギング・アーキテクチャーに基づいて構成されます。詳しくは、[Basic logging in Kubernetes](#) を参照してください。

- Kubernetes Backup Support デプロイメントおよび IBM Spectrum Protect Plus サーバーのデバッグ・ログを含むログ・パッケージを収集するには、次のコマンドを発行します。

```
./baas_install.sh -l -x
```

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。

- 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。
- 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。

関連タスク

[521 ページの『ログ・ファイルのトレース・レベルの設定』](#)

ローカル・ログ・ファイルのトレース・レベルを設定すると、Kubernetes Backup Support で発生する可能性がある問題のトラブルシューティングに役立ちます。

関連資料

[523 ページの『トラブルシューティングのクイック・リファレンス』](#)

基本的な Kubernetes Backup Support の問題の解決策が提供されています。

527 ページの『Kubernetes Backup Support 操作のトラブルシューティング』

Kubernetes Backup Support の問題を診断して解決する上で役立つトラブルシューティング手順を使用できます。

ログ・ファイルのトレース・レベルの設定

ローカル・ログ・ファイルのトレース・レベルを設定すると、Kubernetes Backup Support で発生する可能性がある問題のトラブルシューティングに役立ちます。

このタスクについて

トレース・レベルを設定すると、Kubernetes Backup Support トランザクション・マネージャー、コントローラー、およびスケジューラー・コンポーネントの問題をトラブルシューティングすることができます。設定したトレース・レベルは、Kubernetes Backup Support エージェントのログ・レベル、および IBM Spectrum Protect Plus ジョブ・ログおよび `command.log` ファイル内のログ・レベルにも適用されます。

データ・ムーバー・コンポーネントは、この設定の影響を受けません。

トレース・レベルを設定するには、`baas_config.cfg` 構成ファイルを更新してから、Kubernetes Backup Support のデプロイメントを更新する必要があります。

ヒント: デフォルトのトレース・レベルは `INFO` です。トラブルシューティングが必要な問題が発生している場合は、トレース・レベルを `DEBUG` に設定してください。

手順

トレース・レベルを設定するには、Kubernetes コマンド・ラインで以下のステップを実行します。

1. インストール・ノードとして使用されている Kubernetes クラスターのマスター・ノードでオペレーティング・システムにログインします。
2. `SPP_V10.1.6_for_Containers.tar.gz` インストール・パッケージが解凍されたディレクトリーに移動します。
3. 次のコマンドを発行して、`installer` ディレクトリーに移動します。

```
cd installer
```

4. テキスト・エディターを使用して `baas_config.cfg` ファイルを編集し、**`PRODUCT_LOGLEVEL`** パラメーターの値を変更します。

以下のトレース・オプションが使用可能です。

DEBUG

トランザクション・マネージャー、コントローラー、およびスケジューラーのログ・ファイル内のデバッグ・レベル・メッセージを表示します。

INFO

トランザクション・マネージャー、コントローラー、およびスケジューラーのログ・ファイル内のすべてのユーザー・メッセージ (情報メッセージ、警告メッセージ、およびエラー・メッセージを含む) を表示します。この値はデフォルトです。

WARNING

トランザクション・マネージャー、コントローラー、およびスケジューラーのログ・ファイル内の警告メッセージとエラー・メッセージを表示します。

エラー

トランザクション・マネージャー、コントローラー、およびスケジューラーのログ・ファイル内のエラー・メッセージのみを表示します。

例えば、トレース・レベルをデバッグ・モードに設定するには、**`PRODUCT_LOGLEVEL`** パラメーターを次のように設定します。

```
PRODUCT_LOGLEVEL="DEBUG"
```

5. 以下のコマンドを発行して、Kubernetes Backup Support デプロイメントを更新します。

```
./baas_install.sh -u
```

プロンプトが出されたら、**yes** と入力して続行します。

6. オプション: 更新の状況を確認するには、次のコマンドを発行します。

```
./baas_install.sh -s
```

ヒント: あるいは、**./helm status baas** コマンドを使用して、更新の状況を確認してください。

次のタスク

トラブルシューティング用に Kubernetes Backup Support ログ・ファイルを収集するか、Kibana などの可視化ツールを使用して、トランザクション・マネージャー、コントローラー、およびスケジューラーのログ・ファイル内のデータを表示および照会できます。手順については、以下を参照してください。

- [520 ページの『トラブルシューティング用の Kubernetes Backup Support ログ・ファイルの収集』](#)
- [522 ページの『Kubernetes Backup Support のトレース・ログの表示』](#)

Kubernetes Backup Support のトレース・ログの表示

オプションで、Elasticsearch、Fluentd、および Kibana (EFK) スタックを使用して、Kubernetes Backup Support によって作成されたトレース・ログを表示および分析することができます。

Elasticsearch は、分散型の全文検索エンジンです。Fluentd は、クラスター・ノードからログを収集し、Elasticsearch エンジンに送信するツールです。Kibana は、データの照会に使用される Web ユーザー・インターフェースおよび開発ツールを使用した Elasticsearch 用の可視化ツールです。

始める前に

以下のステップを実行してください。

1. EFK スタックを Kubernetes クラスターにデプロイします。
 - a. Elasticsearch 検索エンジンをデプロイします。手順については、[Installing Elasticsearch](#) を参照してください。
 - b. Fluentd ログ・コレクターを各クラスター・ノードにデプロイします。手順については、[Fluentd documentation](#) を参照してください。
 - c. Kibana 可視化ツールをデプロイします。手順については、[Kibana Guide](#) を参照してください。
2. Kibana に logstash 索引を追加して、EFK スタックのデプロイメントを完了します。
 - a. Web ブラウザーを開き、Kibana が実行されているコンピューターの URL を入力して、Kibana ユーザー・インターフェースにアクセスし、ポート番号を指定します。例えば、Web ブラウザーで次の URL のいずれかを指定します。

```
https://localhost:5601
```

または

```
http://your_domain.com:5601
```

ここで、*your_domain* は、コンピューターのドメイン名を指定します。

- b. データを探索するためのオプションを示すプロンプトが出されたら、「**独自に探索 (Explore on my own)**」を選択します。
- c. 「**検出 (Discover)**」 > 「**索引パターンの作成 (Create Index Pattern)**」をクリックして、logstash-* 索引パターンを作成します。

このタスクについて

EFK スタックを使用すると、すべてのコンテナ・コンポーネントからのログがマージされ、同じビューに表示されます。停止されたポッドのログは、Elasticsearch 永続データ・ストレージ内に保持されます。フィルターを適用すると、特定のエラーまたはメッセージを表示できます。また、時間フィルターを適用して、特定の時間枠に発生したイベントを表示することもできます。

エラー・メッセージとデバッグ・メッセージに加えて、以下の Kubernetes Backup Support コンポーネントのトレース・ログを表示できます。

- トランザクション・マネージャー
- コントローラー
- スケジューラー

手順

Kubernetes Backup Support のトランザクション・ログを表示するには、以下のステップを実行します。

1. Kibana ユーザー・インターフェースを開き、「**検出 (Discover)**」アイコンをクリックします。
2. logstash-* 索引をクリックします。
3. Kubernetes Backup Support のログを表示するには、以下のアクションを実行してフィルターを追加します。
 - a) 「**フィルターの追加**」をクリックし、次のフィルター値を指定します。
 - フィールド: `kubernetes.container_image`
 - オペレーター: `is`
 - 値: `baas-`
 - b) 検索の名前を入力し、「**保存**」をクリックします。
`baas-transaction-manager`、`baas-controller`、および `baas-scheduler` コンテナのトレース・ログが表示されます。
4. 追加フィルターを作成すると、Kubernetes Backup Support トレース・ログのより細分化されたビューを表示できます。

表 65. Kubernetes Backup Support トレース・ログを表示するためのフィルター

表示するデータのタイプ	フィルター 1	フィルター 2
トランザクション・マネージャーのログ	<code>kubernetes.container_image is baas-transaction-manager</code>	なし
コントローラーのログ	<code>kubernetes.container_image is baas-controller</code>	なし
スケジューラーのログ	<code>kubernetes.container_image is baas-scheduler</code>	なし
エラー・メッセージ	<code>kubernetes.container_image is baas-</code>	<code>log is ERROR</code>
デバッグ・メッセージ	<code>kubernetes.container_image is baas-</code>	<code>log is DEBUG</code>

トラブルシューティングのクイック・リファレンス

基本的な Kubernetes Backup Support の問題の解決策が提供されています。

Kubernetes Backup Support の操作で発生する可能性がある基本的な問題を解決するには、次の表の解決策を使用してください。それでも問題を解決できない場合は、さらに詳細なトラブルシューティング手順について、[527 ページの『Kubernetes Backup Support 操作のトラブルシューティング』](#)を参照してください。

表 66. 基本的な問題の解決策

問題	解決策
<p>Kubernetes Backup Support 要求が無効である。</p> <p>例えば、次のコマンドの実行時に、Backupstatus フィールドまたは Restorestatus フィールドが Invalid としてリストされます。</p> <pre>kubect1 describe baasreq request_name -n namespace</pre> <p>ここで、 request_name バックアップ要求またはリストア要求の名前。バックアップ要求の場合、値は、Persistent Volume Claim (PVC) の名前です。リストア要求の場合、値は固有のものでなければならず、PVC の名前と同じであってはなりません。</p> <p>namespace PVC が存在する名前空間。</p>	<p>YAML ファイルで次の要素を調べて、要求が正しく構造化されていることを確認します。</p> <ul style="list-style-type: none"> • タイプミスがないことを確認します。 • ステートメントで大/小文字が正しく使用されていることを確認します。Kubernetes は大文字小文字が区別されます。 <p>例えば、API のバージョン宣言が、apiversion ではなく、apiVersion としてリストされていることを確認します。</p> <ul style="list-style-type: none"> • リストア要求の場合: <ul style="list-style-type: none"> – リストア・ポイントのタイム・スタンプが restorepoint フィールドで正しく指定されていることを確認します。 – リストア・タイプが restoretype フィールドで正しく指定されていることを確認します。 <p>詳しくは、339 ページの『コマンド・ラインを使用したコンテナ・データのリストア』を参照してください。</p>
<p>スナップショットが失敗している。</p>	<p>以下の 1 つ以上のアクションを実行します。</p> <ul style="list-style-type: none"> • Ceph-CSI 構成を調べて、コンテナが正しく稼働していることを確認します。スナップショット・バックアップには CSI ソフトウェアが必要です。 • バックアップされている PVC にボリューム・スナップショット・クラスが定義されていることを確認します。 • シークレットが正しい名前空間 (PVC 用の名前空間) にあることを確認します。 • ConfigMap (baas-configmap) で構成が正しいことを確認します。 <p>詳しくは、528 ページの『スナップショット・バックアップ・ジョブの問題のトラブルシューティング』を参照してください。</p>
<p>データ・ムーバーが開始できない。</p>	<p>以下の 1 つ以上のアクションを実行します。</p> <ul style="list-style-type: none"> • Ceph RBD ボリュームがマウントされていることを確認します。データ・ムーバー・ポッドで kubect1 describe コマンドを実行して、Ceph RBD ボリュームのマウントが失敗しているかどうかを確認できます。 • kubect1 describe コマンドの出力で、イベントを調べて、読み取り/書き込みモードで別のポッドの一部として PVC を実行することによって、ボリュームが初期化されていることを確認します。 • kubect1 describe コマンドの出力で、認証障害イベントがないか確認します。認証エラーを解決するには、セキュアな Docker レジストリーを実行していることを確認します。プル・シークレットが PVC の名前空間にあることを確認します。手順については、Pull an Image from a Private Registry を参照してください。

表 66. 基本的な問題の解決策 (続き)

問題	解決策
vSnap サーバーから NFS ボリュームをマウントしているときに、アクセスが拒否されるか、接続が失敗する。	<p>以下の 1 つ以上のアクションを実行します。</p> <ul style="list-style-type: none"> データ・ムーバーのネットワーク・ポリシーを確認します。vSnap サーバー・アドレスが IBM Spectrum Protect Plus サーバー・アドレスと一致していることを確認します。 Kubernetes クラスターから IBM Spectrum Protect Plus vSnap サーバーへの直接接続が存在していることを確認します。プロキシによる接続はサポートされていません。
<p>スケジューラー、トランザクション・マネージャー、およびコントローラーのポッドは始動したが、各ポッドが再始動を続ける。トランザクション・マネージャー・ポッドに対する kubectl describe コマンドの出力で、イベントにより、活性プローブが失敗したことが示されている。</p>	<p>baas_config.cfg 構成ファイルで CLUSTER_API_SERVER_IP_ADDRESS パラメーターおよび CLUSTER_API_SERVER_PORT パラメーターの値が正しく指定されていることを確認します。</p> <p>baas_config.cfg ファイルでこれらの値を更新する場合は、次のコマンドを実行して構成を更新します。</p> <pre>./baas_install.sh -u</pre> <p>あるいは、Kubernetes Backup Support をアンインストールしてから再インストールし、以前のログ・ファイルを消去することができます。詳しくは、151 ページの『Kubernetes Backup Support のアンインストール』および 146 ページの『Kubernetes 環境での Kubernetes Backup Support イメージのインストールとデプロイメント』を参照してください。</p>
Kubernetes オブジェクトが終了中の状態のままである。	<p>次のコマンドを出します。</p> <pre>kubectl delete object object_name --force --grace-period=0</pre> <p>オブジェクトが引き続き終了中の状態になっている場合は、次のコマンドを実行します。</p> <pre>kubectl patch object -n namespace object_name -p '{"metadata":{"finalizers":null}}'</pre> <p>各構成要素について説明します。</p> <ul style="list-style-type: none"> object は、デプロイメント、ポッド、永続ボリューム (PV)、または PVC など、Kubernetes におけるオブジェクトのタイプです。 object_name は、オブジェクトの名前です。 namespace は、オブジェクトが入っている名前空間の名前です。

表 66. 基本的な問題の解決策 (続き)

問題	解決策
Kubernetes Backup Support が正常にアンインストールされなかった。	<p>以下のコマンドを実行して、環境を手動でクリーンアップします。</p> <pre> kubect1 delete namespace baas kubect1 delete clusterrole baas-controller kubect1 delete clusterrole baas-scheduler kubect1 delete clusterrole baas-spp-agent kubect1 delete clusterrole baas-transaction-manager kubect1 delete clusterrole aggregate-basreqs-admin-edit kubect1 delete clusterrolebinding baas-controller kubect1 delete clusterrolebinding baas-scheduler kubect1 delete clusterrolebinding baas-spp-agent kubect1 delete clusterrolebinding baas-transaction- manager kubect1 delete customresourcedefinition baasreqs.baas.io </pre>

表 66. 基本的な問題の解決策 (続き)

問題	解決策
コピー・バックアップ・ジョブをキャンセルすると、リソースが残されたままになる。	<p>以下のステップを実行して、残りのリソースをクリーンアップします。</p> <ol style="list-style-type: none"> 1. 以下のコマンドを実行して、データ・ムーバーのデプロイメントを削除します。 <pre>kubectl get deploy -n namespace kubectl delete deploy --all -n namespace</pre> 2. 以下のコマンドを実行して、サービス・アカウントを削除します。 <pre>kubectl get serviceaccount -n namespace kubectl delete serviceaccount --all -n namespace</pre> 3. 以下のコマンドを実行して、ネットワーク・ポリシーを削除します。 <pre>kubectl get networkpolicy -n namespace kubectl delete networkpolicy --all -n namespace</pre> 4. PVC および PV を削除します。 <p>コピー・バックアップ操作時に作成された PVC の命名規則は次のとおりです。</p> <pre>pvc-backup-pvcname-jobid-job_timestamp</pre> <p>以下のコマンドを発行します。</p> <pre>kubectl get pvc -n namespace grep pvc-backup kubectl get pvc -n namespace grep pvc-backup awk '{print \$1}' xargs kubectl delete pvc -n namespace</pre> <p>PV がまだ残っている場合は、以下のコマンドを実行します。</p> <pre>kubectl get pv grep pvc-backup kubectl get pv grep pvc-backup awk '{print \$1}' xargs kubectl delete pv</pre> 5. 必要に応じて、以下のコマンドを実行して、<code>volumesnapshot</code> オブジェクトおよび <code>volumesnapshotcontent</code> オブジェクトを削除します。 <pre>kubectl get volumesnapshot -n namespace kubectl get volumesnapshotcontent</pre>

関連タスク

520 ページの『[トラブルシューティング用の Kubernetes Backup Support ログ・ファイルの収集](#)』
Kubernetes 環境でデバッグ・ログ・ファイルを生成して、Kubernetes Backup Support のデプロイメント
および IBM Spectrum Protect Plus サーバー上の Kubernetes Backup Support 操作のトラブルシューティ
ングを行うことができます。

Kubernetes Backup Support 操作のトラブルシューティング

Kubernetes Backup Support の問題を診断して解決する上で役立つトラブルシューティング手順を使用で
きます。

以下の説明が示されています。

- [528 ページの『ログ・ファイルの表示』](#)
- [528 ページの『スナップショット・バックアップ・ジョブの問題のトラブルシューティング』](#)
- [529 ページの『コピー・バックアップ・ジョブの問題のトラブルシューティング』](#)
- [531 ページの『リストア・ジョブのトラブルシューティング』](#)

ログ・ファイルの表示

Kubernetes Backup Support の問題のトラブルシューティングを行うには、最初にログ・ファイル内の情報を表示します。Kubernetes Backup Support のトランザクション・マネージャー、コントローラー、およびスケジューラーのコンポーネントのログ・ファイルを使用できます。

複数のトランザクション・マネージャー・コンポーネントのログ・ファイルを表示できます。例えば、いずれかのトランザクション・マネージャー・コンポーネントのログ・ファイルを表示するには、次のコマンドを実行します。

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager -f
```

トランザクション・マネージャー・ワーカーのログ・ファイルを表示するには、次のコマンドを実行します。

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-transaction-manager/ {print $1;exit}') -n baas -c baas-transaction-manager-worker -f
```

コントローラー・コンポーネントのログ・ファイルを表示するには、次のコマンドを実行します。

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-controller/ {print $1;exit}') -n baas -f
```

スケジューラー・コンポーネントのログ・ファイルを表示するには、次のコマンドを実行します。

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f
```

ヒント: ログ・ファイルの表示を迅速化するために、**--since=duration** フラグを **kubectl logs** コマンドに追加して、相対的な期間よりも新しいログのみが返されるようにすることができます。期間は、秒 (Ns)、分 (Nm)、または時間 (Nh) の単位で指定できます。

例えば、3 時間前よりも新しいスケジューラー・コンポーネントのログ・ファイルを表示するには、次のコマンドを実行します。

```
kubectl logs -f $(kubectl get pods -n baas | awk '/baas-scheduler/ {print $1;exit}') -n baas -f --since=3h
```

スナップショット・バックアップ・ジョブの問題のトラブルシューティング

スナップショット・バックアップ操作が失敗した場合は、一連のアクションを実行して問題を診断することができます。

始める前に、トレース・レベルが **DEBUG** に設定されていることを確認してください。ログ・ファイルのトレース・レベルの設定の説明については、[521 ページの『ログ・ファイルのトレース・レベルの設定』](#)を参照してください。

スナップショット・バックアップの問題のトラブルシューティングを行うには、次のステップを実行します。

1. Kubernetes Backup Support ログ・ファイルが使用可能であることを確認してください。ログ・ファイルを表示する手順については、[528 ページの『ログ・ファイルの表示』](#)を参照してください。
2. IBM Spectrum Protect Plus がスナップショット要求を送信している場合は、**baas-transaction-manager** ポッドで **baas-transaction-manager** コンテナ・ログを確認します。ログ・ファイルで、次の例のようなテキストを探します。

```
/createvolumesnapshot/demo/demo-vol01 Begin
Received parameters {'metadata.name': 'k8s18-1004-2222-1727b1c0828',
```



```
'spec.snapshotClassName':  
'cirrus-csi-rbdplugin-snapclass', 'metadata.labels': {'storage.kubernetes.io/pvc': 'demo-  
vol01'}}
```

予期されるスナップショット名は、`metadata.name` キーの値です。

次に、次の例に示されている `createsnapshot` 呼び出しを探します。

```
2020-06-03 16:55:43,579[MainThread][kubernetes_api:createsnapshot Line 1056][INFO] -  
{'apiVersion':  
'snapshot.storage.k8s.io/v1alpha1', 'kind': 'VolumeSnapshot', 'metadata': {'annotations':  
{}, 'name':  
'k8s18-1004-2222-1727b1c0828', 'namespace': 'demo', 'labels': {'app.kubernetes.io/  
component': 'snapshot',  
'app.kubernetes.io/managed-by': 'baas', 'app.kubernetes.io/name': 'baas', 'app.kubernetes.io/  
version': '10.1.6',  
'storage.kubernetes.io/pvc': 'demo-vol01'}}}, 'spec': {'snapshotClassName': 'cirrus-csi-  
rbdplugin-snapclass',  
'source': {'kind': 'PersistentVolumeClaim', 'name': 'demo-vol01'}}}
```

3. ステップ 2 で例外が検出された場合は、`createsnapshot` 呼び出しで次の例外が見つかる可能性があります。

表 67. 考えられるスナップショット・バックアップ例外	
例外	アクション
スナップショットが存在しません。	次のコマンドを実行して、スナップショットが正しく作成されているかどうかを判別します。 <pre>kubectl describe volumesnapshots snapshotname -n namespace</pre>
スナップショットが適切に作成されていない可能性があります。	

4. 次のアクションを実行して、IBM Spectrum Protect Plus の問題のトラブルシューティングを行います。
- IBM Spectrum Protect Plus ユーザー・インターフェースで、インベントリー・ジョブがハングしていて、その他すべてのジョブが IBM Spectrum Protect Plus に記録されなくなっていないかどうかを確認します。
 - 実行中のジョブのリストまたはジョブ・ヒストリーで、ハングしたジョブを探します。以下の命名規則のジョブ名を探します。

```
k8s_sla_name
```

ここで、`sla_name` は、PVC に割り当てられている SLA ポリシーの名前です。

- ジョブ・ログを確認して、報告された問題があれば修正してください。IBM Spectrum Protect Plus のログ・ファイルの表示およびダウンロードについては、[324 ページの『ジョブ・ログの表示』](#)を参照してください。

ログ・ファイルのパッケージをダウンロードして、パッケージを展開します。ダウンロードしたパッケージの命名規則は次のとおりです。JobLog_job_name_job-timestamp.zip

ジョブについて詳しくは、`command.log` ファイルおよび

JobLog_k8s_sla_name_job_timestamp.csv ファイルを確認してください。

コピー・バックアップ・ジョブの問題のトラブルシューティング

コピー・バックアップが失敗した場合は、一連のアクションを実行して問題を診断することができます。

始める前に、ログ・ファイルのトレース・レベルが `DEBUG` に設定されていることを確認してください。ログ・ファイルのトレース・レベルの設定の説明については、[521 ページの『ログ・ファイルのトレース・レベルの設定』](#)を参照してください。

コピー・バックアップの問題のトラブルシューティングを行うには、次のステップを実行します。

- Kubernetes Backup Support ログ・ファイルが使用可能であることを確認してください。ログ・ファイルを表示する手順については、[528 ページの『ログ・ファイルの表示』](#)を参照してください。

2. IBM Spectrum Protect Plus エージェントが要求を IBM Spectrum Protect Plus スケジューラーに送信しているかどうかを確認します。スケジューラーのログ・ファイルを開き、次の例のようなテキストを探します。

```
Schedule data copy for snapshot: demo:pvc-backup-demo-vol01-1004-1591203980176
```

PVC のコピー・バックアップの命名規則は次のとおりです。

```
namespace:pvc-backup-pvcname-jobid-job_timestamp
```

次の例のように、データ・ムーバーをデプロイするためのトランザクション・マネージャーに対する呼び出しを探します。

```
url tmCopyBackupRequest: https://baas-transaction-manager:5000/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176"
```

スケジューラーがコピー・バックアップ要求を送信していない場合は、スケジューラーの問題を調査して解決してください。

3. スケジューラーがスナップショット要求を送信している場合は、baas-transaction-manager ポッドで baas-transaction-manager コンテナ・ログを確認します。トランザクション・マネージャーのログ・ファイルで、次の例のようなテキストのデータ・ムーバー作成呼び出しを探します。

```
/datamover/demo/pvc-backup-demo-vol01-1004-1591203980176 method=POST
2020-06-03 17:11:26,455[MainThread][main:createdatamover Line 1187][DEBUG] - Creating deployment backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:pvc-backup-demo-vol01-1004-1591203980176
```

baas-transaction-manager ポッドの baas-transaction-manager-worker ログで、要求の先頭に、タスク ID、COPYBACKUP 要求、デプロイメント名またはデータ・ムーバー名、およびボリューム名が示されます。

```
2020-06-03 17:11:26,589: DEBUG/MainProcess] TaskPool: Apply <function _fast_trace_task at 0x7ff1707ac268> (args:('main.backgroundprocess', '29606e23-b6e3-4965-8156-930b42c12a25', {'lang': 'py', 'task': 'main.backgroundprocess', 'id': '29606e23-b6e3-4965-8156-930b42c12a25', 'shadow': None, 'eta': None, 'expires': None, 'group': None, 'retries': 0, 'timelimit': [None, None], 'root_id': '29606e23-b6e3-4965-8156-930b42c12a25', 'parent_id': None, 'argsrepr': '(\n  'COPYBACKUP',\n  {'command': 'backup', 'namespace': 'demo', 'deploymentName': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176', 'volumename': 'pvc-backup-demo-vol01-1004-1591203980176', 'vSnapIPAddresses': ['9.11.62.84'], 'vSnapMountPath': '/vsnap/vpool1/fs489', 'kafkaAddress': 'baas-kafka-svc.baas:9092', 'kafkaStatusLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-status', 'kafkaCommandLog': 'backup-demo-vol01-k8s-k8s18-copy2-1591203980176-command', 'storageClass': None, 'sizeInBytes': None, 'pvclabels': {}},\n  {'kwargsrepr': '{}', 'origin': 'gen28@baas-transaction-manager-69cffc84fd-95kc4', 'reply_to': '38ff7ee8-718f-3b14-bd70-8a3f866823f6', 'correlation_id':... kwargs: {}})\n[2020-06-03 17:11:26,593: DEBUG/MainProcess] Task accepted: main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] pid:24

Create datamover demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176 PVC=pvc-backup-demo-vol01-1004-1591203980176 isBackup=True

[2020-06-03 17:11:27,127: INFO/ForkPoolWorker-1] Task main.backgroundprocess[29606e23-b6e3-4965-8156-930b42c12a25] succeeded in 0.5342374939937145s: 0
```

トランザクション・マネージャーのログで、次のトレース・ステートメントに、Get deployment 呼び出しでデプロイメントが成功したか失敗したかが示されます。

```
Get deployment backup-demo-vol01-k8s-k8s18-copy2-1591203980176 for PVC demo:backup-demo-vol01-k8s-k8s18-copy2-1591203980176
```

4. スケジューラーのログで、次の例のようなトレースを探して、コピー・バックアップが完了したかどうかを確認します。

```
copyBackup volume:demo:pvc-backup-demo-vol01-1004-1591203980176 jobInfoId=1004
ipAddr=[9.11.62.84] fileLocation= volumeSize=1073.741824 nextRunTime=1591290380176"
```

5. 例外が検出された場合は、COPYBACKUP 要求で次の例外が見つかる可能性があります。

表 68. 考えられるコピー・バックアップ例外	
例外	アクション
スナップショットが存在しません。 スナップショットが適切に作成されていない可能性があります。	次のコマンドを実行して、スナップショットが正しく作成されているかどうかを判別します。 <pre>kubectl describe volumesnapshots snapshotname -n namespace</pre>
デプロイメントが存在しません。 データ・ムーバーが適切に作成されていない可能性があります。	問題の詳細情報を確認するには、エラー・メッセージでデータ・ムーバー名を取得して、次のコマンドを実行します。 <pre>kubectl describe deploy backup-pvcname-jobname-job_timestamp -n namespace</pre>

6. 次のアクションを実行して、IBM Spectrum Protect Plus の問題のトラブルシューティングを行います。
- IBM Spectrum Protect Plus ユーザー・インターフェースで、インベントリー・ジョブがハングしていて、その他すべてのジョブが IBM Spectrum Protect Plus に記録されなくなっていないかどうかを確認します。
 - 実行中のジョブのリストまたはジョブ・ヒストリーで、ハングしたジョブを探します。以下の命名規則のジョブ名を探します。

```
k8s_sla_name
```

ここで、*sla_name* は、PVC に割り当てられている SLA ポリシーの名前です。

- ジョブ・ログを確認して、報告された問題があれば修正してください。IBM Spectrum Protect Plus のログ・ファイルの表示およびダウンロードについては、[324 ページの『ジョブ・ログの表示』](#)を参照してください。

ログ・ファイルのパッケージをダウンロードして、パッケージを展開します。ダウンロードしたパッケージの命名規則は次のとおりです。JobLog_*job_name*_job-timestamp.zip

ジョブについて詳しくは、command.log ファイルおよび JobLog_*k8s_sla_name*_job_timestamp.csv ファイルを確認してください。

リストア・ジョブのトラブルシューティング

リストア・ジョブが失敗した場合は、一連のアクションを実行して問題を診断することができます。

始める前に、トレース・レベルが DEBUG に設定されていることを確認してください。ログ・ファイルのトレース・レベルの設定の説明については、[521 ページの『ログ・ファイルのトレース・レベルの設定』](#)を参照してください。

リストア・ジョブの問題のトラブルシューティングを行うには、次のステップを実行します。

- Kubernetes Backup Support ログ・ファイルが使用可能であることを確認してください。ログ・ファイルを表示する手順については、[528 ページの『ログ・ファイルの表示』](#)を参照してください。
- onDemandRestore_*timestamp* という名前の IBM Spectrum Protect Plus サーバーのリストア・ジョブ・ログでエラーがないか確認します。

リストア・ジョブが **kubectl** コマンド・ラインから開始されていた場合は、次のコマンドを実行することにより、リストア・ジョブの進行中に BaasReq オブジェクトでリストア・ジョブの名前を見つけることができます。

```
kubectl describe baasreq restore_request_name -n namespace | grep Inprogress
```

次の例のような出力を探します。

```
Inprogress: onDemandRestore_1591384200276
```

3. **kubectl** コマンド・ラインからデータをリストアした場合は、YAML 構成ファイルの無効なパラメーターが原因でリストア・ジョブが無効になっているかどうかを確認します。**kubectl describe** コマンドを使用して、出力でリストア状況 (Restorestatus) を確認します。

Restorestatus フィールドの値が Invalid である場合、Errmsg フィールドに、リストア要求が無効になった理由が示されます。次の例では、YAML ファイルで **VolumeStorageClass** パラメーターに誤った値が指定されていました。

例えば、名前空間 test のリストア要求 copy-restore-pvc02 のリストア状況を表示するには、次のコマンドを実行します。

```
kubectl describe baasreq copy-restore-pvc02 -n test
```

出力は、以下の例のようになります。

```
Name:          copy-restore-pvc02
Namespace:     test
Labels:        <none>
Annotations:   <none>
API Version:   baas.io/v1alpha1
Backupstatus:  None
Errmsg:        VolumeStorageClass invalid
Kind:          BaaSReq
Metadata:
  Creation Timestamp:  2020-06-05T19:51:29Z
  Generation:         2
  Resource Version:    4396987
  Self Link:           /apis/baas.io/v1alpha1/namespaces/test/baasreqs/copy-restore-pvc02
  UID:                418cc8d5-7347-47ed-9436-9fe49f69b42a
Restorestatus:  Invalid
Spec:
  Inprogress:      None
  Origreqtype:     restore
  Pvcname:         pvc02
  Requesttype:     restore
  Restorepoint:    2020-06-05 17:22:35
  Restoretype:     copy
  Storageclass:    cirrus19-csi-rbd-sc
  Targetvolume:    pvc02-restored
  Volumename:      pvc02
  Events:          <none>
```

このタイプのエラーからリカバリーするには、無効なリストア要求を削除して、YAML ファイルを修正し、リストア要求を再作成してください。

4. IBM Spectrum Protect Plus サーバーの onDemandRestore_timestamp ログでエラー・メッセージを確認してください。通常は、問題の診断に役立てるのにエラー・メッセージで十分です。
5. スナップショット・リストアのトラブルシューティングをさらに行うために、アプリケーション・エージェントの baas-spp-agent ジョブ・ログで次の例のようなトレースを探することができます。

```
DEBUG pid:3402 MainThread restoreDatabase: Starting restore of snapshot
spp-1275-2213-17285db4b80 to test-snap-restore-pvc1
DEBUG pid:3402 MainThread restoreDatabase: Restoring pvc labels {'department': 'sales',
'team': 'green'}
DEBUG pid:3402 MainThread restoreDatabase: Restoring snapshot named spp-1275-2213-17285db4b80
DEBUG pid:3402 MainThread sendRestoreRequest: Sending restore request to https://baas-
transaction-manager:5000/restorevolumebackup/test/test-snap-restore-pvc1?storageclass=cirrus-
csi-rbd-sc&restoretype=FAST
DEBUG pid:3402 MainThread sendRestoreRequest: Get restore response
```

baas-transaction-manager ポッドで baas-transactionmanager コンテナ・ログを確認します。ログ・ファイルで、次の例のようなテキストを探します。

```
/restorevolumebackup/test/test-snap-restore-pvc1 snapshot:spp-1275-2213-17285db4b80
restoretype:FAST
storageclass: cirrus-csi-rbd-sc
```

6. コピー・リストアのトラブルシューティングをさらに 行うために、アプリケーション・エージェントの baas-spp-agent ジョブ・ログで次の例のようなトレースを探することができます。

```
JOBLOG_SUMMARY pid:4219 MainThread jobsummary: <CTGGK3005> Starting to restore a persistent
volume.
DEBUG pid:4219 MainThread copyRestore: Starting restore of database cirrus19:test:pvc02
DEBUG pid:4219 MainThread getPVC: PVC test:test-copy-restore-pvc02 not found.
DEBUG pid:4219 MainThread copyRestore: PVC does not exist, the restore can continue.
DEBUG pid:4219 MainThread createDatamover: PVC labels {'department': 'sales', 'team':
'green'}
INFO pid:4219 MainThread createDatamover: Create datamover request to https://baas-
transaction-manager:5000/datamover/test/test-copy-restore-pvc02
```

baas-transaction-manager ポッドで baas-transactionmanager コンテナ・ログを確認します。ログ・ファイルで、次の例のようなテキストを探します。

```
main:createdatamover Line 1187][DEBUG] - Creating deployment
restore-pvc02-ondemandrestore-1591390864757-1591390865107 for PVC test:test-copy-restore-
pvc02
```

transaction-manager-worker ログ・ファイルで、次の例のようなテキストを探します。

```
DEBUG/ForkPoolWorker-1] Restore worker
DEBUG/ForkPoolWorker-1] Create datamover test:restore-pvc02-
ondemandrestore-1591390864757-1591390865107
PVC=test-copy-restore-pvc02 isBackup=False
```

関連タスク

[521 ページの『ログ・ファイルのトレース・レベルの設定』](#)

ローカル・ログ・ファイルのトレース・レベルを設定すると、Kubernetes Backup Support で発生する可能性のある問題のトラブルシューティングに役立ちます。

関連資料

[523 ページの『トラブルシューティングのクイック・リファレンス』](#)

基本的な Kubernetes Backup Support の問題の解決策が提供されています。

第 21 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。

```
Warning
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 69. 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
CTGGK	IBM Spectrum Protect Plus for Containers
CTGGL	IBM Spectrum Protect Plus for Amazon EC2
CTGGR	IBM Spectrum Protect Plus for Microsoft Office 365
CTGGT	IBM Spectrum Protect Plus for file systems

すべてのメッセージのリストについては、IBM Knowledge Center ([ここをクリック](#)) 参照してください。

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

付録 B IBM Spectrum Protect 製品ファミリーのアクセシビリティ機能

アクセシビリティ機能は、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](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/) が、[US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) (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](http://www.w3.org/TR/WCAG20/) (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、アクセシビリティに対応しています。IBM Knowledge Center のアクセシビリティ機能については、[IBM Knowledge Center ヘルプの「Accessibility」セクション](http://www.ibm.com/support/knowledgecenter/about/releasesnotes.html#accessibility) (www.ibm.com/support/knowledgecenter/about/releasesnotes.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に対する取り組みについて詳しくは、[IBM Accessibility](http://www.ibm.com/able) (www.ibm.com/able) を参照してください。

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を提供し、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。

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をお願いします。

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を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。

登録商標 Linux は、世界中で商標の所有者である Linux Torvalds の独占的ライセンシーである Linux Foundation のサブライセンスに従って使用されています。

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を提供され、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。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。
なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

アクセシビリティ機能 [539](#)
アクセス制御
 MongoDB [421](#)
アドホック・ジョブ
 作成 [487](#)
アプリケーション・サーバー
 Db2 [353](#)
イメージ・プル・シークレットの作成
 Kubernetes Backup Support [143](#)
インストール
 仮想アプライアンス
 Hyper-V 上 [96](#)
 VMware 上 [94](#)
 ダウンロード・パッケージ、入手 [93](#)
 Kubernetes Backup Support [143](#)
 vSnap サーバー
 物理環境 [103](#)
 Hyper-V 環境 [106](#)
 VMware 環境 [104](#)
インベントリ
 ファイル・システム [294](#)
永続ボリュームのリストア
 Kubernetes [320](#)
オブジェクト・クライアント [193, 194](#)
オブジェクト・ストレージ
 Amazon S3 [178](#)
オフライン更新 [173](#)
オンデマンド・バックアップ
 コンテナ [332](#)
オンライン更新 [173](#)

[カ行]

開始
 ジョブ
 オンデマンド [481](#)
 スケジュールどおりに [228, 232, 234](#)
 IBM Spectrum Protect Plus [155](#)
概要
 Kubernetes Backup Support [309](#)
鍵
 削除 [208](#)
 追加 [206](#)
仮想アプライアンス
 アクセス
 Hyper-V [210](#)
 VMware [210](#)
 インストール
 Hyper-V 上 [96](#)
 VMware 上 [94](#)
更新 [173](#)
ストレージ容量の追加 [214](#)

仮想アプライアンス (続き)
 ディスクの追加 [213](#)
仮想環境 [193, 194](#)
管理コンソール、ログオン [204](#)
隔離ネットワーク、作成 [263](#)
キー
 削除 [205](#)
 追加 [205](#)
キーボード [539](#)
緊急修正プログラム [176](#)
クイック・スタート [153](#)
クラウド・サーバー
 Amazon S3 の追加 [178](#)
 IBM Cloud Object Storage リソースの追加 [179](#)
 Microsoft azure クラウド・リソースの追加 [181](#)
 s3 互換クラウド・リソースの追加 [182](#)
クラウド・プロバイダー
 削除 [184](#)
 編集 [184](#)
グローバル設定
 構成 [216](#)
検出
 ファイル・システム・リソース [294](#)
 Db2 [358](#)
更新
 vSnap サーバー (vSnap server) [170](#)
高速リストア
 コンテナ・データ [339](#)
高度なバックアップ・オプション [116](#)
コールド・データ・キャッシュ・ストレージ・プール [186](#)
コピー・バックアップ
 Kubernetes [317](#)
コピー・バックアップ (copy backup)
 Kubernetes Backup Support [329](#)
コピー・リストア
 永続ボリューム [320](#)
 コンテナ・データ [339](#)
コンテナ・データのバックアップ
 オンデマンド [332](#)
 スケジューリング [317, 329](#)
 名前空間別 [336](#)
 ラベル別 [333](#)
コンテナ・データのリストア
 Kubernetes Backup Support [339](#)

[サ行]

サービス・レベル・アグリーメント
 Kubernetes Backup Support [311](#)
 次も参照: SLA ポリシー
再実行
 ジョブ
 オンデマンド [486](#)
サイト
 削除 [200](#)
 スロットル [198, 199](#)
 追加 [198](#)

サイト (続き)
編集 [199](#)

削除
サイト [200](#)
ジョブ [486](#)
デモ [222](#)
役割 [511](#)
ユーザー [514](#)
リソース・グループ [507](#)
ID [515](#)
LDAP サーバー [204](#)
SLA デモ [239](#)
SLA ポリシー [239](#)
SMTP サーバー [204](#)

作成
役割 [509](#)
ユーザー
個別の [512](#)
LDAP グループ [512](#)
リソース・グループ [504](#)
レポート [499](#)
SLA ポリシー [228](#), [232](#), [234](#)
VADP プロキシ [252](#)

システム要件
コンポーネント [21](#)
ハイパーバイザー [37](#)
ファイル索引とリストア [40](#)
ファイル・システム [47](#)
Db2 [56](#)
Exchange Server [62](#)
Kubernetes Backup Support [51](#)
MongoDB [68](#)
Oracle [78](#)
SQL Server [85](#)

手動で登録
Kubernetes クラスター [314](#)

詳細なプロセス・ログ
O365 [349](#)

証明書
削除 [206](#)
追加 [206](#)

除去
デモ [222](#)

ジョブ
一時停止 [484](#)
開始
オンデマンド [481](#)
スケジュールどおりに [228](#), [232](#), [234](#)
解放 [484](#)
キャンセル [485](#)
再実行 [486](#)
削除 [486](#)
作成 [480](#)
進行状況、表示 [483](#)
スケジュール、編集 [485](#)
タイプ [479](#)
同時、表示 [484](#)
名前 [479](#)
表示 [482](#)
編集 [485](#)
ログ
ダウンロード [484](#)
表示 [484](#)
ジョブ・セッションの期限切れ [476](#)

ジョブと操作 [479](#)
ジョブの管理
コンテナのバックアップとリストア [342](#)
ジョブの期限切れ
Kubernetes Backup Support [323](#)
ジョブのスケジュール
バックアップ [362](#), [384](#), [429](#)
ジョブ・ログの表示
コンテナ・バックアップ [324](#)
資料 [ix](#)
身体障害 [539](#)
スケジューリング、バックアップの
Kubernetes [317](#)
Kubernetes Backup Support [329](#)
スナップショット・バックアップ
コンテナ [332](#)
Kubernetes [317](#)
Kubernetes Backup Support [329](#)
スナップショット保存 [476](#)
スナップショット・リストア
永続ボリューム [320](#)
スポンサー・ユーザー・プログラム
概要 [xiii](#)
利点 [xiii](#)
セキュリティ機能
Kubernetes Backup Support [313](#)
接続のテスト
Db2 [359](#)
接続のテスト、ファイル・システム [295](#)
前提条件
ファイル・システム [291](#)
Db2 [353](#)
Kubernetes Backup Support [143](#)
MongoDB [420](#), [421](#)
早期可用性更新、入手および適用 [176](#)

[タ行]

タイム・ゾーン、設定 [209](#)

追加
サイト [198](#)
Amazon EC2 アカウント [281](#)
Hyper-V サーバー [266](#)
ID [514](#)
LDAP サーバー [201](#)
Oracle アプリケーション・サーバー [448](#)
SMTP サーバー [202](#)
SQL Server アプリケーション・サーバー [461](#)
vCenter Server インスタンス [241](#)
vCenter 仮想マシンへの仮想ディスクの [213](#)
vSnap サーバー [109](#)
データ保護 [193](#), [194](#)
テープへのデータ・コピー
構成 [186](#)
テープへのデータのコピー [186](#)
デバッグ・ログ・ファイルの収集 Kubernetes Backup Support [520](#)
デプロイメント・ログ・ファイル Kubernetes Backup Support [520](#)
デモ
サイト [222](#)
SLA [222](#)
vSnap [222](#)
登録

登録 (続き)

Kubernetes クラスター [314](#)

vSnap サーバー [109](#)

トラブルシューティング

Kubernetes Backup Support [520](#)

Kubernetes Backup Support の操作 [527](#)

Kubernetes Backup Support のログの表示 [527](#)

トレースの有効化

Kubernetes Backup Support [521](#)

トレース・レベルの設定

Kubernetes Backup Support [521](#)

[ナ行]

名前空間別のバックアップ

Kubernetes Backup Support [336](#)

ネットワーク

テスト [211](#), [212](#)

ネットワーク構成 [113](#)

[ハ行]

バックアップ

コンテナ・データ [329](#)

ファイル・システム・データ [296](#)

Db2 [360](#)

バックアップ状況の表示

Kubernetes Backup Support [342](#), [344](#)

バックアップ・ジョブ

開始

オンデマンド [481](#)

スケジュールどおりに [228](#), [232](#), [234](#)

再実行

オンデマンド [486](#)

作成

Amazon EC2 [282](#)

Hyper-V [269](#)

IBM Spectrum Protect Plus [475](#)

Oracle [450](#)

SQL Server [463](#)

VMware [245](#)

VMDK の除外 [250](#)

バックアップ・ストレージ

高度なオプション、管理 [116](#)

ストレージ・オプション、ディスクの管理 [111](#)

ストレージ・オプション、パートナーの管理 [114](#)

バックアップ・ストレージ・サーバー

ストレージ・オプション、管理 [113](#), [115](#)

バックアップ・ストレージの構成

ストレージ・オプション、ディスクの追加 [112](#)

バックアップ操作とリストア操作のスクリプト

アップロード [488](#)

バックアップ・タイプ

Kubernetes Backup Support [310](#)

バックアップの削除

Kubernetes Backup Support [345](#)

バックアップの破棄 Kubernetes Backup Support [345](#)

バックアップ・履歴の表示

コンテナ・バックアップ [325](#)

バックアップ・ポリシー、参照: SLA ポリシー

ファイアウォール [99](#)

ファイル

検索 [537](#)

ファイル (続き)

リストア [287](#)

ファイル・システム

システム要件 [47](#)

ファイル・システムの追加 [292](#)

ファイル・システムのドライブの検出 [294](#)

複製パートナー [114](#)

プリファレンス

グローバル

構成 [216](#)

プロパティの変更

Kubernetes クラスター [314](#)

ベータ・プログラム

概要 [xiii](#)

利点 [xiii](#)

編集

サイト [199](#)

ジョブとジョブ・スケジュール [485](#)

設定 [203](#)

役割 [511](#)

ユーザー [513](#)

リソース・グループ [507](#)

ID [514](#)

LDAP サーバー [203](#)

SLA ポリシー [239](#)

SMTP サーバー [203](#)

[マ行]

マルチテナンシー

Kubernetes Backup Support [309](#), [313](#)

メッセージ

接頭語 [535](#)

モニター

コンテナ・バックアップ・ジョブ [324](#)

[ヤ行]

役割

許可タイプ [509](#)

削除 [511](#)

作成 [509](#)

編集 [511](#)

ユーザー

個別の、作成 [512](#)

削除 [514](#)

編集 [513](#)

役割

許可タイプ [509](#)

削除 [511](#)

作成 [509](#)

編集 [511](#)

リソース・グループ

削除 [507](#)

作成 [504](#)

タイプ [505](#)

編集 [507](#)

LDAP グループ、作成 [512](#)

ユーザー・アクセス [10](#), [503](#)

ユーザー役割

Kubernetes Backup Support [312](#)

要求タイプ

Kubernetes Backup Support [327](#)

[ラ行]

- ラベル別のバックアップ
 - Kubernetes Backup Support [333](#)
- リストア
 - ファイル・システム [302](#)
 - Db2 [367](#), [372](#), [375](#)
- リストア状況の表示
 - Kubernetes Backup Support [342](#), [344](#)
- リストア・ジョブ
 - 作成
 - AWS EC2 [284](#)
 - Hyper-V [273](#)
 - IBM Spectrum Protect Plus [475](#)
 - Oracle [453](#)
 - SQL Server [467](#)
 - VMware [256](#)
 - 実行
 - AWS EC2 [284](#)
 - Hyper-V [273](#)
 - Oracle [453](#)
 - SQL Server [467](#)
 - VMware [256](#)
- リストア・タイプ
 - Kubernetes Backup Support [310](#)
- リストア・ポイント、管理 [476](#)
- リストア・ポイント、削除 [477](#)
- リソース・グループ
 - 削除 [507](#)
 - 作成 [504](#)
 - タイプ [505](#)
 - 編集 [507](#)
- リポジトリ・サーバー・プロバイダー
 - 削除 [198](#)
 - 編集 [198](#)
- レポート
 - カスタム、作成 [499](#)
 - 実行、VM [496](#)
 - 実行
 - オンデマンド [498](#)
 - スケジュールどおりに [500](#)
 - タイプ
 - バックアップ・ストレージの使用状況 [491](#)
 - 保護 [492](#)
 - system [495](#)
- レポートの実行
 - コンテナ・バックアップ・ジョブ [324](#)
- ローカル・ホスト
 - vSnap [222](#)
- ログ
 - 監査 (audit)
 - ダウンロード [500](#)
 - 表示 [500](#)
 - system
 - ダウンロード [519](#)
 - 表示 [519](#)
- ログ・アーカイブ
 - Db2 [366](#)

[数字]

- のアンインストール Kubernetes Backup Support [151](#)
- データのリストア [320](#)
- トレース・ログの表示

- トレース・ログの表示 (続き)
 - Kubernetes Backup Support [522](#)
- SLA ポリシー割り当ての除去
 - Kubernetes [317](#)

A

- Amazon EC2
 - アカウント
 - 追加 [281](#)
 - バックアップ・ジョブ、作成 [282](#)
 - リソースの検出 [282](#)
 - IAM ユーザー、作成 [280](#)
- AWS EC2
 - リストア・ジョブ、作成 [284](#)

D

- Db2
 - システム要件 [56](#)
- Db2 区画の追加 [356](#)
- Db2 の検出 [358](#)
- Db2 の設定
 - SLA オプション [364](#)
- Db2 の追加 [356](#)
- Db2 のリストア
 - オリジナル・インスタンス [372](#)
 - 代替インスタンス [375](#)
- Db2 ログ・バックアップ [366](#)
- DEFINE STGPPOOL コマンド [186](#)

E

- Exchange Server
 - システム要件 [62](#)

H

- Hyper-V
 - 仮想アプライアンス
 - アクセス [210](#)
 - 仮想アプライアンスへのインストール [96](#)
 - サーバー
 - 接続のテスト [268](#)
 - リソースの検出 [268](#)
 - WinRM の有効化 [268](#)
 - 追加 [266](#)
 - バックアップ・ジョブ、作成 [269](#)
 - リストア・ジョブ、作成 [273](#)

I

- IBM Knowledge Center [ix](#)
- IBM Spectrum Protect Operations Center
 - への IBM Spectrum Protect Plus の追加 [16](#)
 - IBM Spectrum Protect Plus からのアクセス [15](#)
 - IBM Spectrum Protect Plus からの開始 [19](#)
 - IBM Spectrum Protect Plus のモニター [15](#), [19](#)
 - URL、設定 [18](#)
- IBM Spectrum Protect Plus バージョン バージョン 10.1.6 の新機能 [xi](#)
- IBM spectrum protect サーバー
 - リポジトリ・サーバーの追加 [196](#)

IBM spectrum protect サーバー (続き)
リポジトリ・サーバーの登録 [196](#)

ID

削除 [515](#)
追加 [514](#)
編集 [514](#)

iSCSI ユーティリティー
インストール [101](#)

K

Knowledge Center [ix](#)

Kubernetes

クラスター

手動で登録 [314](#)

プロパティの変更 [314](#)

Kubernetes Backup Support

アンインストール [151](#)

暗号化 [313](#)

イメージ・ブル・シークレットの作成 [143](#)

インストール [143](#)

概要 [309](#)

カスケード・アクション [143](#)

構成ファイル [146](#)

高速リストア [339](#)

コピー・バックアップ (copy backup) [329](#)

コピー・リストア [339](#)

コンテナ・データのバックアップ [329](#)

システム要件 [51](#)

ジョブの管理 [342](#)

ジョブの期限切れ [323](#)

ジョブのモニター [324](#)

ジョブ・ログの表示 [324](#)

スケジューリング、バックアップの [329](#)

スナップショット・バックアップ [329](#), [332](#)

セキュリティ [313](#)

前提条件 [143](#)

データのリストア [339](#)

デバッグ・ログ・ファイルの収集 [520](#)

デプロイメント・ログ [520](#)

トラブルシューティング [520](#)

トレースの有効化 [521](#)

トレース・レベルの設定 [521](#)

トレース・ログの表示 [522](#)

名前空間別の PVC のバックアップ [336](#)

名前空間別のバックアップ [336](#)

バックアップおよびリストアのタイプ [310](#)

バックアップ状況 [344](#)

バックアップ状況の表示 [342](#)

バックアップ・ジョブのトラブルシューティング [527](#)

バックアップの削除 [345](#)

バックアップ・履歴の表示 [325](#)

マルチテナンシー [313](#)

ユーザー役割 [312](#)

要求タイプ [327](#)

要求の破棄 [345](#)

ラベル別の PVC のバックアップ [333](#)

ラベル別のバックアップ [333](#)

リストア状況 [344](#)

リストア状況の表示 [342](#)

リストア・ジョブのトラブルシューティング [527](#)

レポートの実行 [324](#)

ログ・ファイルの表示 [527](#)

baas 要求 [327](#)

Kubernetes Backup Support (続き)

Kubernetes へのインストール [146](#)

Metrics Server の確認 [143](#)

SLA ポリシー [311](#), [329](#)

VolumeSnapshotDataSource フィーチャーの有効化 [143](#)

Kubernetes クラスター

接続のテスト [317](#)

リソースの検出 [316](#)

Kubernetes での構成

Kubernetes Backup Support [146](#)

Kubernetes へのインストール

Kubernetes Backup Support [146](#)

Kubernetes へのデプロイ

Kubernetes Backup Support [146](#)

L

LDAP

グループ、ユーザー・アカウントの作成 [512](#)

サーバー

削除 [204](#)

設定、編集 [203](#)

追加 [201](#)

Linux ベースの vCenter 仮想アプライアンス、バックアップ
[250](#)

M

Metrics Server の確認

Kubernetes Backup Support [143](#)

MongoDB

システム要件 [68](#)

MongoDB アプリケーション・サーバー [420](#)

MongoDB の追加 [423](#)

N

NIC [113](#)

O

O365 ログ・ファイル

詳細 [349](#)

Office 365 [347](#)

Operations Center

への IBM Spectrum Protect Plus の追加 [16](#)

IBM Spectrum Protect Plus からのアクセス [15](#)

IBM Spectrum Protect Plus からの開始 [19](#)

IBM Spectrum Protect Plus のモニター [15](#), [19](#)

URL、設定 [18](#)

Ops Manager

MongoDB [425](#)

Oracle

アプリケーション・サーバー

接続のテスト [450](#)

追加 [448](#)

リソースの検出 [450](#)

システム要件 [78](#)

バックアップ・ジョブ、作成 [450](#)

マルチスレッド・データベース [448](#)

リストア・ジョブ、作成 [453](#)

R

RBAC
MongoDB [421](#)

S

SLA [362](#), [384](#), [429](#)
SLA オプション
Db2 [364](#)
SLA バックアップの定義
Kubernetes [317](#)
SLA ポリシー
削除 [239](#)
追加 [228](#), [232](#), [234](#)
編集 [239](#)
Kubernetes Backup Support [311](#), [329](#)
SMTP
サーバー
削除 [204](#)
設定、編集 [203](#)
追加 [202](#)
SQL Server
アプリケーション・サーバー
接続のテスト [463](#)
追加 [461](#)
リソースの検出 [462](#)
システム要件 [85](#)
データ保護の要件 [460](#)
バックアップ・ジョブ、作成 [463](#)
リストア・ジョブ、作成 [467](#)
SSL 証明書、アップロード
管理コンソールからの [208](#)

V

VADP プロキシ
アンインストール [256](#)
オプション、設定 [254](#)
更新 [175](#)
作成 [252](#)
VMware
仮想アプライアンス
アクセス [210](#)
仮想アプライアンスへのインストール [94](#)
仮想マシンの特権、必要 [242](#)
バックアップ・ジョブ、SLA ポリシーからの VMDK の除外 [250](#)
バックアップ・ジョブ、作成 [245](#)
リストア・ジョブ
隔離ネットワークの作成 [263](#)
リストア・ジョブ、作成 [256](#)
vCenter Server インスタンス
追加 [241](#)
vCenter Server、接続のテスト [245](#)
vCenter Server、リソースの検出 [245](#)
VolumeSnapshotDataSource フィーチャー
Kubernetes Backup Support [143](#)
vSnap
更新 [172](#)
vSnap サーバー
アンインストール [107](#)
インストール

vSnap サーバー (続き)
インストール (続き)
物理環境 [103](#)
Hyper-V 環境 [106](#)
VMware 環境 [104](#)
追加 [109](#)
登録 [109](#)
vSnap サーバー (vSnap server)
管理
カーネル・ヘッダー
カーネル・ツール [128](#)
ストレージ管理 [125](#)
ネットワーク管理 [127](#)
ユーザー管理 [124](#)
初期化
拡張 [120](#)
簡単 [120](#)
ストレージ・プール、拡張 [121](#)
スループットの変更 [122](#)
登録抹消 [110](#)
編集 [110](#)
vSnap の修復 [122](#)
vSnap のリカバリー [122](#)

W

WinRM、Hyper-V サーバーに接続するための有効化 [268](#)

Y

YAML ファイル
Kubernetes Backup Support [327](#)



プログラム番号: 5737-F11

Printed in Japan